Agência Nacional do Cinema

Relatório de Impacto à Proteção de Dados Pessoais - RIPD

HISTÓRICO DE ALTERAÇÕES

Data	Versão	Descrição	Autor
31/03/2021	1.0	Versão Inicial	GT Implantação LGPD
31/01/2022	1.1	Alteração do nome do Encarregado	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 NECESSIDADE DE ELABORAR O RELATÓRIO

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é um documento previsto na Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), em vários dos seus dispositivos. Em especial, destacamos o Art. 38:

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
>
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

A elaboração do presente documento teve como base a seção 2.5 do Guia de Boas Práticas - Lei Geral de Proteção de Dados Pessoais (LGPD), versão 2.0, de agosto de 2020[1], bem como a metodologia de elaboração do Programa de Governança em Privacidade (PGP), ambos disponibilizados pelo Ministério da Economia[2].

Optou-se pela elaboração de um documento único para toda a organização, independentemente de sistema, serviço ou processo, em função de não haver tratamento em quantidade e diversidade expressiva de dados pessoais na ANCINE. A organização de um documento único também facilita a estruturação das informações e a análise dos riscos de forma global.

Este documento deve ser revisto e atualizado em virtude do surgimento de novas orientações da Autoridade Nacional de Proteção de Dados (ANPD), ou quando houver mudança significativa no escopo de tratamento de dados pessoais da ANCINE (alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados).

[1] Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd

[2] Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd

3 DESCRIÇÃO DO TRATAMENTO

Na ANCINE, o tratamento de dados pessoais possui a finalidade de cumprir obrigações legais, regulatórias e fiscalizatórias, além da execução de políticas públicas.

Nas seções subsequentes, serão sumarizados os dados pessoais relativos aos processos regulatórios de registro (obras e agentes econômicos), de fiscalização, e de disponibilização de informações de mercado (publicações no OCA), além dos dados referentes aos processos de fomento e prestação de contas, e dos processos de suporte administrativo, mapeados para tratamento nos termos da LGPD.

Para tanto, esses serão subdivididos em 6 (seis) grandes subconjuntos: Registro de Agentes Econômicos, Registro de Obras Brasileiras (CPB), Fiscalização do Mercado Audiovisual, Publicações do Observatório do Cinema e do Audiovisual (OCA), Processos de Fomento e Prestação de Contas e Processos de Suporte.

3.1 – NATUREZA DO TRATAMENTO

Nos itens a seguir, a ANCINE apresenta como são tratados os dados pessoais em cada um dos 06 (seis) subconjuntos mapeados, identificando os meios de coleta, armazenamento e uso.

3.1.1 Registro de Agentes Econômicos

A propósito da coleta de dados para registro de agentes econômicos (AEs), seu fundamento legal está fixado no art. 22 da MP n.º 2.228-1, de 2001, sendo regulamentado pela IN n.º 91, de 2010. A operação ocorre quando o agente econômico ingressa no portal eletrônico do Sistema Ancine Digital (SAD) (http://sad.ancine.gov.br/), na sequência, insere as informações de registro, nos termos dessa IN n.º 91, e encaminha os documentos comprobatórios via *upload*. O servidor designado pela área de registro da Ancine analisa a documentação enviada e defere ou indefere o registro solicitado. A informação pode ser compartilhada com outras áreas da Agência, mediante consulta ao SAD, ou relatórios do Sistema de Informações Ancine (SIA). Os registros de AEs, a pedido do agente externo interessado ou de ofício, podem ser cancelados ("dado baixa") devido ao fim do exercício das atividades econômicas, ou morte natural da pessoa física, por exemplo.

3.1.2 Registro de Obras Brasileiras (CPB)

No tocante à coleta de dados para registro de obras audiovisuais brasileiras, seu fundamento legal decorre do art. 28 da MP n.º 2.228-1, de 2001. Essa operação ocorre quando o requerente (interessado) ingressa no portal eletrônico do Sistema Ancine Digital (SAD) (http://sad.ancine.gov.br/) e, na sequência, insere as informações de registro de obra audiovisual brasileira, nos termos da IN n.º 104, de 2012, encaminhando os documentos comprobatórios via *upload,* além de envio de mídia física (DVD) via protocolo físico, ou de link de acesso ao conteúdo (plataformas de *streaming* ou armazenamento em nuvem, por exemplo) relativo à obra que se pretende registrar na Agência. Em seguida, o servidor designado pela área de registro da Ancine analisa a documentação enviada pelo requerente e defere ou indefere o registro solicitado. A informação pode ser consultada por outras áreas internas à Agência, mediante consulta ao SAD, ou relatórios SIA.

3.1.3 Fiscalização do Mercado Audiovisual

Relativamente ao tratamento de dados pessoais em processos de trabalho dirigidos à fiscalização do mercado audiovisual, seu fundamento decorre de obrigações estipuladas pela MP n.º 2.228-1 e pela Lei n.º 12.485, de 2011, regulamentadas pela Instrução Normativa nº 109, de 2012. A operação de coleta é efetuada a partir da

base de registro do SAD, na qual estão armazenados os dados pessoais oriundos das operações de registro de agente econômico junto à Ancine. De forma geral, essas informações, após essa coleta, são inseridas nos processos fiscalizatórios e/ou sancionatórios abertos no Sistema Eletrônico de Informações (SEI), sendo utilizadas para identificar a pessoa natural responsável, em casos de indícios de irregularidade, de comprovada irregularidade, ou de aplicação de sanções. Tanto a ação de coleta quanto a de tratamento são realizadas por servidores em exercício na área de fiscalização e com acesso autorizado ao SAD e ao SEI. Quando pertinente e regularmente solicitados, esses processos podem ser compartilhados internamente com a Procuradoria Federal ou com Auditoria Interna mediante acesso e/ou tramitação eletrônicos via SEI.

3.1.4 Publicações do Observatório do Cinema e do Audiovisual (OCA)

Quanto ao tratamento de dados pessoais coletados e tratados previamente à publicação de informes e estudos acerca do mercado audiovisual no OCA, seu fundamento legal decorre das competências de monitoramento fixadas no inciso XIV do art. 7º da MP n.º 2.228-1, de 2001. Em caso de "nome da pessoa natural", esse dado é requisitado junto à área de registro da Agência, em formato de planilha eletrônica. Em caso de dados referentes ao nome de diretor ou de produtor (pessoa física), esses podem ser tratados de forma que o nome da pessoa natural seja transformado em nome artístico, caso isso melhore a comunicação acerca de quem se pretende citar em determinado estudo de mercado. A unidade da federação (UF) de investidor pessoa física de projetos audiovisuais, quando se trata de publicação sobre recursos financeiros destinados ao setor audiovisual, é informação que advém do fomento, em formato de planilha eletrônica, não passando por nenhum tratamento adicional prévio à publicação no Observatório. A unidade da federação (UF) de produtores (pessoa física) é informação que advém da área de registro, em formato de planilha eletrônica, e não passa por nenhum tratamento adicional prévio à publicação no Observatório.

Por fim, em relação ao formulário OCA (canal de atendimento "contato" por meio do qual interessados externos enviam dúvidas ou solicitam informações sobre publicações disponíveis no portal via <https://oca.ancine.gov.br/contato>), os dados são coletados a partir do preenchimento desse formulário pela pessoa natural e armazenados no site de administração do OCA, em formato ".csv". Nesse caso, salienta-se que esses dados não são utilizados para além da finalidade de identificação do interessado ou compartilhados internamente.

3.1.5 Processos de Fomento e Prestação de Contas

No escopo dos processos de fomento e de prestação de contas, os dados pessoais são coletados mediante preenchimento de formulário eletrônico e upload em sistemas, através de recebimento de documentos físicos e digitalizados e inspeções *in loco*.

Os dados são retidos e armazenados nos respectivos sistemas e replicados em processo eletrônico no Sistema Eletrônico de Informações (SEI). Há também a guarda de documentos em processos físicos e mídias físicas, como CDs, DVDs etc.

Alguns dados são compartilhados com agentes financeiros e entes de fomento regionais, como secretarias municipais e estaduais de cultura, a depender da modalidade de fomento.

Os dados podem ser compartilhados também a pedido de terceiros ou de interessados através da ouvidoria e através de órgãos de controle e judiciais, para realização de estudos por órgão de pesquisa. No caso do serviço de autorização de filmagem estrangeira no Brasil, os dados são compartilhados com representações diplomáticas para concessão de visto para profissionais estrangeiros atuantes em filmagens em solo nacional.

Seja em função dos pedidos por meio da Lei de Acesso de Informação - LAI, ou via transparência ativa, com a disponibilização de dados em portais e 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.

3.1.6 Processos de Suporte (Administração de Pessoal e Terceiros)

No escopo dos processos de suporte, destacam-se o tratamento de dados pessoais de servidores e estagiários, coletados mediante apresentação voluntária dos documentos pelo interessado, juntados no Assentamento Funcional ou nos sistemas estruturantes específicos (SIGEPE, SIASS, SIAPE). Os dados são consultados pela Gerência de Recursos Humanos para operacionalização de suas atividades. Os dados pessoais podem ser compartilhados a pedido de órgãos de controle e judiciais, ou com autorização do servidor, como no empréstimo consignado.

Ainda dentro do escopo dos processos de suporte, importante mencionar os dados pessoais de terceirizados colaboradores, coletados de acordo com o normativo que gere a fiscalização dos contratos administrativos. São armazenados no SEI podendo ocasionalmente serem armazenados nas pastas eletrônicas setoriais. Os dados são consultados para fins de verificação de obrigações trabalhistas, tratamento de ações judiciais de colaboradores, e validação de representantes legais das empresas. Podem ser compartilhados a pedido de órgãos de controle e judiciais.

3.2 – ESCOPO DO TRATAMENTO

A seguir, estão relacionados os tipos dos dados pessoais tratados em cada subconjunto, identificando quais deles englobam dados pessoais sensíveis. Encontram-se também apontados: a extensão e frequência em que os dados são tratados; o período de retenção, a abrangência da área geográfica do tratamento, dentre outras informações.

3.2.1 Registro de Agentes Econômicos

I - Registro de agentes econômicos (pessoa física ou pessoa jurídica) agrega os seguintes dados pessoais: Nome da pessoa natural, Endereço residencial, Telefone residencial e/ou celular, Endereço eletrônico (e-mail), Nacionalidade, Data de Naturalização, Data de Nascimento, Página eletrônica (referente a pessoa natural), Nome artístico (referente a pessoa natural), Situação do registro de Agente Econômico Pessoa Física (deferido e indeferido), Residência no Brasil (sim ou não e data de início de residência no Brasil), CPF, Documento de Identidade, Número de Registro Ancine, procurações de outorga por parte do agente econômico, gênero da pessoa natural (feminino ou masculino), data de nascimento, local de nascimento, nacionalidade, participação em outras empresas e/ou grupo econômico (sócio, cotas patrimoniais, ou representante). Tais dados são tratados durante o expediente de trabalho de registro de agente econômico pela área responsável. A respeito da temporalidade, conforme Tabela de Temporalidade Ancine, o prazo de retenção seria de 15 anos. A abrangência geográfica seria nacional.

3.2.2 Registro de Obras Brasileiras (CPB)

Registro de obras brasileiras (CPB) engloba as seguintes informações pessoais: Nome da pessoa natural requerente de CPB, Autores do argumento e/ou roteiro, Nome e CPF dos integrantes da equipe técnica, Nome do diretor da obra audiovisual brasileira, Nome da equipe técnica contratada para realização da obra audiovisual brasileira, Agente econômico pessoal física financiador da obra audiovisual brasileira, Detentores (pessoa física) dos direitos patrimoniais (cotas patrimoniais e poder dirigente), Detentores (pessoa física) de direitos de exploração comercial da obra, Detentores (pessoa física) de direitos de comunicação pública da obra, Detentores (pessoa física) de direitos sobre a receita de exploração comercial da obra, Nome de

produtores pessoas físicas, CPF ou RNE (Registro Nacional de Estrangeiro), ou Carteira de Registro Nacional Migratório (CRNM) em caso de estrangeiros, gênero da pessoa natural (feminino ou masculino), imagem e som de pessoa natural contida na mídia (DVD) submetida à registro de CPB. Esses dados são tratados durante o expediente de trabalho de registro de obra brasileira pela área responsável. A respeito da temporalidade, conforme Tabela de Temporalidade Ancine, o prazo de retenção seria de 130 anos. A abrangência geográfica seria nacional.

3.2.3 Fiscalização do Mercado Audiovisual

Fiscalização do Mercado Audiovisual reúne os seguintes dados pessoais: Nome da pessoa natural, endereço, contato telefônico, e-mail, CPF, Documento de Identidade. Dados esses que são coletados a partir da base de registro de agente econômico do SAD. Tais dados são tratados durante o expediente de trabalho de fiscalização das obrigações regulatórias (IN nº 109, de 2012) em face de agentes econômicos de mercado regulado pela Ancine. A respeito da temporalidade, conforme Tabela de Temporalidade Ancine, o prazo de retenção seria de 10 anos. A abrangência geográfica seria nacional.

3.2.4 Publicações do Observatório do Cinema e do Audiovisual (OCA)

Publicações do Observatório do Cinema e do Audiovisual (OCA) engloba os seguintes dados pessoais: nome da pessoa natural (diretor e produtor) e unidade da federação de produtor pessoa física – ambos da base de registro do SAD -; unidade da federação de investidor pessoa física – dado oriundo do fomento-; nome da pessoa natural requerente, e-mail e atividade profissional – dados informados pelo interessado em caso de solicitações via Formulário do OCA. Esses dados são tratados durante o expediente de trabalho de operação do OCA pela área responsável. A propósito da temporalidade, conforme Tabela de Temporalidade Ancine, o prazo de retenção seria de 15 anos. A abrangência geográfica seria nacional.

Ressalte-se que o escopo do tratamento de dados pessoais em processos regulatórios detalhado segundo os quatro subconjuntos de dados pessoais supracitados não engloba dados pessoais sensíveis.

3.2.5 Processos de Fomento e Prestação de Contas

No escopo dos processos de fomento e prestação de contas são tratados dados de identificação pessoal, dados financeiros (atividade profissional e acordos e ajustes comerciais), características pessoais (detalhes pessoais e situação de imigração), composição familiar, penalidades administrativas, dados residenciais, dados de educação, treinamento, profissão e emprego (dados acadêmicos, qualificação e experiência profissional, emprego atual e carreira), registros de vídeo, imagem e voz. No âmbito dos apoios internacionais, adicionalmente são tratados dados de identificação e situação financeira, viagens e deslocamentos e associação a programas setoriais de exportação.

Em relação a dados pessoais sensíveis, as áreas tratam informações de origem racial ou étnica. Eventualmente, no contexto de participação cidadã na elaboração de políticas públicas, são coletados indiretamente dados referentes a filiação a sindicato.

Os titulares afetados são representantes legais de agentes econômicos e terceiros interessados na obtenção de fomento a obras audiovisuais, tais como profissionais nacionais e estrangeiros do setor audiovisual. Os dados possuem abrangência geográfica nacional. Em relação à temporalidade, sua guarda é por tempo indefinido. A coleta e tratamento é realizada durante o expediente, por servidores e estagiários.

3.2.6 Processos de Suporte (Administração de Pessoal e Terceiros)

No escopo dos processos de suporte, no caso de servidores e estagiários, são tratados dados de identificação pessoal, dados financeiros incluindo transações financeiras, características pessoais, composição familiar, associações, dados residenciais, dados de educação e treinamento e profissão e emprego (dados acadêmicos, qualificação e experiência profissional, emprego atual e carreira). A respeito da temporalidade, são mantidos de forma indefinida nas bases dos sistemas estruturantes de governo. A abrangência geográfica é nacional.

Para os terceirizados colaboradores, são tratados dados de identificação pessoal, dados financeiros, características pessoais, composição familiar, associações, dados residenciais, dados de educação e treinamento e profissão e emprego (dados acadêmicos, qualificação e experiência profissional, emprego atual, rescisão e carreira). Os dados pessoais são eliminados, após finalização do contrato, de acordo com a tabela de temporalidade dos documentos. A abrangência geográfica é nacional.

3.3 – CONTEXTO DO TRATAMENTO

A ANCINE trata os dados pessoais com o objetivo de cumprir com suas competências, obrigações e compromissos com a sociedade, tendo em vista o interesse público. A seguir, destacamos os parâmetros que demonstram este equilíbrio entre a necessidade da Agência em tratar os dados pessoais e os direitos dos titulares de tais dados.

3.3.1 Processos Regulatórios: Registro de Agentes Econômicos, Registro de Obras Brasileiras (CPB), Fiscalização do Mercado Audiovisual, Publicações do Observatório do Cinema e do Audiovisual

Os processos regulatórios, aqui mapeados para tratamento nos termos da LGPD e apresentados sob a forma de quatro subconjuntos de dados: Registro de agentes econômicos (pessoa física ou jurídica), registro de obras brasileiras (CPB), Fiscalização do mercado audiovisual, Publicações do Observatório do Cinema e do Audiovisual, decorrem da relação regulatória entre Ancine e agentes econômicos que exploram atividade em segmentos de mercado audiovisual regulados no país, seja pela MP n.º 2.228-1, de 2001, seja pela Lei n.º 12.485, de 2011. No caso de agente externo que entram em contato com o OCA via formulário disponível na página do Observatório, o mesmo pode ser interessado em informações de mercado (pesquisadores e cidadãos, em geral).

Os servidores e colaboradores que tratam esses dados regulatórios estão autorizados a executar essa atividade no âmbito de suas unidades de lotação e exercício e de acordo com as competências regimentais dessas fixadas nas Resoluções de Diretoria Colegiada n.º 59, de 2014, e n.º 60, de 2014, (Regimento Interno e Norma Complementar).

Por fim, salienta-se que os supra referidos subconjuntos regulatórios, em regra, não envolvem tratamento de dados pessoais de vulneráveis. No caso específico de Registro de Obras Brasileiras (CPB), se essas obras contarem com a participação de crianças, adolescentes ou vulneráveis, dados pessoais envolvendo esses grupos serão objeto de tratamento (registro de vídeo, som, imagem e ficha técnica de equipe).

3.3.2 Processos de Fomento e Prestação de Contas

O tratamento de dados pessoais em processos de fomento e prestação de contas decorre do acesso dos agentes regulados aos mecanismos de fomento de incentivo fiscal ou fomento direto, em especial investimentos do Fundo Setorial do Audiovisual, e ocorre em decorrência da legislação do setor: Lei 8.313, de 1991, Lei nº 8.685, de 1993, MP n.º 2.228-1, de 2001 e Lei nº 11.473, de 2006. O objetivo prioritário das ações

de fomento e prestação de contas são agentes econômicos empresariais, de modo que o tratamento de dados pessoais é, na maioria dos processos, e não envolve tratamento de dados pessoais de vulneráveis na maioria dos casos. Especificamente para obras que contam com participação de crianças, adolescentes ou vulneráveis, dados pessoais envolvendo esses grupos serão objeto de tratamento (registro de vídeo, som, imagem, e dados associados a contratos e pagamentos).

3.3.3 Processos de Suporte (Administração de Pessoal e Terceiros)

O tratamento de dados pessoais em processos de suporte, se dá por servidores das áreas de Gerência de Recursos Humanos e Gerência de Administração. Os servidores que tratam esses dados estão autorizados a executar essa atividade no âmbito de suas unidades de lotação e exercício e de acordo com as competências regimentais dessas fixadas nas Resoluções de Diretoria Colegiada n.º 59, de 2014, e n.º 60, de 2014, (Regimento Interno e Norma Complementar). Os referidos subconjuntos regulatórios, em regra, não envolvem tratamento de dados pessoais de vulneráveis.

No que tange aos aspectos tecnológicos da segurança da informação, a ANCINE adota boas práticas e tecnologias de mercado que visam proteger os dados pessoais em formato digital. O uso de mecanismos de proteção para redes e de softwares contra a disseminação de malwares são exemplos de ações que mitigam eventuais ataques direcionados ao ambiente computacional, onde são processados e armazenados os dados pessoais digitais da Agência. Soma-se a isso a proteção do ambiente por meio da utilização de controles de acesso lógico e físico, assim como o armazenamento de registros (logs) dos serviços e sistemas, que podem ser usados para análises forense em caso de incidentes de segurança que envolvam dados pessoais.

3.4 – FINALIDADE DO TRATAMENTO

Em consonância com o disposto no art. 7 º da LGPD, o tratamento dos dados pessoais pela ANCINE tem como finalidade o cumprimento de obrigação legal e regulatória, e a execução de políticas públicas. Nesta seção, são apresentadas as razões e benefícios do tratamento de dados pessoais em cada um dos 06 (seis) subconjuntos mapeados para tratamento nos termos da LGPD.

3.4.1 Processos Regulatórios: Registro de Agentes Econômicos (pessoa física ou jurídica), Registro de Obras Brasileiras (CPB), Fiscalização do Mercado Audiovisual, Publicações do Observatório do Cinema e do Audiovisual

Dentre os processos regulatórios executados pela Ancine focados no mercado audiovisual, os registros de agentes econômicos (pessoa jurídica e pessoa física) e de obras audiovisuais brasileiras são obrigações cujo cumprimento é exigível dos agentes de mercado, consoante previsões fixadas nos artigos. 22 e 28 da MP n.º 2.228-1, de 2001, respectivamente.

Relativamente aos processos fiscalizatórios executados pela agência sobre esse mercado, há um conjunto de obrigações estipuladas pela MP n.º 2.228-1 e pela Lei 12.485, de 2011, cujos processos sancionadores, abertos em caso de eventuais infrações, estão regulamentados pela Instrução Normativa nº 109, de 2012.

Por fim, no que tange ao processo destinado à geração e à difusão de informação e de conhecimento acerca do mercado audiovisual, sobretudo o regulado, por meio do Observatório Brasileiro do Cinema e do Audiovisual (OCA), compete à Agência também efetuar o monitoramento das atividades econômicas da indústria audiovisual por meio da circulação de estudos, painéis, e análises de mercado, em consonância com

o inciso XIV do art. 7º da MP n.º 2.228-1, de 2001.

A propósito dessas três finalidades regulatórias mapeadas ao longo do levantamento de inventário de dados pessoais, todas essas estão relacionadas à hipótese de "cumprimento de obrigação legal ou regulatória pelo controlador" (inciso II do art. 7º e alínea "a" do inciso II do art. 11 da LGPD). A partir do tratamento dos dados pessoais coletados durante a execução desses processos, pretende-se viabilizar o exercício dos direitos dos titulares dos dados, em regra, cidadãos que desempenham atividades e negócios audiovisuais regulados e passíveis de fiscalização pela Ancine. Com isso, almeja-se alcançar benefícios de adequação à LGPD e de efetivação da proteção aos direitos fundamentais de inviolabilidade da intimidade, vida privada, honra e imagem dos agentes regulados que depositarem informações pessoais junto à Agência no decorrer de cada um desses processos.

3.4.2 Processos de Fomento e Prestação de Contas

Os processos de fomento e prestação de contas realizados na Ancine são resultado do cumprimento de obrigações legais, conforme previsto na legislação do setor: Lei 8.666/93, Lei 8685/93, Lei 8313/91, Lei 11437/2006 e MP 2228-1/01. A regulamentação específica encontra-se nas Instruções Normativas nº 106, nº125 e nº150, no Regulamento Geral do Prodav, além das Chamadas Públicas do FSA e contratos de apoio e investimento. Os processos atendem aos interesses do titular de dados no exercício do seu direito próprio, ou de pessoas jurídicas que representam, de ter acesso aos mecanismos de fomento.

Nos processos de prestação de contas, o objetivo é analisar e decidir sobre a prestação de contas financeira dos projetos realizados com recursos públicos geridos pela ANCINE, além do cumprimento de seu objeto, bem como a tomada de contas especial de projetos audiovisuais incentivados. Além disso, é atribuição da Superintendência de Prestação de Contas propor a cobrança extrajudicial de débitos oriundos de projetos audiovisuais financiados com recursos públicos geridos pela ANCINE, bem como efetuar a cobrança e gerir o parcelamento da devolução de recursos de renúncia fiscal. Para tanto, há a coleta e tratamento de dados pessoais, notadamente os financeiros e bancários, tais como notas fiscais, recibos, declarações e informações de órgãos sobre solvência.

Em um espectro mais amplo, a execução da política pública do audiovisual visa ampliar a oferta de conteúdo e o acesso à cultura, gerando benefícios para a sociedade como um todo. Nesse cenário, a finalidade da coleta e tratamento dos dados pessoais nos processos de fomento e prestação de contas é meio para cumprir as obrigações legais e regulatórias do setor audiovisual, além de permitir a execução de políticas públicas no setor, atendendo também ao interesse público, do momento em que proporciona a adequada averiguação da aplicação de recursos.

3.4.3 Processos de Suporte (Administração de Pessoal e Terceiros)

No escopo dos processos de suporte, no caso de servidores e estagiários, o tratamento se justifica para atendimento do disposto na Lei 8112/90, Lei 12813/2013 (Conflito de Interesses), Decreto 7203/2010 (Nepotismo) e Decreto 9991/2019 (Política Nacional de Desenvolvimento de Pessoas). Para os terceirizados colaboradores, a finalidade do tratamento dos dados pessoais está amparada na Lei 8666/93 e Instrução Normativa nº 5, de 26 de maio de 2017 do Ministério do Planejamento, Desenvolvimento e Gestão.

4 PARTES INTERESSADAS CONSULTADAS

Para a elaboração da versão inicial deste Relatório, foi formado um Grupo de Trabalho composto por representantes das áreas que participam do Comitê de Segurança de Informação e Comunicação – CSIC da ANCINE: Secretaria de Gestão Interna, Gerência de Tecnologia de Informação, Coordenação de Documentação e Patrimônio, Secretaria de Políticas Regulatórias, Secretária de Políticas de Financiamento e Ouvidoria Geral.

A Secretaria de Gestão Interna coordenou os trabalhos, ajudando a consolidar as informações das diferentes áreas da organização e a adequação à metodologia de elaboração do PGP. A Gerência de Tecnologia de Informação contribuiu avaliando os riscos de segurança de informação a partir dos processos, ferramentas e infraestrutura computacional instalada. A Coordenação de Documentação e Patrimônio da Gerência de Administração contribuiu na área de gestão documental, em especial os parâmetros de guarda e eliminação de documentos.

Em relação aos processos regulatórios, a Secretaria de Políticas Regulatórias consultou servidores das áreas finalísticas da Agência que recepcionam e fazem tratamento de dados pessoais de agentes econômicos para fins de regulação e fiscalização do mercado audiovisual (Coordenação de Registro de Obras, Coordenação de Registro de Agentes Econômicos, Superintendência de Fiscalização e Coordenação de Gestão das Informações Regulatórias).

Em relação aos processos de fomento, a Secretaria de Políticas de Financiamento consultou servidores das áreas finalísticas que operam as ações de fomento e prestação de contas – Superintendência de Fomento, Superintendência de Prestação de Contas e Coordenação de Programas Internacionais.

Já a Ouvidora Geral, através do papel de Encarregado de Tratamento de Dados Pessoais da ANCINE, auxiliou na revisão, validação e complementação das informações do Relatório, esclarecendo as dúvidas técnicas e conceituais dos integrantes do Grupo de Trabalho, utilizando a base de conhecimento acumulada em função do atendimento às demandas externas ligadas à Lei de Acesso à Informação.

5 NECESSIDADE E PROPORCIONALIDADE

A hipótese legal para tratamento de dados pessoais pela ANCINE se enquadra no previsto pelo art. 7º, incisos II e III da LGPD:

> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (...);

De uma forma geral, o tratamento de dados pessoais na ANCINE possui a finalidade de cumprir obrigações legais, regulatórias e fiscalizatórias, bem como, 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 (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 decorre do legítimo exercício das competências regulatórias da Ancine fixadas na MP n.º 2.228-1, de 2001 e na Lei n.º 12.485, de 2011, sendo imprescindíveis e proporcionais ao regular exercício e aos objetivos desses marcos regulatórios do setor audiovisual brasileiro.

No âmbito dos processos de fomento, o tratamento de dados pessoais se dá para a concretização dos objetivos dos processos de fomento e de prestação de contas, com a finalidade última de cumprir sua função regulatória em prol do setor audiovisual. A coleta dos dados pessoais, em muitos casos, é feita de forma incidental aos procedimentos, como na hipótese de informações adquiridas no corpo de contratos de prestação de serviços ou notas fiscais. O fundamento legal para os procedimentos executados por essas áreas encontra respaldo nas Leis nº 8.666, de 1993, Lei nº 8.685, de 1993, Lei nº 8.313, de 1991, Lei nº 11.437, de 2006 e MP nº 2.228-1, de 2001, além das Instruções Normativas da ANCINE nº 79, 106, 125 e 150; e das Portarias ANCINE nº 27-E de 2019 e nº 120 de 2016.

A coleta dos dados pessoais realizada pela ANCINE está circunscrita ao mínimo de dados necessários para a realização das finalidades informadas ao titular, com o propósito de cumprimento de obrigação legal e regulatória, de monitoramento, de fomento, além de publicação e divulgação de informes e estudos atinentes ao mercado audiovisual No caso do Sistema Ancine Digital, as informações pessoais são providas pelos agentes econômicos, regulados e proponentes, ao solicitar os serviços digitais da ANCINE. Para dados pessoais armazenados em outros órgãos públicos, como a Receita Federal, existe uma integração com o objetivo de assegurar a qualidade e a atualização dos dados pessoais.

O tratamento de dados pessoais conforme as normas da LGPD e os critérios estabelecidos pela instituição são assegurados através de diferentes linhas de defesa, especialmente através do acompanhamento do Programa de Governança em Privacidade – PGP pelo Comitê de Segurança de Informação e Comunicação – CSIC, e a atuação das instâncias de controle interno como Auditoria, Ouvidoria, Comissão de Correição e Comissão de Ética. Além disso, em observância ao Plano Diretor de Tecnologia de Informação e Comunicação – PDTIC, a infraestrutura computacional instalada está em constante aprimoramento com o objetivo de mitigar os riscos de segurança de informação.

Importante destacar que todo servidor ou terceirizado deve seguir o código de conduta do agente público civil do Poder Executivo Federal (https://www.gov.br/economia/pt-br/centrais-de-conteudo/publicacoes/guias-e-manuais/manual-de-conduta-do-agente-publico-civil.pdf), bem como o Decreto n.º 1.171, de 22 de junho de 1994 que trata do Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal. Além disso, os sistemas de informação possuem l*ogs* e controles com definição de níveis de acesso, concedidos aos usuários mediante autorização prévia das respectivas chefias.

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 externos como TCU e CGU.

Em relação aos direitos do titular, em atendimento aos art. 18 a 20 da LGPD, estes podem ser exercidos preferencialmente através da plataforma Fala.BR (https://falabr.cgu.gov.br). 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 LGPD e na Lei de Proteção e Defesa do Usuários de Serviços Públicos, de nº 13.460, de 23 de junho de 2017.

6 IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Segundo a LGPD, art. 5º, XVII, o RIPD deve descrever medidas e mecanismos de mitigação de riscos:

> XVII - 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;

E no Art. 46 da LGPD verificamos que:

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito

Para a etapa de identificação e avaliação dos riscos de privacidade, nessa primeira versão do RIPD, optou-se por seguir estritamente a metodologia apresentada na seção 2.5.2.6 do Guia de Boas Práticas, incluindo o rol de 14 riscos sugeridos e que foram obtidos da norma ISO/IEC 29134:2017 seção 6.4.4.

Tal metodologia utiliza um questionário de aplicação de 131 controles para pontuar, de forma automatizada, para cada um dos riscos, a probabilidade de ocorrência do evento e o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento, conforme figura abaixo.

Controles implementados	Probabilidade	Impacto
0 a 50 por cento	Alta	
50 a 85 por cento	Moderada	Alto
85 a 100 por cento	Baixa	Moderado

Figura 1 - Relação Controle x Probabilidade e Impacto

Importante observar que a ANCINE possui uma Política de Gestão de Riscos formalizada através da Resolução de Diretoria Colegiada No. 78 de 6 de setembro de 2017 (posteriormente alterada pelas Resoluções Nos. 79, 90 e 107), que indica no seu Art. 7º a utilização da Metodologia de Gestão de Riscos institucional. No entanto, como na Metodologia sugerida pelo Ministério da Economia a gradação dos 14 riscos é feita de forma objetiva a partir de controles consagrados em normas ISO de segurança de informação, optou-se por utilizá-la na elaboração da primeira versão do RIPD a fim de obter os níveis de risco e as medidas mitigadoras associadas com maior acurácia.

A avaliação do apetite a risco, a governança e o monitoramento dos riscos associados ao RIPD seguirão conforme a Política de Gestão de Riscos e a Metodologia de Gestão de Riscos da ANCINE, bem como eventuais avaliações de novos riscos nas eventuais revisões do documento.

A Figura 2 apresenta a Matriz Probabilidade x Impacto utilizada como apoio para a definição dos critérios de classificação do nível de risco na metodologia do Ministério da Economia, utilizada neste documento.

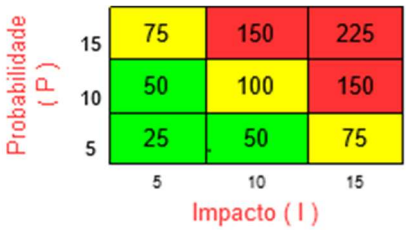

Figura 2 - Matriz Probabilidade x Impacto
(Ministério da Economia)

Já a Figura 3, apresenta a Matriz utilizada na metodologia da ANCINE. Observa-se que, apesar das gradações diferentes de probabilidade e impacto, os níveis de risco escalares são semelhantes, tornando possível uma compatibilização entre as metodologias disponíveis.

Quadro 5: Matriz de Riscos

Nível de Risco		Probabilidade				
Extremo Alto Médio Baixo		Raro 1	Improvável 2	Possível 3	Provável 4	Quase Certo 5
Impacto	Extremo 16	16	32	48	64	80
	Alto 8	8	16	24	32	40
	Médio 4	4	8	12	16	20
	Baixo 2	2	4	6	8	10
	Muito baixo 1	1	2	3	4	5

Figura 3 - Matriz Probabilidade x Impacto (ANCINE)

Assim, riscos considerados altos de uma metodologia (em vermelho na Figura 2), seriam compatíveis com os riscos considerados altos e extremos da outra (em vermelho e laranja na Figura 3), consequentemente formando o grupo que deverá sofrer tratamento para se adequar ao apetite de riscos institucional.

As tabelas seguintes mostram a descrição dos 14 riscos e sua avaliação conforme questionário disponibilizado pelo Ministério da Economia[3]. O detalhamento dos controles aplicados para cada um dos riscos que foram utilizados pela ferramenta para gradação da probabilidade e impacto estão no Anexo I.

[3] Disponível em: https://pesquisa.sisp.gov.br/index.php/468289?lang=pt-BR

Id	Risco referente ao tratamento de dados pessoais	Descrição
R01	**Acesso não autorizado**	Acesso indevido (permissões indevidas) a um ambiente físico ou lógico
R02	**Modificação não autorizada**	Usuário sem permissões de alteração para um determinado dado pessoal ou registro realiza a modificação não autorizada. Um processamento indevido pode gerar uma modificação não autorizada
R03	**Perda**	Perdas provocadas por ações intencionais de usuários oriundas de uma exclusão indevida ou devida e não comunicada, e provenientes de ações não intencionais como falhas em sistemas, sobrescrita de dados, falhas em hardware, entre outras
R04	**Roubo**	Dados roubados nas dependências interna do controlador/operador, falhas nos controles de segurança dos sistemas (a exemplo da ausência ou fraca criptografia, falha de sistema que permita escalação de privilégio ou tratamentos indevidos), entre outras
R05	**Remoção não autorizada**	Usuário não tem a permissão para retirar ou copiar dados pessoais para outro local
R06	**Coleção excessiva**	Coleta de dados pessoais em quantidade superior ao mínimo necessário à finalidade do tratamento ou atividade que fará uso do dado pessoal
R07	**Informação insuficiente sobre a finalidade do tratamento**	O tratamento de dados pessoais realizado de forma eletrônica ou documento em papel deve atender a uma finalidade e ser exposto de forma transparente e clara ao detentor dos dados pessoais
R08	**Tratamento sem consentimento do titular dos dados pessoais**	Controlador de dados pessoais não obtém consentimento do titular para realizar um tratamento de dados pessoais sem embasamento legal
R09	**Falha em considerar os direitos do titular dos dados pessoais**	Garantia de atendimento dos direitos do titular, conforme descrito nos artigos 17 a 23 da LGPD
R10	**Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais**	Instituição não atende sua finalidade legal e compartilha os dados sem consentimento do titular dos dados pessoais (LGPD, art. 27)
R11	**Retenção prolongada de dados pessoais sem necessidade**	O término da prestação de um serviço ou do prazo da retenção dos dados pessoais para fins legais deve culminar com a exclusão e/ou descarte seguro(a) dos dados pessoais
R12	**Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular**	A realização de operação de processamento de dados pessoais deve estar em conformidade com a LGPD. Qualquer operação de processamento que não atenda esse requisito pode produzir informações com vinculações ou associações indevidas
R13	**Falha/erro de processamento**	Dados de entrada que não são corretamente validados, operações de tratamento automatizadas de sistema que alteram de maneira indevida a composição do dado armazenado
R14	**Reidentificação de dados pseudonimizados**	Dados pessoais podem ser reidentificados por cruzamento simples de dados pessoais (LGPD, art. 12 e 13)

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado	Alta (15) (44%)	Alto (15) (54.35%)	Alto (225)
R02	Modificação não autorizada	Alta (15) (43.51%)	Alto (15) (49.21%)	Alto (225)
R03	Perda	Moderada (10) (51.02%)	Alto (15) (29.17%)	Alto (150)
R04	Roubo	Alta (15) (44.2%)	Alto (15) (34.65%)	Alto (225)
R05	Remoção não autorizada	Alta (15) (44.53%)	Alto (15) (49.23%)	Alto (225)
R06	Coleção excessiva	Alta (15) (22.22%)	Alto (15) (0%)	Alto (225)
R07	Informação insuficiente sobre a finalidade do tratamento	Alta (15) (13.04%)	Alto (15) (0%)	Alto (225)
R08	Tratamento sem consentimento do titular dos dados pessoais	Alta (15) (28.89%)	Alto (15) (38.46%)	Alto (225)
R09	Falha em considerar os direitos do titular dos dados pessoais	Alta (15) (24.59%)	Alto (15) (44%)	Alto (225)
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	Alta (15) (25.93%)	Alto (15) (0%)	Alto (225)
R11	Retenção prolongada de dados pessoais sem necessidade	Alta (15) (21.21%)	Alto (15) (0%)	Alto (225)
R12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular	Alta (15) (27.87%)	Alto (15) (25%)	Alto (225)
R13	Falha/erro de processamento	Alta (15) (26.67%)	Alto (15) (46.67%)	Alto (225)
R14	Reidentificação de dados pseudonimizados	Alta (15) (13.33%)	Alto (15) (0%)	Alto (225)

Legenda: P – Probabilidade (ISO/IEC 31000:2009, item 2.19); I – Impacto (ISO/IEC 31000:2009, item 2.18); Nível de Risco (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

Nas colunas P – Probabilidade e I – Impacto, estão descritas a escala resultante da avaliação dos controles implementados (Baixa – 5; Moderada – 10; Alta – 15) e o percentual de controles implementados, de acordo com o cálculo feito pela ferramenta. O produto destas duas dimensões, conforme a Figura 2, resulta no nível de risco final.

7 MEDIDAS PARA TRATAR RISCOS

Como demonstrado na seção anterior, todos os 14 riscos elencados tiveram seu nível avaliado como "Alto" a partir de uma avaliação inicial. Dessa forma, recomenda-se que todos estes riscos devam ser objeto de tratamento, identificando as medidas e controles que devem ser implementados para que o nível de risco residual possa estar adequado ao apetite de riscos organizacional.

Importante destacar que as medidas de tratamento, em geral, envolvem o aprimoramento da governança, dos processos e controles internos e de implementação de tecnologias e boas práticas de segurança, conforme as normas da ISO. Cada medida implementada melhora a segurança dos dados pessoais, favorecendo a prevenção ou a mitigação dos riscos, reduzindo sua probabilidade e/ou seu impacto para um nível de risco aceitável pela organização.

O acompanhamento das medidas mitigadoras e demais ações do PGP será realizada no âmbito do Comitê de Segurança de Informação e Comunicação – CSIC, ao passo que o monitoramento e a avaliação dos riscos descritos no RIPD serão realizados conforme a Política de Gestão de Riscos da ANCINE.

A partir da avaliação inicial realizada na seção anterior, foram identificados um conjunto de controles de segurança passíveis de serem implementados dentro do escopo do Programa de Governança de Privacidade – PGP. Assim, uma nova avaliação de riscos foi efetuada a partir do mesmo questionário, sendo verificado se no relatório final o novo nível de risco corresponde a um Risco Residual aceitável (Moderado ou Baixo) para cada um dos 14 riscos tratados. O detalhamento dos controles a serem implementados no escopo do PGP está no Anexo II.

Risco	Medida(s)	Efeito sobre o Risco[1]	Risco Residual[2]		
			P	I	Nível (P x I)
R01 - Acesso não autorizado	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Gestão de Riscos; Resposta a Incidente; Cópia de Segurança; Controles de Acesso; Registro de Eventos, Rastreabilidade e Salvaguarda de Logs; Desenvolvimento Seguro; Controles de Segurança em Redes, Proteção Física e do Ambiente; Legitimidade e Especificação de Propósito; Controles Criptográficos; Segurança Web; Controle de Acesso e Privacidade; Uso, Retenção e Limitação de Divulgação; Continuidade de Negócio	Reduzir	Baixa (05) (95.2%)	Moderado (10) (95.65%)	Baixo (50)
R02 - Modificação não autorizada	Responsabilização; Compliance com a Privacidade; Controles de Segurança em Redes, Proteção Física e do Ambiente; Gestão de Mudanças; Gestão de Riscos; Resposta a Incidente; Cópia de Segurança; Legitimidade e Especificação de Propósito; Controles de Acesso Lógico; Registro de Eventos, Rastreabilidade e Salvaguarda de Logs; Desenvolvimento Seguro; Controles Criptográficos; Segurança Web; Controle de Acesso e Privacidade; Continuidade de Negócio	Reduzir	Baixa (05) (94.66%)	Moderado (10) (90.48%)	Baixo (50)

R03 - Perda	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Gestão de Riscos; Resposta a Incidente; Cópia de Segurança; Legitimidade e Especificação de Propósito; Controles de Acesso Lógico; Desenvolvimento Seguro; Registro de Eventos, Rastreabilidade e Salvaguarda de Logs; Controles de Segurança em Redes, Proteção Física e do Ambiente; Controle de Acesso e Privacidade; Gestão de Capacidade e Redundância; Continuidade de Negócio; Controles Criptográficos; Segurança Web	Reduzir	Baixa (05) (93.88%)	Moderado (10) (93.75%)	Baixo (50)
R04 - Roubo	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Gestão de Riscos; Resposta a Incidente; Cópia de Segurança; Legitimidade e Especificação de Propósito; Controles Criptográficos; Controles de Acesso Lógico; Registro de Eventos, Rastreabilidade e Salvaguarda de Logs; Desenvolvimento Seguro; Segurança Web; Controles de Segurança em Redes, Proteção Física e do Ambiente; Controle de Acesso e Privacidade; Uso, Retenção e Limitação de Divulgação; Continuidade de Negócio	Reduzir	Baixa (05) (91.3%)	Moderado (10) (94.06%)	Baixo (50)
R05 - Remoção não autorizada	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Gestão de Riscos; Resposta a Incidente; Cópia de Segurança; Controles de Acesso Lógico; Registro de Eventos, Rastreabilidade e Salvaguarda de Logs; Legitimidade e Especificação de Propósito; Controles de Segurança em Redes, Proteção Física e do Ambiente; Desenvolvimento Seguro; Controles Criptográficos; Segurança Web; Controle de Acesso e Privacidade; Continuidade de Negócio	Reduzir	Baixa (05) (94.16%)	Moderado (10) (93.85%)	Baixo (50)
R06 - Coleção excessiva	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Limitação de Coleta; Abertura, Transparência e Notificação; Gestão de Riscos; Legitimidade e Especificação de Propósito	Reduzir	Baixa (05) (91.67%)	Alto (15) (83.33%)	Moderado (75)
R07 - Informação insuficiente sobre a finalidade do tratamento	Compliance com a Privacidade; Abertura, Transparência e Notificação; Responsabilização; Gestão de Mudanças; Gestão de Riscos; Legitimidade e Especificação de Propósito	Reduzir	Baixa (05) (95.65%)	Moderado (10) (100%)	Baixo (50)
R08 - Tratamento sem consentimento do titular dos dados pessoais	Compliance com a Privacidade; Registro de Eventos, Rastreabilidade e Salvaguarda de Logs; Abertura, Transparência e Notificação; Responsabilização; Legitimidade e Especificação de Propósito; Gestão de Mudanças; Desenvolvimento Seguro; Controles de Acesso Lógico	Reduzir	Baixa (05) (88.89%)	Alto (15) (84.62%)	Moderado (75)

R09 - Falha em considerar os direitos do titular dos dados pessoais	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Cópia de Segurança; Abertura, Transparência e Notificação; Legitimidade e Especificação de Propósito; Participação Individual e Acesso; Gestão de Riscos; Controles de Segurança em Redes, Proteção Física e do Ambiente; Desenvolvimento Seguro; Controles de Acesso Lógico; Segurança Web; Precisão e qualidade; Gestão de Capacidade e Redundância	Reduzir	Baixa (05) (96.72%)	Moderado (10) (96%)	Baixo (50)
R10 - Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Desenvolvimento Seguro; Legitimidade e Especificação de Propósito	Reduzir	Baixa (05) (92.59%)	Moderado (10) (100%)	Baixo (50)
R11 - Retenção prolongada de dados pessoais sem necessidade	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Abertura, Transparência e Notificação; Gestão de Capacidade e Redundância; Cópia de Segurança; Legitimidade e Especificação de Propósito	Reduzir	Baixa (05) (93.94%)	Alto (15) (80%)	Moderado (75)
R12 - Vinculação/ associação indevida, direta ou indireta, dos dados pessoais ao titular	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Registro de Eventos, Rastreabilidade e Salvaguarda de Logs; Limitação de Coleta; Abertura, Transparência e Notificação; Desenvolvimento Seguro; Legitimidade e Especificação de Propósito; Controles de Acesso Lógico; Controle de Acesso e Privacidade; Uso, Retenção e Limitação de Divulgação	Reduzir	Moderada (10) (81.97%)	Moderado (10) (85%)	Moderado (100)
R13 - Falha/erro de processamento	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Legitimidade e Especificação de Propósito; Cópia de Segurança; Abertura, Transparência e Notificação; Precisão e qualidade; Gestão de Capacidade e Redundância; Continuidade de Negócio	Reduzir	Baixa (05) (93.33%)	Moderado (10) (100%)	Baixo (50)
R14 - Reidentificação de dados pseudonimizados	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Desenvolvimento Seguro; Legitimidade e Especificação de Propósito	Reduzir	Moderada (10) (80%)	Moderado (10) (100%)	Moderado (100)

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6.

[1] Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.

[2] Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratar o risco.

8 ANEXO I – CONTROLES APLICADOS POR RISCO

Abaixo podem ser visualizados os 14 riscos e os controles a eles relacionados. Os controles são divididos em três categorias de atuação: Mitigação e Prevenção, apenas Prevenção ou apenas Mitigação perante um determinado risco.

R01 - Acesso não autorizado
Mitigação e Prevenção

16 - Existe um prazo formalmente definido para o tratamento de vulnerabilidades técnicas relevantes identificadas?
19 - Existe uma equipe de detecção, tratamento e resposta a incidentes de segurança cibernética (CSIRT)?
20 - Existe um canal apropriado para notificar os incidentes de segurança da informação de forma rápida?
22 - Os ativos de informação estão configurados de forma a registrar todos os eventos relevantes de segurança da informação, contendo, pelo menos, a identificação inequívoca do usuário, a natureza do evento, a data, hora e fuso horário, o identificador do ativo de informação, as coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento?
23 - Há um sistema para monitoramento de aplicações, alertas e vulnerabilidades utilizado para auxiliar na detecção e tratamento de incidentes de segurança cibernética (IPS, IDS, etc.)?
25 - Nos casos em que seja inviável preservar as mídias de armazenamento em razão da necessidade de pronto restabelecimento do serviço afetado, o agente responsável pelo CSIRT coleta e armazena cópia dos arquivos afetados pelo incidente, tais como: logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original, bem como os “metadados” desses arquivos, como data, hora de criação e permissões; registrando em relatório a impossibilidade de preservar as mídias afetadas e listando todos os procedimentos adotados?
27 - Há uma política ou norma de backup que aborde os procedimentos operacionais que padronizam os processos de geração de cópias de segurança e recuperação de arquivos, assim como os processos de controle de acesso, armazenamento, movimentação e descarte das mídias que contêm cópias de segurança?
57 - O log registra identificação do usuário, incluindo administrador e acessos privilegiados?
58 - O log registra endereço IP ou outro atributo que permita a identificação de onde o usuário efetuou o acesso?
59 - O log registra as ações executadas pelos usuários?
60 - O log registra data e hora do evento com alguma fonte de tempo sincronizada?
61 - Os logs gerados são protegidos, quando da geração, contra edição e exclusão?
62 - Os logs são protegidos contra o acesso indevido?

Prevenção

7 - O local que processa as informações é restrito somente ao pessoal autorizado?
8 - O trabalho nas áreas seguras é supervisionado?
9 - A rede corporativa é segmentada em domínios lógicos (limitando aos funcionários o acesso às redes e aos serviços de rede especificamente autorizados a usar), de acordo com cada rede local, atendendo às necessidades de fornecimento de serviço público e proteção da rede corporativa?
10 - O acesso externo aos sistemas é provido de meios de segurança que protegem a confidencialidade e integridade dos dados trafegados, tais como o uso de VPN?
12 - É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC?
13 - Mudanças são planejadas e testadas?
15 - As mudanças são comunicadas para todas as partes interessadas?
30 - As mídias que contêm cópias de segurança são armazenadas em uma localidade remota (“offsite”), a uma distância suficiente que garanta sua integridade e disponibilidade contra possíveis danos advindos de um desastre ocorrido no sítio primário?
32 - É exigida autorização prévia da autoridade competente para liberação das credenciais de acesso para o gerenciamento dos sistemas que suportam o serviço?
34 - As áreas de desenvolvimento, teste, homologação e produção são segregadas a fim de reduzir as possibilidades de modificação ou uso indevido dos recursos de processamento da informação, com controles de segurança adequados para cada ambiente?
35 - Em caso de desenvolvimento de sistemas de informação por terceiros, o proprietário do ativo da informação supervisiona o processo do planejamento até a implantação?
36 - Quando há a cópia dos dados de produção para os ambientes de desenvolvimento, teste e homologação, há autorização do proprietário do ativo de informação?
38 - Os recursos de segurança da informação e de tecnologia da informação encontram-se em versões seguras, estáveis e

atualizadas?
39 - O responsável pelo sistema acompanha junto aos fabricantes o período de obsolescência do produto, para evitar que os componentes se tornem expostos a vulnerabilidades sem correção?
48 - O sistema em análise segue uma política de senha com definição de tamanho mínimo e formato?
51 - Um mecanismo de recuperação de senha está implementado de forma a assegurar a recuperação da senha de maneira segura, sem fornecimento de senha por parte da aplicação, e que obrigue a alteração de senha do usuário no primeiro acesso?
55 - O sistema implementa restrições/limitadores para sucessivas tentativas de acesso mal sucedidas?
64 - Existem controles de versão para garantir a gestão dos códigos-fonte?
79 - A instituição controla por meio de um processo formal a concessão de direitos de acesso privilegiado para o processamento de dados?
80 - Os dados pessoais utilizados em ambiente de TDH (teste, desenvolvimento e homologação) passaram por um processo de anonimização?

Mitigação

28 - Está estabelecida a abrangência dos procedimentos de backup para cada tipo de informação (por exemplo, completa ou diferencial)?
46 - Existe uma frequência estabelecida para geração dos backups?
47 - É realizada cópias de segurança dos logs de acordo com períodos de retenção, que consideram os requisitos de negócio, contratuais, regulamentares ou legais?
49 - As informações das credenciais de acesso dos usuários estão gravadas em recursos de tecnologia da informação protegidos e sob a forma criptografada?

R02 - Modificação não autorizada

Mitigação e Prevenção

16 - Existe um prazo formalmente definido para o tratamento de vulnerabilidades técnicas relevantes identificadas?
19 - Existe uma equipe de detecção, tratamento e resposta a incidentes de segurança cibernética (CSIRT)?
20 - Existe um canal apropriado para notificar os incidentes de segurança da informação de forma rápida?
22 - Os ativos de informação estão configurados de forma a registrar todos os eventos relevantes de segurança da informação, contendo, pelo menos, a identificação inequívoca do usuário, a natureza do evento, a data, hora e fuso horário, o identificador do ativo de informação, as coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento?
23 - Há um sistema para monitoramento de aplicações, alertas e vulnerabilidades utilizado para auxiliar na detecção e tratamento de incidentes de segurança cibernética (IPS, IDS, etc.)?
25 - Nos casos em que seja inviável preservar as mídias de armazenamento em razão da necessidade de pronto restabelecimento do serviço afetado, o agente responsável pelo CSIRT coleta e armazena cópia dos arquivos afetados pelo incidente, tais como: logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original, bem como os “metadados” desses arquivos, como data, hora de criação e permissões; registrando em relatório a impossibilidade de preservar as mídias afetadas e listando todos os procedimentos adotados?
27 - Há uma política ou norma de backup que aborde os procedimentos operacionais que padronizam os processos de geração de cópias de segurança e recuperação de arquivos, assim como os processos de controle de acesso, armazenamento, movimentação e descarte das mídias que contêm cópias de segurança?
57 - O log registra identificação do usuário, incluindo administrador e acessos privilegiados?
58 - O log registra endereço IP ou outro atributo que permita a identificação de onde o usuário efetuou o acesso?
59 - O log registra as ações executadas pelos usuários?
60 - O log registra data e hora do evento com alguma fonte de tempo sincronizada?
61 - Os logs gerados são protegidos, quando da geração, contra edição e exclusão?
62 - Os logs são protegidos contra o acesso indevido?

Prevenção

7 - O local que processa as informações é restrito somente ao pessoal autorizado?
8 - O trabalho nas áreas seguras é supervisionado?

9 - A rede corporativa é segmentada em domínios lógicos (limitando aos funcionários o acesso às redes e aos serviços de rede especificamente autorizados a usar), de acordo com cada rede local, atendendo às necessidades de fornecimento de serviço público e proteção da rede corporativa?
10 - O acesso externo aos sistemas é provido de meios de segurança que protegem a confidencialidade e integridade dos dados trafegados, tais como o uso de VPN?
12 - É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC?
13 - Mudanças são planejadas e testadas?
15 - As mudanças são comunicadas para todas as partes interessadas?
30 - As mídias que contêm cópias de segurança são armazenadas em uma localidade remota (“offsite”), a uma distância suficiente que garanta sua integridade e disponibilidade contra possíveis danos advindos de um desastre ocorrido no sítio primário?
32 - É exigida autorização prévia da autoridade competente para liberação das credenciais de acesso para o gerenciamento dos sistemas que suportam o serviço?
34 - As áreas de desenvolvimento, teste, homologação e produção são segregadas a fim de reduzir as possibilidades de modificação ou uso indevido dos recursos de processamento da informação, com controles de segurança adequados para cada ambiente?
35 - Em caso de desenvolvimento de sistemas de informação por terceiros, o proprietário do ativo da informação supervisiona o processo do planejamento até a implantação?
36 - Quando há a cópia dos dados de produção para os ambientes de desenvolvimento, teste e homologação, há autorização do proprietário do ativo de informação?
38 - Os recursos de segurança da informação e de tecnologia da informação encontram-se em versões seguras, estáveis e atualizadas?
39 - O responsável pelo sistema acompanha junto aos fabricantes o período de obsolescência do produto, para evitar que os componentes se tornem expostos a vulnerabilidades sem correção?
48 - O sistema em análise segue uma política de senha com definição de tamanho mínimo e formato?
51 - Um mecanismo de recuperação de senha está implementado de forma a assegurar a recuperação da senha de maneira segura, sem fornecimento de senha por parte da aplicação, e que obrigue a alteração de senha do usuário no primeiro acesso?
55 - O sistema implementa restrições/limitadores para sucessivas tentativas de acesso mal sucedidas?
64 - Existem controles de versão para garantir a gestão dos códigos-fonte?
79 - A instituição controla por meio de um processo formal a concessão de direitos de acesso privilegiado para o processamento de dados?

Mitigação

28 - Está estabelecida a abrangência dos procedimentos de backup para cada tipo de informação (por exemplo, completa ou diferencial)?
46 - Existe uma frequência estabelecida para geração dos backups?
47 - É realizada cópias de segurança dos logs de acordo com períodos de retenção, que consideram os requisitos de negócio, contratuais, regulamentares ou legais?
49 - As informações das credenciais de acesso dos usuários estão gravadas em recursos de tecnologia da informação protegidos e sob a forma criptografada?

R03 - Perda

Mitigação e Prevenção

16 - Existe um prazo formalmente definido para o tratamento de vulnerabilidades técnicas relevantes identificadas?
19 - Existe uma equipe de detecção, tratamento e resposta a incidentes de segurança cibernética (CSIRT)?
20 - Existe um canal apropriado para notificar os incidentes de segurança da informação de forma rápida?
22 - Os ativos de informação estão configurados de forma a registrar todos os eventos relevantes de segurança da informação, contendo, pelo menos, a identificação inequívoca do usuário, a natureza do evento, a data, hora e fuso horário, o identificador do ativo de informação, as coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento?
23 - Há um sistema para monitoramento de aplicações, alertas e vulnerabilidades utilizado para auxiliar na detecção e tratamento de incidentes de segurança cibernética (IPS, IDS, etc.)?
25 - Nos casos em que seja inviável preservar as mídias de armazenamento em razão da necessidade de pronto restabelecimento do serviço afetado, o agente responsável pelo CSIRT coleta e armazena cópia dos arquivos afetados pelo incidente, tais como:

logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original, bem como os “metadados” desses arquivos, como data, hora de criação e permissões; registrando em relatório a impossibilidade de preservar as mídias afetadas e listando todos os procedimentos adotados?
27 - Há uma política ou norma de backup que aborde os procedimentos operacionais que padronizam os processos de geração de cópias de segurança e recuperação de arquivos, assim como os processos de controle de acesso, armazenamento, movimentação e descarte das mídias que contêm cópias de segurança?
64 - Existem controles de versão para garantir a gestão dos códigos-fonte?

Prevenção

7 - O local que processa as informações é restrito somente ao pessoal autorizado?
8 - O trabalho nas áreas seguras é supervisionado?
9 - A rede corporativa é segmentada em domínios lógicos (limitando aos funcionários o acesso às redes e aos serviços de rede especificamente autorizados a usar), de acordo com cada rede local, atendendo às necessidades de fornecimento de serviço público e proteção da rede corporativa?
10 - O acesso externo aos sistemas é provido de meios de segurança que protegem a confidencialidade e integridade dos dados trafegados, tais como o uso de VPN?
12 - É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC?
13 - Mudanças são planejadas e testadas?
15 - As mudanças são comunicadas para todas as partes interessadas?
30 - As mídias que contêm cópias de segurança são armazenadas em uma localidade remota (“offsite”), a uma distância suficiente que garanta sua integridade e disponibilidade contra possíveis danos advindos de um desastre ocorrido no sítio primário?
32 - É exigida autorização prévia da autoridade competente para liberação das credenciais de acesso para o gerenciamento dos sistemas que suportam o serviço?
34 - As áreas de desenvolvimento, teste, homologação e produção são segregadas a fim de reduzir as possibilidades de modificação ou uso indevido dos recursos de processamento da informação, com controles de segurança adequados para cada ambiente?
35 - Em caso de desenvolvimento de sistemas de informação por terceiros, o proprietário do ativo da informação supervisiona o processo do planejamento até a implantação?
36 - Quando há a cópia dos dados de produção para os ambientes de desenvolvimento, teste e homologação, há autorização do proprietário do ativo de informação?
38 - Os recursos de segurança da informação e de tecnologia da informação encontram-se em versões seguras, estáveis e atualizadas?
39 - O responsável pelo sistema acompanha junto aos fabricantes o período de obsolescência do produto, para evitar que os componentes se tornem expostos a vulnerabilidades sem correção?
48 - O sistema em análise segue uma política de senha com definição de tamanho mínimo e formato?
51 - Um mecanismo de recuperação de senha está implementado de forma a assegurar a recuperação da senha de maneira segura, sem fornecimento de senha por parte da aplicação, e que obrigue a alteração de senha do usuário no primeiro acesso?
55 - O sistema implementa restrições/limitadores para sucessivas tentativas de acesso mal sucedidas?
57 - O log registra identificação do usuário, incluindo administrador e acessos privilegiados?
58 - O log registra endereço IP ou outro atributo que permita a identificação de onde o usuário efetuou o acesso?
59 - O log registra as ações executadas pelos usuários?
60 - O log registra data e hora do evento com alguma fonte de tempo sincronizada?
61 - Os logs gerados são protegidos, quando da geração, contra edição e exclusão?
62 - Os logs são protegidos contra o acesso indevido?
79 - A instituição controla por meio de um processo formal a concessão de direitos de acesso privilegiado para o processamento de dados?

Mitigação

2 - Há mecanismos para monitoramento do uso dos recursos, de forma a atender as necessidades de capacidade futura e garantir o desempenho requerido das aplicações?
3 - São implementados mecanismos e procedimentos para mitigar ataques de negação de serviço, tais como balanceamento de carga, proxy, firewall, etc.?
28 - Está estabelecida a abrangência dos procedimentos de backup para cada tipo de informação (por exemplo, completa ou diferencial)?
40 - Há redundância dos recursos de processamento da informação suficiente para atender aos requisitos de disponibilidade previstos em contrato?

46 - Existe uma frequência estabelecida para geração dos backups?
47 - É realizada cópias de segurança dos logs de acordo com períodos de retenção, que consideram os requisitos de negócio, contratuais, regulamentares ou legais?
49 - As informações das credenciais de acesso dos usuários estão gravadas em recursos de tecnologia da informação protegidos e sob a forma criptografada?

R04 - Roubo

Mitigação e Prevenção

16 - Existe um prazo formalmente definido para o tratamento de vulnerabilidades técnicas relevantes identificadas?
19 - Existe uma equipe de detecção, tratamento e resposta a incidentes de segurança cibernética (CSIRT)?
20 - Existe um canal apropriado para notificar os incidentes de segurança da informação de forma rápida?
22 - Os ativos de informação estão configurados de forma a registrar todos os eventos relevantes de segurança da informação, contendo, pelo menos, a identificação inequívoca do usuário, a natureza do evento, a data, hora e fuso horário, o identificador do ativo de informação, as coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento?
23 - Há um sistema para monitoramento de aplicações, alertas e vulnerabilidades utilizado para auxiliar na detecção e tratamento de incidentes de segurança cibernética (IPS, IDS, etc.)?
25 - Nos casos em que seja inviável preservar as mídias de armazenamento em razão da necessidade de pronto restabelecimento do serviço afetado, o agente responsável pelo CSIRT coleta e armazena cópia dos arquivos afetados pelo incidente, tais como: logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original, bem como os “metadados” desses arquivos, como data, hora de criação e permissões; registrando em relatório a impossibilidade de preservar as mídias afetadas e listando todos os procedimentos adotados?
27 - Há uma política ou norma de backup que aborde os procedimentos operacionais que padronizam os processos de geração de cópias de segurança e recuperação de arquivos, assim como os processos de controle de acesso, armazenamento, movimentação e descarte das mídias que contêm cópias de segurança?
57 - O log registra identificação do usuário, incluindo administrador e acessos privilegiados?
58 - O log registra endereço IP ou outro atributo que permita a identificação de onde o usuário efetuou o acesso?
59 - O log registra as ações executadas pelos usuários?
60 - O log registra data e hora do evento com alguma fonte de tempo sincronizada?
61 - Os logs gerados são protegidos, quando da geração, contra edição e exclusão?
62 - Os logs são protegidos contra o acesso indevido?
64 - Existem controles de versão para garantir a gestão dos códigos-fonte?

Prevenção

7 - O local que processa as informações é restrito somente ao pessoal autorizado?
8 - O trabalho nas áreas seguras é supervisionado?
9 - A rede corporativa é segmentada em domínios lógicos (limitando aos funcionários o acesso às redes e aos serviços de rede especificamente autorizados a usar), de acordo com cada rede local, atendendo às necessidades de fornecimento de serviço público e proteção da rede corporativa?
10 - O acesso externo aos sistemas é provido de meios de segurança que protegem a confidencialidade e integridade dos dados trafegados, tais como o uso de VPN?
12 - É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC?
13 - Mudanças são planejadas e testadas?
15 - As mudanças são comunicadas para todas as partes interessadas?
30 - As mídias que contêm cópias de segurança são armazenadas em uma localidade remota (“offsite”), a uma distância suficiente que garanta sua integridade e disponibilidade contra possíveis danos advindos de um desastre ocorrido no sítio primário?
32 - É exigida autorização prévia da autoridade competente para liberação das credenciais de acesso para o gerenciamento dos sistemas que suportam o serviço?
34 - As áreas de desenvolvimento, teste, homologação e produção são segregadas a fim de reduzir as possibilidades de modificação ou uso indevido dos recursos de processamento da informação, com controles de segurança adequados para cada ambiente?
35 - Em caso de desenvolvimento de sistemas de informação por terceiros, o proprietário do ativo da informação supervisiona o

processo do planejamento até a implantação?
36 - Quando há a cópia dos dados de produção para os ambientes de desenvolvimento, teste e homologação, há autorização do proprietário do ativo de informação?
38 - Os recursos de segurança da informação e de tecnologia da informação encontram-se em versões seguras, estáveis e atualizadas?
39 - O responsável pelo sistema acompanha junto aos fabricantes o período de obsolescência do produto, para evitar que os componentes se tornem expostos a vulnerabilidades sem correção?
48 - O sistema em análise segue uma política de senha com definição de tamanho mínimo e formato?
51 - Um mecanismo de recuperação de senha está implementado de forma a assegurar a recuperação da senha de maneira segura, sem fornecimento de senha por parte da aplicação, e que obrigue a alteração de senha do usuário no primeiro acesso?
55 - O sistema implementa restrições/limitadores para sucessivas tentativas de acesso mal sucedidas?
79 - A instituição controla por meio de um processo formal a concessão de direitos de acesso privilegiado para o processamento de dados?

Mitigação

28 - Está estabelecida a abrangência dos procedimentos de backup para cada tipo de informação (por exemplo, completa ou diferencial)?
46 - Existe uma frequência estabelecida para geração dos backups?
47 - É realizada cópias de segurança dos logs de acordo com períodos de retenção, que consideram os requisitos de negócio, contratuais, regulamentares ou legais?
49 - As informações das credenciais de acesso dos usuários estão gravadas em recursos de tecnologia da informação protegidos e sob a forma criptografada?
80 - Os dados pessoais utilizados em ambiente de TDH (teste, desenvolvimento e homologação) passaram por um processo de anonimização?

R05 - Remoção não autorizada

Mitigação e Prevenção

16 - Existe um prazo formalmente definido para o tratamento de vulnerabilidades técnicas relevantes identificadas?
19 - Existe uma equipe de detecção, tratamento e resposta a incidentes de segurança cibernética (CSIRT)?
20 - Existe um canal apropriado para notificar os incidentes de segurança da informação de forma rápida?
22 - Os ativos de informação estão configurados de forma a registrar todos os eventos relevantes de segurança da informação, contendo, pelo menos, a identificação inequívoca do usuário, a natureza do evento, a data, hora e fuso horário, o identificador do ativo de informação, as coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento?
23 - Há um sistema para monitoramento de aplicações, alertas e vulnerabilidades utilizado para auxiliar na detecção e tratamento de incidentes de segurança cibernética (IPS, IDS, etc.)?
25 - Nos casos em que seja inviável preservar as mídias de armazenamento em razão da necessidade de pronto restabelecimento do serviço afetado, o agente responsável pelo CSIRT coleta e armazena cópia dos arquivos afetados pelo incidente, tais como: logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original, bem como os “metadados” desses arquivos, como data, hora de criação e permissões; registrando em relatório a impossibilidade de preservar as mídias afetadas e listando todos os procedimentos adotados?
27 - Há uma política ou norma de backup que aborde os procedimentos operacionais que padronizam os processos de geração de cópias de segurança e recuperação de arquivos, assim como os processos de controle de acesso, armazenamento, movimentação e descarte das mídias que contêm cópias de segurança?
57 - O log registra identificação do usuário, incluindo administrador e acessos privilegiados?
58 - O log registra endereço IP ou outro atributo que permita a identificação de onde o usuário efetuou o acesso?
59 - O log registra as ações executadas pelos usuários?
60 - O log registra data e hora do evento com alguma fonte de tempo sincronizada?
61 - Os logs gerados são protegidos, quando da geração, contra edição e exclusão?
62 - Os logs são protegidos contra o acesso indevido?

Prevenção

7 - O local que processa as informações é restrito somente ao pessoal autorizado?
8 - O trabalho nas áreas seguras é supervisionado?
9 - A rede corporativa é segmentada em domínios lógicos (limitando aos funcionários o acesso às redes e aos serviços de rede especificamente autorizados a usar), de acordo com cada rede local, atendendo às necessidades de fornecimento de serviço público e proteção da rede corporativa?
10 - O acesso externo aos sistemas é provido de meios de segurança que protegem a confidencialidade e integridade dos dados trafegados, tais como o uso de VPN?
12 - É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC?
13 - Mudanças são planejadas e testadas?
15 - As mudanças são comunicadas para todas as partes interessadas?
30 - As mídias que contêm cópias de segurança são armazenadas em uma localidade remota (“offsite”), a uma distância suficiente que garanta sua integridade e disponibilidade contra possíveis danos advindos de um desastre ocorrido no sítio primário?
32 - É exigida autorização prévia da autoridade competente para liberação das credenciais de acesso para o gerenciamento dos sistemas que suportam o serviço?
34 - As áreas de desenvolvimento, teste, homologação e produção são segregadas a fim de reduzir as possibilidades de modificação ou uso indevido dos recursos de processamento da informação, com controles de segurança adequados para cada ambiente?
35 - Em caso de desenvolvimento de sistemas de informação por terceiros, o proprietário do ativo da informação supervisiona o processo do planejamento até a implantação?
36 - Quando há a cópia dos dados de produção para os ambientes de desenvolvimento, teste e homologação, há autorização do proprietário do ativo de informação?
38 - Os recursos de segurança da informação e de tecnologia da informação encontram-se em versões seguras, estáveis e atualizadas?
39 - O responsável pelo sistema acompanha junto aos fabricantes o período de obsolescência do produto, para evitar que os componentes se tornem expostos a vulnerabilidades sem correção?
48 - O sistema em análise segue uma política de senha com definição de tamanho mínimo e formato?
51 - Um mecanismo de recuperação de senha está implementado de forma a assegurar a recuperação da senha de maneira segura, sem fornecimento de senha por parte da aplicação, e que obrigue a alteração de senha do usuário no primeiro acesso?
55 - O sistema implementa restrições/limitadores para sucessivas tentativas de acesso mal sucedidas?
64 - Existem controles de versão para garantir a gestão dos códigos-fonte?
79 - A instituição controla por meio de um processo formal a concessão de direitos de acesso privilegiado para o processamento de dados?

Mitigação

28 - Está estabelecida a abrangência dos procedimentos de backup para cada tipo de informação (por exemplo, completa ou diferencial)?
46 - Existe uma frequência estabelecida para geração dos backups?
47 - É realizada cópias de segurança dos logs de acordo com períodos de retenção, que consideram os requisitos de negócio, contratuais, regulamentares ou legais?
49 - As informações das credenciais de acesso dos usuários estão gravadas em recursos de tecnologia da informação protegidos e sob a forma criptografada?

R06 - Coleção Excessiva

Prevenção

12 - É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC?
13 - Mudanças são planejadas e testadas?
15 - As mudanças são comunicadas para todas as partes interessadas?
96 - O tratamento de dados pessoais é 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 (embasamento legal)?

R07 - Informação insuficiente sobre a finalidade do tratamento
Prevenção

12 - É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC?
13 - Mudanças são planejadas e testadas?
15 - As mudanças são comunicadas para todas as partes interessadas?

R08 - Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente)
Mitigação e Prevenção

57 - O log registra identificação do usuário, incluindo administrador e acessos privilegiados?
58 - O log registra endereço IP ou outro atributo que permita a identificação de onde o usuário efetuou o acesso?
59 - O log registra as ações executadas pelos usuários?
60 - O log registra data e hora do evento com alguma fonte de tempo sincronizada?

Prevenção

6 - Os dados pessoais encontram-se classificados em sensíveis e não sensíveis, incluindo categorias de informações pessoais de saúde, informações pessoais financeiras, entre outras?
12 - É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC?
13 - Mudanças são planejadas e testadas?
15 - As mudanças são comunicadas para todas as partes interessadas?
36 - Quando há a cópia dos dados de produção para os ambientes de desenvolvimento, teste e homologação, há autorização do proprietário do ativo de informação?

R09 - Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso)
Mitigação e Prevenção

27 - Há uma política ou norma de backup que aborde os procedimentos operacionais que padronizam os processos de geração de cópias de segurança e recuperação de arquivos, assim como os processos de controle de acesso, armazenamento, movimentação e descarte das mídias que contêm cópias de segurança?
112 - A instituição permite aos titulares dos dados pessoais, quando permitido pela legislação aplicável, a capacidade de acessar e revisar seus dados pessoais para elevar a integridade e precisão das informações?
113 - Há um canal de comunicação ativo, seguro e autenticado para o recebimento de reclamações e manter um ponto de contato para receber e responder a reclamações, preocupações ou perguntas dos titulares sobre o tratamento de dados pessoais realizados pela instituição?

Prevenção

6 - Os dados pessoais encontram-se classificados em sensíveis e não sensíveis, incluindo categorias de informações pessoais de saúde, informações pessoais financeiras, entre outras?
7 - O local que processa as informações é restrito somente ao pessoal autorizado? 8 - O trabalho nas áreas seguras é supervisionado?
8 - O trabalho nas áreas seguras é supervisionado?
12 - É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC?
13 - Mudanças são planejadas e testadas?
15 - As mudanças são comunicadas para todas as partes interessadas?
30 - As mídias que contêm cópias de segurança são armazenadas em uma localidade remota (“offsite”), a uma distância suficiente que garanta sua integridade e disponibilidade contra possíveis danos advindos de um desastre ocorrido no sítio primário?
51 - Um mecanismo de recuperação de senha está implementado de forma a assegurar a recuperação da senha de maneira segura, sem fornecimento de senha por parte da aplicação, e que obrigue a alteração de senha do usuário no primeiro acesso?

96 - O tratamento de dados pessoais é 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 (embasamento legal)?

Mitigação

28 - Está estabelecida a abrangência dos procedimentos de backup para cada tipo de informação (por exemplo, completa ou diferencial)?
40 - Há redundância dos recursos de processamento da informação suficiente para atender aos requisitos de disponibilidade previstos em contrato?
46 - Existe uma frequência estabelecida para geração dos backups?
49 - As informações das credenciais de acesso dos usuários estão gravadas em recursos de tecnologia da informação protegidos e sob a forma criptografada?

R10 - Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais

Prevenção

12 - É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC?
13 - Mudanças são planejadas e testadas?
15 - As mudanças são comunicadas para todas as partes interessadas?
36 - Quando há a cópia dos dados de produção para os ambientes de desenvolvimento, teste e homologação, há autorização do proprietário do ativo de informação?

R11 - Retenção prolongada de dados pessoais sem necessidade

Prevenção

12 - É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC?
13 - Mudanças são planejadas e testadas?
15 - As mudanças são comunicadas para todas as partes interessadas?
27 - Há uma política ou norma de backup que aborde os procedimentos operacionais que padronizam os processos de geração de cópias de segurança e recuperação de arquivos, assim como os processos de controle de acesso, armazenamento, movimentação e descarte das mídias que contêm cópias de segurança?
28 - Está estabelecida a abrangência dos procedimentos de backup para cada tipo de informação (por exemplo, completa ou diferencial)?
46 - Existe uma frequência estabelecida para geração dos backups?

R12 - Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular

Mitigação e Prevenção

57 - O log registra identificação do usuário, incluindo administrador e acessos privilegiados?
58 - O log registra endereço IP ou outro atributo que permita a identificação de onde o usuário efetuou o acesso?
59 - O log registra as ações executadas pelos usuários?
60 - O log registra data e hora do evento com alguma fonte de tempo sincronizada?

Prevenção

6 - Os dados pessoais encontram-se classificados em sensíveis e não sensíveis, incluindo categorias de informações pessoais de saúde, informações pessoais financeiras, entre outras?

12 - É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC?
13 - Mudanças são planejadas e testadas?
15 - As mudanças são comunicadas para todas as partes interessadas?
36 - Quando há a cópia dos dados de produção para os ambientes de desenvolvimento, teste e homologação, há autorização do proprietário do ativo de informação?
80 - Os dados pessoais utilizados em ambiente de TDH (teste, desenvolvimento e homologação) passaram por um processo de anonimização?
96 - O tratamento de dados pessoais é 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 (embasamento legal)?

R13 - Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada, etc.)

Mitigação e Prevenção

27 - Há uma política ou norma de backup que aborde os procedimentos operacionais que padronizam os processos de geração de cópias de segurança e recuperação de arquivos, assim como os processos de controle de acesso, armazenamento, movimentação e descarte das mídias que contêm cópias de segurança?

Prevenção

6 - Os dados pessoais encontram-se classificados em sensíveis e não sensíveis, incluindo categorias de informações pessoais de saúde, informações pessoais financeiras, entre outras?
12 - É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC?
13 - Mudanças são planejadas e testadas?
15 - As mudanças são comunicadas para todas as partes interessadas?

Mitigação

2 - Há mecanismos para monitoramento do uso dos recursos, de forma a atender as necessidades de capacidade futura e garantir o desempenho requerido das aplicações?
3 - São implementados mecanismos e procedimentos para mitigar ataques de negação de serviço, tais como balanceamento de carga, proxy, firewall, etc.?
28 - Está estabelecida a abrangência dos procedimentos de backup para cada tipo de informação (por exemplo, completa ou diferencial)?
46 - Existe uma frequência estabelecida para geração dos backups?

R14 - Reidentificação de dados pseudonimizados

Prevenção

12 - É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC?
13 - Mudanças são planejadas e testadas?
15 - As mudanças são comunicadas para todas as partes interessadas?

9 ANEXO II – CONTROLES A SEREM APLICADOS PARA MITIGAÇÃO DOS RISCOS

Controle a ser aplicado para mitigação	Riscos associados
1 - Há uma matriz de responsabilidades com atribuição das responsabilidades pela segurança da informação na organização, pela proteção de dados (encarregado), identificação dos gestores de serviços com dados pessoais, operadores de tratamento de dados, de forma a evidenciar a segregação de funções e assegurar que colaboradores e partes externas entendam suas responsabilidades?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R06 - Coleção Excessiva; R07 - Informação insuficiente; R08 - Tratamento sem consentimento; R09 - Falha em considerar os direitos do titular; R10 - Compartilhar ou distribuir dados pessoais com terceiros; R11 - Retenção prolongada; R12 - Vinculação ou associação indevida; R13 - Falha ou erro de processamento; R14 - Reidentificação de dados
4 - Existe um Plano de Continuidade de Negócio, que garanta o nível adequado de continuidade para a segurança da informação durante uma situação adversa?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R09 - Falha em considerar os direitos do titular
5 - A Política de Segurança da Informação já foi revisada para se adequar a medidas que objetivem a proteção de dados pessoais?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R06 - Coleção Excessiva; R07 - Informação insuficiente; R08 - Tratamento sem consentimento; R09 - Falha em considerar os direitos do titular; R10 - Compartilhar ou distribuir dados pessoais com terceiros; R11 - Retenção prolongada; R12 - Vinculação ou associação indevida; R13 - Falha ou erro de processamento; R14 - Reidentificação de dados
11 - Existem e são executados processos periódicos de cópias de segurança das configurações e sistemas operacionais dos switches e roteadores?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada;
14 - Há uma avaliação de impactos potenciais, riscos e consequências, incluindo impactos de segurança cibernética, quando da identificação de necessidade de mudanças?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R06 - Coleção Excessiva; R07 - Informação insuficiente; R08 - Tratamento sem consentimento; R09 - Falha em considerar os direitos do titular; R10 - Compartilhar ou distribuir dados pessoais com terceiros; R11 - Retenção prolongada; R12 - Vinculação ou associação indevida; R13 - Falha ou erro de processamento; R14 - Reidentificação de dados
17 - Há um inventário completo e atualizado dos ativos de informação, contendo o fornecedor, o número da versão, os dados pessoais processados, a classificação dos dados pessoais (sensíveis ou apenas dados pessoais), quais softwares estão instalados e em quais sistemas, e a(s) pessoa(s) na organização responsável(s) pelos ativos?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R05 - Remoção não autorizada; R06 - Coleção Excessiva; R07 - Informação insuficiente; R09 - Falha em considerar os direitos do titular; R11 - Retenção prolongada;
18 - Há um processo de análise e monitoramento de vulnerabilidades?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada;
21 - Existem formalmente e são executados procedimentos específicos para resposta aos incidentes, contemplando: a definição de incidente; o escopo da resposta; quando e por quem as autoridades devem ser contatadas; papéis, responsabilidades e autoridades; avaliação de impacto do incidente; medidas para reduzir a probabilidade e mitigar o impacto do incidente; descrição da natureza dos dados pessoais afetados; as informações sobre os titulares de dados pessoais envolvidos; procedimentos para determinar se um aviso para indivíduos afetados e outras entidades designadas (por exemplo, órgãos reguladores) é necessário?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada;
24 - O plano de comunicação foi atualizado para incluir os contatos que devem ser notificados, caso haja uma violação de privacidade, ou para reportar detalhes de processamento, como contatos com a autoridade de proteção de dados e/ou grupos diretamente relacionados?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada;

26 - Os arquivos coletados como evidências são gravados em conjunto com o arquivo com a lista dos resumos criptográficos?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada;
29 - É definido a abrangência dos testes de backup e sua periodicidade, de forma que os testes sejam planejados observando as dependências e relacionamentos entre sistemas, considerando inclusive os ambientes de continuidade de negócios, com o objetivo de minimizar a possibilidade de que a ausência de sincronismo entre os dados inviabilize ou dificulte sua recuperação?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R09 - Falha em considerar os direitos do titular; R13 - Falha ou erro de processamento
31 - O período de retenção das cópias de segurança e os requisitos de releitura são predefinidos, levando-se em consideração os requisitos de negócio, contratuais, regulamentares ou legais?	R03 - Perda; R04 – Roubo; R09 - Falha em considerar os direitos do titular; R11 - Retenção prolongada; R13 - Falha ou erro de processamento
33- Existe e é executado um processo formal de desenvolvimento de sistema seguro?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R09 - Falha em considerar os direitos do titular
37-É realizada periodicamente uma análise/avaliação de riscos da arquitetura da Solução de TIC, indicando os eventos de risco e seus respectivos níveis de risco ao qual o sistema está exposto, baseada em prévia análise de vulnerabilidades dos ativos que compõem a Solução de TIC?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada;
41- Foi elaborada uma política de privacidade para o serviço?	R06 - Coleção Excessiva; R07 - Informação insuficiente; R08 - Tratamento sem consentimento; R09 - Falha em considerar os direitos do titular; R11 - Retenção prolongada; R12 - Vinculação ou associação indevida;
42- Existe Relatório de Impacto à Proteção de Dados Pessoais, conforme previsto na Lei 13.709 de 14 de agosto de 2018, relacionado à solução de TIC?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R06 - Coleção Excessiva; R07 - Informação insuficiente; R08 - Tratamento sem consentimento; R09 - Falha em considerar os direitos do titular; R10 - Compartilhar ou distribuir dados pessoais com terceiros; R11 - Retenção prolongada; R12 - Vinculação ou associação indevida; R13 - Falha ou erro de processamento; R14 - Reidentificação de dados
43- Há um inventário completo e atualizado dos dados pessoais, contendo os agentes de tratamento (controlador e operador), encarregado, descrição do fluxo de tratamento dos dados pessoais (como são coletados, armazenados, processados, retidos e eliminados), abrangência da área geográfica do tratamento (nacional, estadual, municipal), finalidade do tratamento dos dados pessoais, categoria dos dados pessoais (identificação pessoal, financeiros, características pessoais, outros), categoria de dados sensíveis, dados pessoais compartilhados e transferência internacional?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R06 - Coleção Excessiva; R07 - Informação insuficiente; R08 - Tratamento sem consentimento; R09 - Falha em considerar os direitos do titular; R10 - Compartilhar ou distribuir dados pessoais com terceiros; R11 - Retenção prolongada; R12 - Vinculação ou associação indevida; R13 - Falha ou erro de processamento; R14 - Reidentificação de dados
44- São realizados, em intervalos de tempo predefinidos, simulações e/ou testes planejados, levando-se em consideração as menores indisponibilidades e impactos possíveis nos processos de negócio, de forma que seja possível identificar falhas que venham a comprometer qualquer parte do processo de continuidade, com vistas a promover revisões e atualizações periódicas dos Planos relacionados?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R09 - Falha em considerar os direitos do titular
52- Uma análise crítica de direitos de acesso é realizada em um período de tempo previamente definido ou a qualquer momento depois de qualquer mudança nos direitos de usuários ou para verificação de incidentes de segurança?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada;
53- Há mecanismos para encerramento (expirar) de qualquer sessão cuja inatividade do usuário exceda um período de tempo predeterminado?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R08 - Tratamento sem consentimento; R09 - Falha em considerar os direitos do titular; R12 - Vinculação ou associação indevida;

54- Existem restrições de autenticação do usuário para acesso simultâneo a serviço(s), sistema(s) e/ou rede(s)?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R08 - Tratamento sem consentimento; R09 - Falha em considerar os direitos do titular; R12 - Vinculação ou associação indevida;
56- As credenciais de acesso e logs são armazenadas separadamente dos dados das aplicações e dos sistemas?	R01 – Acesso Não Autorizado; R03 - Perda; R04 – Roubo;
63- Requisitos de segurança são identificados e considerados em todas as fases do projeto do sistema?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada;
66- É realizada análise estática e/ou análise dinâmica dos requisitos de segurança cibernética do sistema?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R09 - Falha em considerar os direitos do titular
68- O servidor da aplicação tem configurado o cabeçalho HTTP com X-XSS-Protection para evitar que usuários de navegadores antigos sejam vulneráveis a ataques de Cross-site Scripting (XSS)?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R09 - Falha em considerar os direitos do titular
69- O servidor da aplicação tem configurado o cabeçalho HTTP com X-Frame-Options para evitar que usuários caiam em ataques de clickjacking?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R09 - Falha em considerar os direitos do titular
70- O servidor da aplicação tem configurado o cabeçalho HTTP com HTTP Strict-Transport-Security (HSTS) para garantir que todo o tráfego de dados ocorra criptografado?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R09 - Falha em considerar os direitos do titular
71- O servidor da aplicação implementa políticas (Content Security Policy (CSP)) que validam a renderização da página e protegem contra ataques de injeção de conteúdo como Cross-Site Scripting (XSS)?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R09 - Falha em considerar os direitos do titular
72- O servidor da aplicação implementa o X-Content-Type-Options para evitar que navegadores como Internet Explorer e Chrome interpretem o conteúdo da página e execute o dado como código?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R09 - Falha em considerar os direitos do titular
73 - Os cookies da aplicação são enviados para o usuário apenas através de conexões criptografadas (flag SECURE)?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R09 - Falha em considerar os direitos do titular
74 - A aplicação está configurada para que os cookies não possam ser acessíveis via comando JavaScript, evitando assim ataques cross-site scripting (XSS) (flag HTTPOnly)?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R09 - Falha em considerar os direitos do titular
75 - O servidor da aplicação está configurado com o cabeçalho Subresource Integrity (SRI) para proteger contra invasores que modifiquem o conteúdo de bibliotecas JavaScript hospedadas em redes de entrega de conteúdo (CDNs)?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R09 - Falha em considerar os direitos do titular
76 - As permissões de acesso (incluir, consultar, alterar, excluir) dos usuários que executam a operação de processamento de dados pessoais se limitam ao mínimo necessário para realizar o processamento?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R12 - Vinculação ou associação indevida;
77 - O acesso para realizar as operações de tratamento de dados pessoais é provido ao número mínimo de indivíduos necessários para executar as operações de tratamento?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R12 - Vinculação ou associação indevida;
82 - Ao fornecer a base de informações para órgãos de pesquisa, os dados pessoais são anonimizados ou pseudoanonimizados?	R12 - Vinculação ou associação indevida;
83 - O compartilhamento ou transferência de dados pessoais é realizado por meio de um canal criptografado e de cifra recomendada pelos sítios especializados de segurança (Exemplo: https://www.ssllabs.com/ssltest/)?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada;
85 - Acordos de confidencialidade, termos de responsabilidade, termos de sigilo são assinados com os órgãos e operadores de dados pessoais? É	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 -

importante que os termos e acordos informem a respeito dos itens a seguir, mas a eles não se limitem: tipos de tratamento de dados pessoais a serem realizados por quem irá receber os dados; ações requeridas quando do encerramento do compartilhamento, como destruição dos dados, responsabilidade e ações dos signatários para evitar a divulgação não autorizada dos dados pessoais; base legal para o compartilhamento; direito de auditar e monitorar as atividades que envolvem os dados pessoais; processo para notificar ou relatar vazamentos; violações ou divulgações não autorizadas dos dados pessoais; ações a serem tomadas diante da violação do acordo; e outras medidas possíveis.	Remoção não autorizada; R08 - Tratamento sem consentimento; R09 - Falha em considerar os direitos do titular; R10 - Compartilhar ou distribuir dados pessoais com terceiros;
88 - O desenvolvimento dos sistemas tem como base os riscos e as medidas de segurança identificadas no RIPD (Relatório de Impacto de Proteção à Dados Pessoais)?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R06 - Coleção Excessiva; R07 - Informação insuficiente; R08 - Tratamento sem consentimento; R09 - Falha em considerar os direitos do titular; R10 - Compartilhar ou distribuir dados pessoais com terceiros; R11 - Retenção prolongada; R12 - Vinculação ou associação indevida; R13 - Falha ou erro de processamento; R14 - Reidentificação de dados
89 - O desenvolvimento dos sistemas é orientado à proteção da privacidade dos dados pessoais (Privacy by Design)?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R06 - Coleção Excessiva; R07 - Informação insuficiente; R08 - Tratamento sem consentimento; R09 - Falha em considerar os direitos do titular; R10 - Compartilhar ou distribuir dados pessoais com terceiros; R11 - Retenção prolongada; R12 - Vinculação ou associação indevida; R13 - Falha ou erro de processamento; R14 - Reidentificação de dados
91 - Há uma política ou norma de proteção de dados pessoais que aborde a finalidade da instituição perante o processamento de dados; a transparência com relação à coleta e processamento de dados pessoais; a estrutura estabelecida para a proteção de dados pessoais; regras para tomar decisões em questões de proteção de dados pessoais; critérios de aceitação de risco de privacidade; compromisso de satisfazer os requisitos aplicáveis de proteção à privacidade?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R06 - Coleção Excessiva; R07 - Informação insuficiente; R08 - Tratamento sem consentimento; R09 - Falha em considerar os direitos do titular; R10 - Compartilhar ou distribuir dados pessoais com terceiros; R11 - Retenção prolongada; R12 - Vinculação ou associação indevida; R13 - Falha ou erro de processamento; R14 - Reidentificação de dados
93 - É implementada e mantida uma estratégia abrangente de treinamento e conscientização, destinada a garantir que os envolvidos entendam suas responsabilidades e os procedimentos de proteção de dados pessoais?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R06 - Coleção Excessiva; R07 - Informação insuficiente; R08 - Tratamento sem consentimento; R09 - Falha em considerar os direitos do titular; R10 - Compartilhar ou distribuir dados pessoais com terceiros; R11 - Retenção prolongada; R12 - Vinculação ou associação indevida; R13 - Falha ou erro de processamento; R14 - Reidentificação de dados
94 - A instituição monitora continuamente as ações de proteção de dados pessoais, a fim de 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?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R06 - Coleção Excessiva; R07 - Informação insuficiente; R08 - Tratamento sem consentimento; R09 - Falha em considerar os direitos do titular; R10 - Compartilhar ou distribuir dados pessoais com terceiros; R11 - Retenção prolongada; R12 - Vinculação ou associação indevida; R13 - Falha ou erro de processamento; R14 - Reidentificação de dados
98 - Os dados coletados limitam-se ao mínimo necessário para atendimento da finalidade do tratamento?	R06 - Coleção Excessiva; R12 - Vinculação ou associação indevida;

99 - É realizada uma análise periódica sobre os dados coletados, se eles continuam limitados ao mínimo necessário para o atendimento a finalidade?	R06 - Coleção Excessiva; R12 - Vinculação ou associação indevida;
100 - A finalidade do tratamento é comunicada ao titular dos dados pessoais, mesmo no caso de execução de políticas públicas e competência legal, antes que as informações sejam coletadas ou usadas?	R06 - Coleção Excessiva; R07 - Informação insuficiente; R08 - Tratamento sem consentimento; R09 - Falha em considerar os direitos do titular; R11 - Retenção prolongada; R12 - Vinculação ou associação indevida;
103 - Os titulares de dados pessoais são notificados de alterações na forma de tratamento de dados?	R07 - Informação insuficiente; R13 - Falha ou erro de processamento
104 - São fornecidas aos titulares de dados pessoais informações claras e facilmente acessíveis sobre as políticas, procedimentos, práticas do controlador de dados pessoais em relação ao manuseio de dados pessoais (dados coletados, processamento efetuado, finalidade a ser alcançada com o processamento, com quem compartilha e a finalidade, capacidade de consentir compartilhamento específicos), como os dados são protegidos, dados de comunicação com o encarregado, entre outras informações de importância a transparência e publicidade?	R06 - Coleção Excessiva; R07 - Informação insuficiente; R08 - Tratamento sem consentimento; R09 - Falha em considerar os direitos do titular; R11 - Retenção prolongada; R12 - Vinculação ou associação indevida;
107 - A instituição revisa periodicamente as medidas de segurança aplicadas nos ativos que realizam o tratamento de dados pessoais (coleta, retenção, processamento, compartilhamento e eliminação)?	R01 – Acesso Não Autorizado; R02 - Modificação não autorizada; R03 - Perda; R04 – Roubo; R05 - Remoção não autorizada; R12 - Vinculação ou associação indevida; R14 - Reidentificação de dados
108 - A instituição implementa processos para que o tratamento dos dados pessoais seja preciso, completo, atualizado, adequado e relevante para a finalidade de uso?	R09 - Falha em considerar os direitos do titular; R13 - Falha ou erro de processamento
109 - A instituição implementa medidas que garantam e maximizem a precisão dos dados pessoais coletados, antes de qualquer armazenamento ou processamento de dados pessoais?	R13 - Falha ou erro de processamento