Auditoria para avaliar a adequação das organizações públicas à LGPD

A Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), que entrou em vigor em agosto de 2020, dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado. Um ano após o início de sua vigência, o Tribunal de Contas da União (TCU) constatou que 76,7% das organizações públicas federais ainda permaneciam nos graus inexpressivo ou inicial de adequação à LGPD (TC 039.606/2020-1; Acórdão 1.384/2022-TCU-Plenário, relator Ministro Augusto Nardes).

Com isso, o presente momento mostra-se oportuno para a realização de nova ação de controle, com vistas a verificar a evolução do cumprimento da legislação por parte dos órgãos e entidades da Administração Pública. De acordo com previsão incluída na Ação 29 do Plano Anual de Trabalho (PAT) 2024 da Rede Integrar, essa nova auditoria será realizada em parceria com os Tribunais de Contas Estaduais (TCEs) que aderiram à ação, de modo a ampliar o escopo da avaliação para incluir, além das organizações federais, também um conjunto de organizações públicas estaduais e municipais. No total, tribunais de nove estados da federação aderiram à fiscalização (TCE-AM, TCE-BA, TCE-CE, TCE-PA, TCE-PE, TCE-PR, TCE-RJ, TCE-RN e TCE-SC).

O método utilizado é denominado autoavaliação de controles internos (do inglês *Control Self-Assessment* – CSA), no qual disponibiliza-se um questionário para que os gestores preencham as respostas que melhor reflitam a situação atual das respectivas organizações com relação à implementação de controles e medidas para assegurar a conformidade com a LGPD, anexando-se as evidências correspondentes. Cada organização federal, estadual e municipal fiscalizada deverá designar uma pessoa para responder as perguntas a seguir em nome da instituição, realizando o respectivo envio (clique no botão “Enviar” disponível na última página do questionário) até às 23h59 do dia 12/7/2024 (sexta-feira).

Espera-se que esta fiscalização sirva para conscientizar e orientar gestores e unidades de auditoria interna de diferentes níveis federativos na condução de iniciativas para que seus órgãos e entidades se adequem à legislação e, também, possam continuar se autoavaliando ao longo dos próximos anos. A partir dos resultados levantados junto às organizações fiscalizadas, planeja-se, também, construir um painel nacional de implementação da LGPD.

Este código de acesso (*token*: {TOKEN:TOKEN}) corresponde às respostas da organização **{TOKEN:LASTNAME}**.

Observações importantes:

1) Todos os textos do questionário foram previamente validados com o intuito de minimizar dúvidas de interpretação em relação às perguntas e às opções de resposta correspondentes. Aconselha-se que o questionário seja preenchido o quanto antes, idealmente logo nos primeiros dias do prazo disponível (a partir de 24/6/2024), frisando-se que eventuais

solicitações de esclarecimentos (a serem encaminhadas para o e-mail **auditoria.lgpd@tcu.gov.br**) podem não ser respondidas a tempo e que isso não justifica o não preenchimento completo e envio do questionário **até às 23h59 do dia 12/7/2024 (sexta-feira)**.

2) O questionário não contempla todas as medidas e controles possíveis de serem implementados para a adequação das organizações à LGPD, podendo, ainda, abranger questões e opções de resposta que tratam de medidas e controles que podem não ser aplicáveis a algumas organizações, por diversas razões (*e.g.* contexto específico, porte, objetivos institucionais, características particulares da instituição).

3) A partir deste questionário, esta Corte de Contas pretende diagnosticar a maturidade das organizações em relação aos critérios questionados, ciente de que uma maturidade maior implica em custos mais elevados e que, portanto, a definição do grau de maturidade mais adequado a cada organização é, essencialmente, uma decisão de gestão (tomada com base no tipo de negócio, apetite a riscos, custo e expectativa de retorno da implementação de controles internos específicos etc.), a qual deve estar amparada por análises devidamente fundamentadas.

4) As questões tiveram como referência a própria legislação (sobretudo a Lei 13.709/2018), normas e códigos de boas práticas, em especial a norma ABNT NBR ISO/IEC 27701:2019 (“Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes”).

5) O questionário envolve a solicitação de informações e, em casos pontuais, solicita o envio/anexação de arquivos capazes de evidenciar as respostas fornecidas. Nas questões que permitem a marcação de uma única opção de resposta (TIPO A), as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação às práticas e aos controles envolvidos. Para essas questões, o respondente deve decidir qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização. Nas questões que permitem a marcação de múltiplas opções de resposta (TIPO B), o respondente deve marcar todas as opções atendidas pela sua organização.

6) Nas questões do TIPO A, além de marcar a opção que melhor reflete a situação da sua organização em relação ao tópico questionado, o gestor **DEVE** complementar textualmente a sua resposta, no respectivo campo de comentário (que aceita texto aberto). Caso marque a opção “Não se aplica”, o gestor deve justificar nesse campo o seu entendimento pela não aplicação daquela medida/controle à sua organização. Caso marque alguma das demais opções de resposta, o gestor deve fornecer nesse campo detalhes que permitam compreender melhor a escolha por aquela opção, considerando o contexto específico da sua organização. Por exemplo, o gestor deve utilizar esse campo para descrever, quando aplicável, datas, períodos, responsáveis, projetos e iniciativas, bem como referenciar artefatos, evidências, atas e outros documentos internos, indicando os respectivos nomes, datas e números de identificação, se houver. A qualquer momento, inclusive após encerrado o prazo para o preenchimento do questionário, os auditores poderão requisitar informações adicionais, bem como o envio desses elementos (artefatos, evidências, atas, documentos) eventualmente mencionados pelo gestor.

7) O respondente pode navegar à vontade entre os grupos de questões por meio dos botões “Próximo” e “Anterior” localizados no rodapé das páginas. O botão “Próximo”, no entanto, só permitirá o avanço se as perguntas obrigatórias do grupo/página (marcadas com um asterisco vermelho) estiverem preenchidas. No ponto onde estiver, o respondente também pode clicar em “Retomar mais tarde” para salvar as respostas marcadas até então e voltar a preencher o questionário em outro momento. Após clicar em “Próximo” no último grupo de questões, haverá uma última tela com o intuito de fornecer ao respondente mais uma oportunidade de voltar e revisar todas as respostas fornecidas no questionário.

8) Para eventuais consultas, uma cópia completa deste questionário (em PDF), bem como outras informações relacionadas, estão disponíveis na página da fiscalização, hospedada no portal do TCU (https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/auditoria-sobre-lgpd (https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/auditoria-sobre-lgpd)). Recomenda-se, também, imprimir esta página, tendo em vista que estas orientações poderão ser úteis ao longo do preenchimento de todo o questionário.

9) Esta Corte de Contas comunica que, assim como ocorreu na fiscalização anterior (Acórdão 1.384/2022-TCU-Plenário, item 9.10), à exceção das informações pessoais dos gestores respondentes e dos textos fornecidos nos campos de comentário, os dados das respostas individuais das organizações ao questionário da auditoria serão classificados como públicos, à luz do art. 3º, inciso I, da Lei 12.527/2011 (Lei de Acesso à Informação – LAI; https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm (https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm)).

10) Incluindo a identificação do respondente (Q1.1), este questionário contém, no total, 22 questões, sendo que algumas só abrem de forma condicionada a respostas anteriores e algumas destinam-se apenas à anexação de documentos. Para esses casos, é aceito o upload de um único arquivo, em formato PDF (se o arquivo original estiver em outro formato, será necessário imprimi-lo em PDF), com tamanho máximo de 20MB.

11) Este questionário foi avaliado pela Autoridade Nacional de Proteção de Dados (ANPD). Existe(m) 22 questão(ões) neste questionário.

1. Identificação do respondente

1. Identificação do respondente

De acordo com o ofício de comunicação de fiscalização enviado previamente, a organização deve indicar um servidor responsável pela resposta ao questionário.

1.1 Dados do servidor responsável pela resposta ao questionário: *

Os dados pessoais solicitados se limitam ao que é estritamente necessário para que a equipe de auditoria possa entrar em contato com o respondente, caso haja necessidade.

2. Preparação

2. Preparação

Antes de iniciar o processo de adequação à LGPD, a organização deve adotar medidas e realizar ações no sentido de construir um ambiente propício para o sucesso dessa empreitada.

A questão desta seção, então, aborda aspectos relacionados à identificação, ao planejamento e à concretização dessas medidas preparatórias.

Um exemplo de medida preparatória pode ser a instituição de um comitê ou de um grupo de trabalho para tratar do tema. Ademais, mesmo antes de formalizar qualquer normativo interno especificamente relacionado à proteção e à privacidade de dados, a organização pode produzir determinados artefatos iniciais, tais como estudos, planos de ação, atas de reuniões, trocas de e-mails com propostas a respeito etc.

É importante que, desde o início, essas iniciativas contem com o apoio e, idealmente, até mesmo com a participação direta da alta direção da organização. Ademais, convém que sejam envolvidas pessoas da organização pertencentes a unidades que exercem atividades relevantes para o tratamento de dados pessoais (*e.g.* Segurança da Informação, Tecnologia da Informação, Direito, Auditoria/Conformidade, Ouvidoria).

Em um primeiro estágio de maturidade, a organização terá apenas documentado informações relacionadas aos objetivos dessas iniciativas de adequação e às ações necessárias para alcançá-los, possivelmente especificando os recursos necessários, os responsáveis e os prazos previstos.

Avançando, em um estágio intermediário, a organização já terá normatizado as principais questões relacionadas ao tema tratamento de dados (*e.g.* política de proteção de dados pessoais, plano de capacitação associado, política de privacidade), levando em consideração os princípios gerais ou todos os elementos elencados na LGPD.

Por fim, no nível mais maduro em relação ao tema, a organização possuirá programa de governança em privacidade de dados implementado, amplamente divulgado a todas as partes interessadas e sendo periodicamente avaliado e revisado, com vistas à melhoria contínua.

Referências úteis:

- Lei 13.709/2018, art. 50, em especial § 2º, inciso I (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm));

- ABNT NBR ISO/IEC 27701:2019, item 5.4 (Planejamento).

2.1 (TIPO A) A organização conduziu iniciativas para identificar, planejar e executar medidas preparatórias com vistas a se adequar à LGPD? *

Favor escolher apenas uma das opções a seguir:

◯ Não se aplica (justificar no campo de comentário)

◯ Não (a organização não realizou medidas preparatórias com vistas a se adequar à LGPD)

◯ A organização iniciou, mas ainda não concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD

◯ A organização concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD (possui plano de ação, plano de projeto ou documento similar para direcionar os esforços nesse sentido), porém ainda não formalizou normativo interno relacionado à proteção e à privacidade de dados

◯ A organização concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD e já publicou uma política (ou documento similar) que considera os princípios e aspectos gerais relacionados ao tratamento de dados

◯ A organização já mapeou seus principais processos de tratamento de dados (natureza, escopo, finalidade, benefícios, probabilidade e gravidade dos riscos associados) e publicou normativos internos que tratam dos aspectos mais importantes relacionados à proteção e à privacidade de dados, porém ainda não possui um programa de governança em privacidade de dados implementado

◯ A organização já mapeou todos os processos de tratamento de dados (natureza, escopo, finalidade, benefícios, probabilidade e gravidade dos riscos associados), publicou normativos internos que tratam dos temas proteção e privacidade de dados de forma abrangente e possui programa de governança em privacidade de dados implementado, periodicamente monitorado/avaliado e atualizado continuamente

Comente aqui sua escolha:

Questão TIPO A:

Esta questão permite a marcação de uma única opção de resposta, sendo que as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação às práticas e aos controles envolvidos. No caso, o respondente deve assinalar qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização.

Além de marcar a opção que melhor reflete a situação da sua organização em relação ao tópico questionado, o gestor **DEVE** complementar textualmente a sua resposta, no respectivo campo de comentário (que aceita texto aberto). Caso marque a opção “Não se aplica”, o gestor deve justificar nesse campo o seu entendimento pela não aplicação daquela medida/controle à sua organização. Caso marque alguma das demais opções de resposta, o gestor deve fornecer nesse campo detalhes que permitam compreender melhor a escolha por aquela opção, considerando o contexto específico da sua organização. Por exemplo, o gestor deve utilizar esse campo para descrever, quando aplicável, datas, períodos, responsáveis, projetos e iniciativas, bem como referenciar artefatos, evidências, atas e outros documentos internos, indicando os respectivos nomes, datas e números de identificação, se houver. A qualquer momento, inclusive após encerrado o prazo para o preenchimento do questionário, os auditores poderão requisitar informações adicionais, bem como o envio desses elementos (artefatos, evidências, atas, documentos) eventualmente mencionados pelo gestor.

3. Contexto organizacional

3. Contexto organizacional

Para alcançar os resultados pretendidos pelas iniciativas de adequação à LGPD, a organização deve avaliar uma série de fatores internos e externos relevantes para atingir os objetivos associados.

A questão desta seção, então, aborda aspectos relacionados ao mapeamento dos normativos correlatos à proteção de dados pessoais que devem ser respeitados pela organização, à identificação das partes interessadas e às análises dos diferentes tipos de dados pessoais tratados pela organização e dos processos organizacionais que realizam o tratamento desses dados. (Obs.: por dado pessoal, entende-se qualquer informação relacionada à pessoa natural identificada ou identificável [*e.g.* nome, RG, CPF, telefone, e-mail]; por tratamento de dados, entende-se qualquer operação [*e.g.* coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão, extração] realizada com dados pessoais).

Por exemplo, o Decreto-Lei 5.452/1943 (Consolidação das Leis do Trabalho – CLT) e as Leis 8.078/1990 (Código de Defesa do Consumidor – CDC), 12.414/2011 (Cadastro Positivo), 12.527/2011 (Lei de Acesso à Informação – LAI) e 13.787/2018 (digitalização e utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuários de pacientes) contém diversos dispositivos que, eventualmente, podem se aplicar à organização.

Além dessas leis, também podem existir normas infralegais, regulamentos, portarias, instruções normativas, decisões judiciais/administrativas e requisitos contratuais que tragam comandos relacionados à proteção de dados pessoais e que também devem ser respeitados pela organização.

Convém, ainda, que a organização identifique todas as partes que possuem interesses ou responsabilidades associadas ao tratamento de dados pessoais, tais como os titulares de dados pessoais, os controladores conjuntos e os operadores. O titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (*e.g.* cidadão, cliente, servidor público, representante de fornecedor, terceirizado). O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (controlador conjunto é aquele que determina os propósitos e as formas do tratamento de dados pessoais junto com outro controlador). A seu turno, o operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Considerando que o controlador é obrigado a reparar danos causados em razão da atividade de tratamento de dados pessoais (LGPD, art. 42), a organização deve ter contrato firmado com os agentes contratados que realizam tratamento de dados em seu nome (operadores), bem como com os controladores conjuntos, contendo cláusulas com vistas a definir papéis e responsabilidades e a assegurar que estes adotem medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais compartilhados com eles.

Ademais, tanto o controlador quanto o operador devem manter registro das operações de tratamento de dados pessoais realizadas (LGPD, art. 37), sendo que a ANPD poderá determinar ao controlador que elabore Relatório de Impacto à Proteção de Dados Pessoais (RIPD) com descrição, dentre outros elementos, dos dados coletados e das metodologias de coleta e de garantia da segurança das informações (art. 38).

A organização deve, ainda, estabelecer políticas e salvaguardas adequadas, com base em avaliações sistemáticas dos impactos e dos riscos à privacidade, relativamente aos dados pessoais tratados, com vistas a mitigar possíveis probabilidades e impactos da ocorrência de situações indesejadas (art. 50, § 2º, inciso I, alínea “d”). Esses riscos devem ser avaliados sob o prisma das diversas operações realizadas com os dados (*e.g.* coleta, produção, acesso, transmissão, armazenamento, eliminação). Inclusive, tais avaliações devem nortear a organização quanto a eventual necessidade de priorizar as iniciativas de adequação à LGPD em relação a processos de negócio específicos, de mais alto risco.

Referências úteis:

- Lei 13.709/2018, art. 5º, em especial incisos I, V, VI, VII e X, art. 7º, § 5º, e arts. 37, 39, 42-46 e 50, § 1º e § 2º, inciso I, alínea “d” (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm));

- ABNT NBR ISO/IEC 27701:2019, itens 5.2.1 (Entendendo a organização e seu contexto), 5.2.2 (Entendendo as necessidades e as expectativas das partes interessadas), 5.4.1.2 (Avaliação de riscos de segurança da informação), 6.5.1 (Responsabilidade pelos ativos), 6.5.2 (Classificação da informação), 7.2.6 (Contratos com operadores de dados pessoais), 7.2.7 (Controlador conjunto de dados pessoais) e 7.2.8 (Registros relativos ao tratamento de dados pessoais).

3.1 (TIPO B) A organização conduziu iniciativa com vistas a IDENTIFICAR: *

Por favor, escolha as opções que se aplicam:

☐ A organização AINDA NÃO CONDUZIU INICIATIVA com vistas a identificar qualquer dos objetos mencionados nos itens anteriores

☐ E AVALIAR OS RISCOS associados aos processos de tratamento de dados pessoais que foram identificados

☐ OS LOCAIS DE ARMAZENAMENTO dos dados pessoais tratados pela organização (e.g. servidor de arquivos, nuvem, dispositivo USB, storage, fita de backup, arquivos físicos [pastas, armários])

☐ OS DADOS PESSOAIS TRATADOS pela organização

☐ OS PROCESSOS DE NEGÓCIO que realizam tratamento de dados pessoais e os respectivos RESPONSÁVEIS (e.g. pessoas, departamentos, operadores, controladores conjuntos)

☐ E ADEQUAR OS INSTRUMENTOS CONTRATUAIS (e.g. contrato, convênio, acordo de cooperação) firmados com os operadores e os controladores conjuntos identificados, de forma a estabelecer suas respectivas responsabilidades e papéis com relação à proteção de dados pessoais

☐ Se há tratamento de dados que envolva CONTROLADOR CONJUNTO

☐ OS OPERADORES que realizam tratamento de dados pessoais em seu nome

☐ AS DIFERENTES CATEGORIAS DE TITULARES de dados pessoais com os quais se relaciona (e.g. cidadão, cliente, servidor público, representante de fornecedor, terceirizado)

☐ OUTROS NORMATIVOS (e.g. leis, regulamentos, portarias, instruções normativas, decisões judiciais/administrativas, requisitos contratuais), além da LGPD, que abrangem comandos relacionados à proteção de dados pessoais, os quais a organização deve respeitar

Questão TIPO B:

Esta questão permite a marcação de múltiplas opções de resposta. No caso, o respondente deve marcar todas as opções que contém iniciativas que já foram realizadas pela sua organização.

4. Liderança

4. Liderança

A alta direção da organização deve demonstrar claramente liderança e comprometimento com a iniciativa de adequação à LGPD.

Nesse sentido, a elaboração e a ampla divulgação de políticas relacionadas à proteção de dados pessoais, bem como a nomeação de um encarregado pelo tratamento de dados pessoais (normalmente chamado de DPO, do inglês *Data Protection Officer*), são ações fundamentais para o processo de adequação à LGPD. O encarregado nomeado deve ter independência (não ser gestor responsável por sistema de informação e não fazer parte de setor/departamento que possa gerar conflito de interesses quanto à sua atuação, a exemplo das unidades de TI [IN SGD/ME 117/2020, art. 1º, § 1º, inciso II]) e autonomia suficientes para reportar à alta administração, servindo como canal de comunicação efetivo entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Deve, ainda, além de profundo entendimento da própria LGPD (Lei 13.709/2018), possuir conhecimentos multidisciplinares relativos a uma série de temas correlatos (*e.g.* Direito, Governança Corporativa e de Dados, Gestão de Riscos, Tecnologia da Informação, Segurança da Informação, Privacidade e Proteção de Dados).

A questão desta seção, então, aborda aspectos atinentes à nomeação desse encarregado e à formalização de políticas (ou documentos similares) que busquem assegurar, no âmbito da organização, a segurança das informações e a proteção dos dados pessoais. A título de exemplo, citam-se:

- Política de Segurança da Informação (PSI): aprovada pela alta direção, estabelece a abordagem da organização para gerenciar os objetivos nessa área, em linha com os requisitos do negócio e com leis e regulamentações aplicáveis; é obrigatória para os órgãos e entidades da Administração Pública federal (Decreto 9.637/2018, art. 15, inciso II);

- Política de Classificação da Informação (PCI): fornece diretrizes para assegurar que as diferentes informações recebam níveis adequados de proteção, de acordo com a sua importância para a organização e os riscos associados; documento importante para direcionar a implementação de controles adequados para a proteção de dados pessoais;

- Política de Proteção de Dados Pessoais (PPDP): alinhada à PSI e à PCI, estabelece regras e diretrizes para o tratamento e para a governança de dados pessoais dentro da organização (público interno), reforçando seu compromisso para alcançar a conformidade com os normativos de proteção de dados pessoais [ver https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/modelo_ppdp.docx (https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/modelo_ppdp.docx)].

Em especial no que tange à classificação das informações, a LGPD demanda que sejam adotados cuidados específicos para o tratamento de dados pessoais sensíveis (que envolvem origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico) e de dados pessoais de crianças e de adolescentes (Lei 13.709/2018, art. 5º, inciso II, e arts. 11-14).

Referências úteis:

- Lei 13.709/2018, em especial art. 5º, incisos I, II e VIII, arts. 11-14, art. 23, inciso III, e arts. 41, 46 e 50, § 2º, inciso I, alíneas “a” e “d” (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm));

- IN SGD/ME 117/2020 (Dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais na APF), em especial art. 1º, § 1º, incisos I e II, e art. 2º (https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-117-de-19-de-novembro-de-2020-289515596 (https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-117-de-19-de-novembro-de-2020-289515596));

- ABNT NBR ISO/IEC 27701:2019, itens 5.3.2 (Política), 6.2 (Políticas de segurança da informação), 6.2.1 (Orientação da Direção para segurança da informação), 6.3.1 (Organização interna) e 6.5.2 (Classificação da informação), 6.5.2.2 (Rótulos e tratamento da informação);

- Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado (https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf (https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf)).

4.1 (TIPO B) A organização: *

Por favor, escolha as opções que se aplicam e faça um comentário:

☐ AINDA NÃO ATENDE NENHUM dos itens anteriores

☐ DIVULGA EM SEU SÍTIO ELETRÔNICO INSTITUCIONAL a identidade e as informações de contato (nome, e-mail, telefone) do encarregado pelo tratamento de dados pessoais, em local de fácil acesso aos titulares de dados pessoais

☐ Nomeou o ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS (Data Protection Officer – DPO) e publicou essa nomeação em veículo de comunicação oficial (e.g. Diário Oficial da União – DOU)

☐ Instituiu formalmente e mantém atualizada POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS (ou instrumento similar)

☐ Instituiu formalmente e mantém atualizada POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO (ou instrumento similar), sendo que abordou nesse documento questões específicas relacionadas à classificação de dados pessoais, de dados pessoais sensíveis e de dados pessoais de crianças e de adolescentes

☐ Instituiu formalmente e mantém atualizada POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (ou instrumento similar)

Questão TIPO B:

Esta questão permite a marcação de múltiplas opções de resposta. No caso, o respondente deve marcar todas as opções que são atendidas pela sua organização.

Caso marque alguma das opções relativas às políticas, no campo de comentário associado especifique o documento interno e informe, se houver, o endereço da internet (URL) onde este está publicado. Por exemplo, no caso do TCU, a Política de Proteção de Dados Pessoais foi estabelecida por meio da Portaria-TCU 163/2023 (https://pesquisa.apps.tcu.gov.br/documento/norma/*/KEY%253ANORMA-23222/score%2520desc/0 (https://pesquisa.apps.tcu.gov.br/documento/norma/*/KEY%253ANORMA-23222/score%2520desc/0)). Caso marque

alguma das outras opções, nos campos de comentário associados informe os endereços da internet (URLs) onde podem ser verificadas a publicação da nomeação do encarregado em veículo de comunicação oficial e/ou as suas respectivas informações de contato.

4.1.1 Anexe a Política de Proteção de Dados Pessoais (ou instrumento similar) da organização:

Só responder essa pergunta sob as seguintes condições:
((Q41_SQ003.NAOK (/pesquisas/index.php/questionAdministration/view/surveyid/542191/gid/655/qid/10374) == 'Y'))

Kindly attach the aforementioned documents along with the survey

Só é aceito o *upload* de um único arquivo no formato PDF, com tamanho máximo de 20MB.

5. Capacitação

5. Capacitação

É necessário que todas as pessoas da organização estejam cientes da importância dos temas privacidade e proteção de dados pessoais, bem como dos impactos e prejuízos que podem ser causados devido às violações desses dados (*e.g.* sanções aplicadas pela ANPD, indenizações, danos financeiros e à imagem da instituição). Com isso, a organização deve conduzir iniciativas tanto para conscientizar quanto para capacitar seus colaboradores nessas áreas. A conscientização é importante para que os colaboradores conheçam a legislação, bem como as políticas e normativos institucionais relacionados à proteção de dados pessoais, e para que reconheçam como as suas decisões e ações podem afetar a preservação da privacidade dos titulares de dados.

Nesse sentido, é conveniente que a organização elabore um Plano de Capacitação que contemple ações de conscientização e que determine os conhecimentos e as competências necessárias para os recursos humanos relativamente a essa temática, sobretudo no que tange aos colaboradores diretamente envolvidos em atividades que realizam o tratamento de dados pessoais. Assim, o Plano de Capacitação deve mapear as lacunas de conhecimentos e habilidades associadas ao tema e planejar ações de treinamento para sua redução gradual.

As ações de capacitação devem considerar diferentes níveis de envolvimento dos colaboradores com essa temática, de forma que aquelas pessoas envolvidas em atividades críticas relacionadas ao tratamento de dados pessoais e que ocupam funções com responsabilidades essenciais relacionadas à proteção de dados pessoais recebam treinamento diferenciado, além do nível básico fornecido aos demais colaboradores.

Por fim, vale ressaltar que tanto a LGPD, ao focar na proteção dos dados pessoais e na privacidade dos indivíduos, quanto a Lei 12.527/2011 (Lei de Acesso à Informação – LAI), ao promover a transparência e o acesso às informações públicas, buscam garantir direitos fundamentais relacionados à informação em sentido amplo. Ambas (LGPD e LAI) atuam para fortalecer a proteção dos direitos dos cidadãos e exigir das entidades, públicas e privadas, maior zelo quanto à gestão e ao tratamento das informações. Para isso, embora tenham finalidades distintas, essas normas se complementam de forma harmônica, sendo que a conformidade com ambas é fundamental para as organizações.

As questões desta seção, então, abordam aspectos atinentes à avaliação, ao planejamento e à realização de ações de capacitação relacionadas à privacidade e à proteção de dados pessoais, bem como à necessidade de harmonização entre a LGPD e a LAI.

Referências úteis:

- Lei 12.527/2011 (https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm (https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm));

- ABNT NBR ISO/IEC 27701:2019, itens 5.5.2 (Competência), 5.5.3 (Conscientização) e 5.5.4 (Comunicação).

5.1 (TIPO A) Acerca da capacitação dos seus colaboradores em proteção de dados pessoais, a organização: *

Favor escolher apenas uma das opções a seguir:

◯ Não se aplica (justificar no campo de comentário)

◯ Não possui PLANO DE CAPACITAÇÃO (ou instrumento similar) e seus colaboradores ainda não realizaram treinamento em proteção de dados pessoais

◯ Não possui PLANO DE CAPACITAÇÃO (ou instrumento similar), mas colaboradores específicos já realizaram treinamento em proteção de dados pessoais

◯ Possui PLANO DE CAPACITAÇÃO (ou instrumento similar) e, apesar de este não contemplar a temática de proteção de dados pessoais de maneira específica, já realizou treinamento abrangente (não direcionado apenas a determinados colaboradores) nessa área

◯ Possui PLANO DE CAPACITAÇÃO (ou instrumento similar), contemplou nesse documento a temática de proteção de dados pessoais e já realizou treinamento da maioria dos colaboradores nessa área

◯ Possui PLANO DE CAPACITAÇÃO (ou instrumento similar), contemplou nesse documento a temática de proteção de dados pessoais, incluindo a necessidade de treinamento diferenciado para as pessoas que exercem funções com responsabilidades essenciais quanto à proteção de dados pessoais, e já realizou treinamento de todos os colaboradores nessa área

Comente aqui sua escolha:

Questão TIPO A:

Esta questão permite a marcação de uma única opção de resposta, sendo que as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação às práticas e aos controles envolvidos. No caso, o respondente deve assinalar qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização.

Além de marcar a opção que melhor reflete a situação da sua organização em relação ao tópico questionado, o gestor **DEVE** complementar textualmente a sua resposta, no respectivo campo de comentário (que aceita texto aberto). Caso marque a opção “Não se aplica”, o gestor deve justificar nesse campo o seu entendimento pela não aplicação daquela medida/controle à sua organização. Caso marque alguma das demais opções de resposta, o gestor deve fornecer nesse campo detalhes que permitam compreender melhor a escolha por aquela opção, considerando o contexto específico da sua organização. Por exemplo, o gestor deve utilizar esse campo para descrever, quando aplicável, datas, períodos, responsáveis, projetos e iniciativas, bem como referenciar artefatos, evidências, atas e outros documentos internos, indicando os respectivos nomes, datas e números de identificação, se houver. A qualquer momento, inclusive após encerrado o prazo para o preenchimento do questionário, os auditores poderão requisitar informações adicionais, bem como o envio desses elementos (artefatos, evidências, atas, documentos) eventualmente mencionados pelo gestor.

5.1.1 Anexe o Plano de Capacitação (ou instrumento similar) da organização:

Só responder essa pergunta sob as seguintes condições:
A resposta foi 'Possui PLANO DE CAPACITAÇÃO (ou instrumento similar), contemplou nesse documento a temática de proteção de dados pessoais, incluindo a necessidade de treinamento diferenciado para as pessoas que exercem funções com responsabilidades essenciais quanto à proteção de dados pessoais, e já realizou treinamento de todos os colaboradores nessa área' *ou* 'Possui PLANO DE CAPACITAÇÃO (ou instrumento similar), contemplou nesse documento a temática de proteção de dados pessoais e já realizou treinamento da maioria dos colaboradores nessa área' na questão ' [Q51]' (5.1 (TIPO A) Acerca da capacitação dos seus colaboradores em proteção de dados pessoais, a organização:)

Kindly attach the aforementioned documents along with the survey

Só é aceito o *upload* de um único arquivo no formato PDF, com tamanho máximo de 20MB.

5.2 (TIPO B) Acerca das ações de capacitação em proteção de dados pessoais realizadas nos últimos 3 (três) anos, a organização: *

Só responder essa pergunta sob as seguintes condições:
((Q51.NAOK (/pesquisas/index.php/questionAdministration/view/surveyid/542191/gid/418/qid/10338) == 'AO03' or Q51.NAOK (/pesquisas/index.php/questionAdministration/view/surveyid/542191/gid/418/qid/10338) == 'AO04' or Q51.NAOK (/pesquisas/index.php/questionAdministration/view/surveyid/542191/gid/418/qid/10338) == 'AO05' or Q51.NAOK (/pesquisas/index.php/questionAdministration/view/surveyid/542191/gid/418/qid/10338) == 'AO06'))

Por favor, escolha as opções que se aplicam:

☐ NÃO ATENDEU NENHUM dos itens anteriores

☐ ORIENTOU OS PARTICIPANTES nesses treinamentos, mesmo que a posteriori, sobre a necessidade de observarem as diretrizes e orientações publicadas pela CGU por meio do “PARECER SOBRE ACESSO À INFORMAÇÃO para atender ao Despacho Presidencial de 1º de janeiro de 2023” (https://www.gov.br/acessoainformacao/pt-br/entendimentos-e-estudos-sobre-a-lai/copy_of_parecerfinalsobreacessoinformao_cgu_fev2023.pdf)

☐ ORIENTOU OS PARTICIPANTES nesses treinamentos, mesmo que a posteriori, sobre a necessidade de observarem os Enunciados da CGU divulgados por meio da PORTARIA NORMATIVA CGU 71/2023 (https://www.in.gov.br/en/web/dou/-/portaria-normativa-cgu-n-71-de-10-de-abril-de-2023-477406468)

☐ OFERECEU AÇÃO DE CAPACITAÇÃO QUE TENHA ABORDADO CONJUNTAMENTE, de forma integrada, as temáticas da proteção de dados pessoais (LGPD) e da transparência da gestão (LAI)

☐ Efetivamente CAPACITOU NO TEMA TRANSPARÊNCIA da gestão relativa às informações de interesse coletivo ou geral (LAI) MAIS DE 50% dos colaboradores que receberam treinamento em proteção de dados pessoais

☐ Levou em consideração a necessidade de COMPLEMENTAR A CAPACITAÇÃO dos participantes nesses treinamentos COM CONTEÚDO SOBRE TRANSPARÊNCIA da gestão relativa às informações de interesse coletivo ou geral (Lei 12.527/2011 – Lei de Acesso à Informação)

Questão TIPO B:

Esta questão permite a marcação de múltiplas opções de resposta. No caso, o respondente deve marcar todas as opções que são atendidas pela sua organização.

6. Conformidade do tratamento

6. Conformidade do tratamento

A organização deve ser capaz de provar que os tratamentos de dados pessoais que realiza são lícitos. Para isso, é fundamental demonstrar que os princípios estabelecidos no art. 6º da LGPD são seguidos e que os tratamentos são fundamentados em, ao menos, uma das bases legais descritas na legislação.

A questão desta seção, então, aborda aspectos atinentes à conformidade das atividades de tratamento de dados pessoais realizadas pela organização frente a alguns dos princípios da LGPD, a exemplo de possuir propósitos legítimos, específicos, explícitos e informados aos titulares, de modo que estes sejam capazes de compreender claramente a(s) finalidade(s) para a(s) qual(is) os seus dados pessoais são tratados.

Ademais, a coleta deve se restringir aos dados pessoais estritamente necessários para cumprir com as finalidades de tratamento informadas, a retenção (armazenamento) dos dados deve durar apenas o tempo estritamente necessário para cumprir com essas mesmas finalidades, bem como devem ser identificadas e documentadas as bases legais que fundamentam todas as atividades de tratamento de dados pessoais da organização. As possíveis bases legais são relacionadas nos incisos I a X do art. 7º da Lei 13.709/2018 (consentimento, cumprimento de obrigação legal/regulatória, execução de políticas públicas pela Administração Pública, estudos por parte de órgão de pesquisa, execução de contratos, exercício regular de direitos em processo judicial/administrativo/arbitral, proteção da vida ou da incolumidade física do titular ou de terceiro, tutela da saúde, interesse legítimo do controlador ou de terceiro e proteção do crédito).

A organização também deve manter registro detalhado (*e.g.* inventário) das operações de tratamento de dados pessoais que realiza, especialmente quando baseado no legítimo interesse (LGPD, art. 37). Esse registro pode contemplar, por exemplo: a identificação do tratamento, sua finalidade, a base legal que o fundamenta, a descrição das categorias dos titulares de dados pessoais envolvidos, os dados pessoais coletados, o tempo de retenção dos dados, o local de armazenamento dos dados, o responsável pelo processo de tratamento e as medidas de segurança adotadas.

Por fim, relativamente às suas operações de maior risco (ver Resolução CD/ANPD 2/2022 [https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022 (https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022)], Anexo I, art. 4º), a organização deve elaborar Relatório de Impacto à Proteção de Dados Pessoais (RIPD), inclusive de dados sensíveis, para avaliar os possíveis riscos associados (LGPD, art. 38). Por meio do RIPD, a organização descreverá os tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações, identificará a probabilidade de ocorrência de cada fator de risco e o seu impacto sobre as liberdades e direitos fundamentais dos titulares de dados e avaliará as medidas, as salvaguardas e os mecanismos de mitigação de risco apropriados a cada hipótese

(https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd (https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd)).

Referências úteis:

- Lei 13.709/2018, art. 5º, inciso XVII, art. 6º, em especial incisos I, II e III, e arts. 7º, 37, 38 e 40 (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm));

- ABNT NBR ISO/IEC 27701:2019, itens 7.2.1 (Identificação e documentação do propósito), 7.2.2 (Identificação de bases legais), 7.2.5 (Avaliação de impacto de privacidade), 7.2.8 (Registros relativos ao tratamento de DP), 7.4.1 (Limite de coleta) e 7.4.7 (Retenção).

6.1 (TIPO B) A organização: *

Por favor, escolha as opções que se aplicam:

☐ Identificou e DOCUMENTOU AS FINALIDADES de todas as suas principais atividades de tratamento de dados pessoais

☐ Avaliou se COLETA APENAS OS DADOS ESTRITAMENTE NECESSÁRIOS para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas

☐ Avaliou se OS DADOS PESSOAIS SÃO RETIDOS/ARMAZENADOS DURANTE O TEMPO ESTRITAMENTE NECESSÁRIO para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas

☐ Identificou e DOCUMENTOU AS BASES LEGAIS que fundamentam todas as suas principais atividades de tratamento de dados pessoais

☐ AINDA NÃO ATENDE NENHUM dos itens anteriores

☐ JÁ IMPLEMENTOU CONTROLES para mitigar os riscos identificados por meio da elaboração de RIPD (Relatório de Impacto à Proteção de Dados Pessoais)

☐ JÁ ELABOROU ALGUM RIPD – Relatório de Impacto à Proteção de Dados Pessoais (LGPD, art. 5º, inciso XVII)

☐ Mantém REGISTRO DAS OPERAÇÕES de tratamento de dados pessoais que realiza, em especial quando o tratamento se baseia no legítimo interesse

☐ CATALOGOU NO(S) REGISTRO(S)/INVENTÁRIO(S) DE DADOS PESSOAIS informações que abrangem todas as suas principais atividades de tratamento de dados pessoais

☐ POSSUI REGISTRO(S) (e.g. INVENTÁRIO[S] DE DADOS PESSOAIS) instituído(s) para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais

Questão TIPO B:

Esta questão permite a marcação de múltiplas opções de resposta. No caso, o respondente deve marcar todas as opções que contém iniciativas que já foram realizadas pela sua organização.

6.1.1 Anexe o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) elaborado pela organização:

Só responder essa pergunta sob as seguintes condições:
A resposta foi na questão ' [Q61]' (6.1 (TIPO B) A organização:)

Kindly attach the aforementioned documents along with the survey

Só é aceito o *upload* de um único arquivo no formato PDF, com tamanho máximo de 20MB.

7. Direitos do titular

7. Direitos do titular

A organização deve assegurar que os titulares tenham acesso a informações relacionadas ao tratamento de seus dados pessoais. Para isso, a organização deve publicar, de maneira clara e concisa, informações relativas ao tratamento de dados pessoais. A organização também deve estar preparada para atender todos os direitos dos titulares que são elencados na LGPD (arts. 9º e 17-22), em especial aqueles previstos no art. 18.

O art. 9º da LGPD, por exemplo, prevê o direito, aos titulares de dados, de acesso facilitado a uma série de informações: finalidade do tratamento; formas e duração do tratamento; identificação e dados de contato do controlador; informações acerca do uso compartilhado de dados e sua finalidade; responsabilidades dos agentes que realizam o tratamento; e direitos do titular. Além disso, a organização deve informar as hipóteses em que, no exercício de suas competências, realiza tratamento de dados pessoais, fornecendo informações sobre a finalidade, a base legal, os procedimentos e as práticas utilizadas para a execução dessas atividades.

As questões desta seção, então, abordam aspectos atinentes à elaboração da Política de Privacidade (também chamada de “Aviso de Privacidade”) e ao atendimento dos direitos do titular de dados pessoais (*e.g.* confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos/inexatos/desatualizados; revogação do consentimento; anonimização, bloqueio ou eliminação de dados desnecessários/excessivos ou que dependam de consentimento do titular; portabilidade dos dados; informações sobre compartilhamento de dados).

A Política/Aviso de Privacidade é um documento endereçado aos usuários de um site, serviço ou sistema (titulares de dados – público externo), com o propósito de dar visibilidade ao tratamento de dados pessoais que ocorre no âmbito desse site/serviço/sistema, de modo a demonstrar que os princípios da LGPD são atendidos (ver https://www.serpro.gov.br/lgpd/noticias/2019/elabora-politica-privacidade-aderente-lgpd-dados-pessoais (https://www.serpro.gov.br/lgpd/noticias/2019/elabora-politica-privacidade-aderente-

lgpd-dados-pessoais)). Além de fornecer acesso ao documento no momento da coleta dos dados pessoais, convém que a organização o divulgue de forma permanente em seu sítio institucional, em local de fácil acesso aos titulares de dados pessoais.

Referências úteis:

- Lei 13.709/2018, art. 6º, em especial incisos IV e VI, arts. 9º e 17-22, art. 23, inciso I, e art. 50, inciso I, alíneas “a”, “d” e “e” (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm));

- ABNT NBR ISO/IEC 27701:2019, itens 7.3 (Obrigações dos titulares de dados pessoais), 7.3.2 (Determinando as informações para os titulares de dados pessoais) e 7.3.3 (Fornecendo informações aos titulares de dados pessoais).

7.1 (TIPO A) A organização elaborou e divulga em seu sítio eletrônico institucional Política de Privacidade (ou instrumento similar)? *

Favor escolher apenas uma das opções a seguir:

◯ Não se aplica (justificar no campo de comentário)

◯ A organização NÃO ELABOROU POLÍTICA DE PRIVACIDADE (ou instrumento similar)

◯ A organização ELABOROU A POLÍTICA DE PRIVACIDADE (ou instrumento similar), MAS NÃO A DIVULGA em seu sítio eletrônico institucional

◯ A organização ELABOROU A POLÍTICA DE PRIVACIDADE (ou instrumento similar) E A DIVULGA em seu sítio eletrônico institucional [no campo de comentário, informar o endereço da internet (URL) onde a política está publicada]

Comente aqui sua escolha:

Questão TIPO A:

Esta questão permite a marcação de uma única opção de resposta, sendo que as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação às práticas e aos controles envolvidos. No caso, o respondente deve assinalar qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização.

Além de marcar a opção que melhor reflete a situação da sua organização em relação ao tópico questionado, o gestor **DEVE** complementar textualmente a sua resposta, no respectivo campo de comentário (que aceita texto aberto). Caso marque a opção “Não se aplica”, o gestor deve justificar nesse campo o seu entendimento pela não aplicação daquela medida/controle à sua organização. Caso marque alguma das demais opções de resposta, o gestor deve fornecer nesse campo detalhes que permitam compreender melhor a escolha por aquela opção, considerando o contexto específico da sua organização. Por exemplo, o gestor deve utilizar esse campo para descrever, quando aplicável, datas, períodos, responsáveis, projetos e iniciativas, bem como referenciar artefatos, evidências, atas e outros documentos internos, indicando os respectivos nomes, datas e números de identificação, se houver. A qualquer

momento, inclusive após encerrado o prazo para o preenchimento do questionário, os auditores poderão requisitar informações adicionais, bem como o envio desses elementos (artefatos, evidências, atas, documentos) eventualmente mencionados pelo gestor.

7.1.1 Anexe a Política de Privacidade (ou instrumento similar) da organização:

Só responder essa pergunta sob as seguintes condições:
A resposta foi 'A organização ELABOROU A POLÍTICA DE PRIVACIDADE (ou instrumento similar) E A DIVULGA em seu sítio eletrônico institucional [no campo de comentário, informar o endereço da internet (URL) onde a política está publicada]' *ou* 'A organização ELABOROU A POLÍTICA DE PRIVACIDADE (ou instrumento similar), MAS NÃO A DIVULGA em seu sítio eletrônico institucional' na questão ' [Q71]' (7.1 (TIPO A) A organização elaborou e divulga em seu sítio eletrônico institucional Política de Privacidade (ou instrumento similar)?)

Kindly attach the aforementioned documents along with the survey

Só é aceito o *upload* de um único arquivo no formato PDF, com tamanho máximo de 20MB.

7.2 (TIPO A) Foram implementados mecanismos para atender os direitos dos titulares aplicáveis à organização, relacionados à obtenção de informações sobre o tratamento dos dados, de modo geral (LGPD, art. 9º), bem como sobre os seus dados específicos e o respectivo tratamento (art. 18)? *

Favor escolher apenas uma das opções a seguir:

◯ Não se aplica (justificar no campo de comentário)

◯ Não foram implementados mecanismos para atender os direitos dos titulares (LGPD, arts. 9º e 18)

◯ Foram implementados mecanismos para atender alguns dos direitos dos titulares (LGPD, arts. 9º e 18), mas não todos

◯ Foram implementados mecanismos para atender todos os direitos dos titulares (LGPD, arts. 9º e 18) aplicáveis à organização

Comente aqui sua escolha:

Questão TIPO A:

Esta questão permite a marcação de uma única opção de resposta, sendo que as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação às práticas e aos controles envolvidos. No caso, o respondente deve assinalar qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização.

Além de marcar a opção que melhor reflete a situação da sua organização em relação ao tópico questionado, o gestor **DEVE** complementar textualmente a sua resposta, no respectivo campo de comentário (que aceita texto aberto). Caso marque a opção “Não se aplica”, o gestor deve justificar nesse campo o seu entendimento pela não aplicação daquela medida/controle à sua organização. Caso marque alguma das demais opções de resposta, o gestor deve fornecer nesse campo detalhes que permitam compreender melhor a escolha por aquela opção, considerando o contexto específico da sua organização. Por exemplo, o gestor deve utilizar esse campo para descrever, quando aplicável, datas, períodos, responsáveis, projetos e iniciativas, bem como referenciar artefatos, evidências, atas e outros documentos internos, indicando os respectivos nomes, datas e números de identificação, se houver. A qualquer

momento, inclusive após encerrado o prazo para o preenchimento do questionário, os auditores poderão requisitar informações adicionais, bem como o envio desses elementos (artefatos, evidências, atas, documentos) eventualmente mencionados pelo gestor.

8. Compartilhamento de dados pessoais

8. Compartilhamento de dados pessoais

A organização deve identificar, avaliar e documentar detalhes relacionados aos compartilhamentos de dados pessoais com terceiros.

A realização de compartilhamento de dados pessoais demanda a adoção de controles adequados com vistas a mitigar os riscos que possam comprometer a segurança e a proteção desses dados. Diante disso, a LGPD defende, por exemplo, que as partes envolvidas no compartilhamento adotem determinadas precauções, inclusive, em certos casos, exigindo a formalização de contrato, convênio ou instrumento congênere (LGPD, art. 26, § 1º, inciso IV) e a sua respectiva comunicação à ANPD (art. 26, § 2º). Nos casos de eventual transferência internacional dos dados, a LGPD também apregoa, além da conformidade com os princípios, os direitos e o regime de proteção de dados previsto em seu escopo geral, a adoção de uma série de requisitos e cuidados especiais (arts. 33-36), os quais a organização precisa avaliar e cumprir.

No caso de eventual utilização de solução de computação em nuvem (*cloud computing*), a IN GSI/PR 5/2021 prevê requisitos mínimos de segurança da informação, obrigatórios para órgãos e entidades da Administração Pública federal, porém que servem de parâmetro de boas práticas para qualquer organização que se preocupe com a segurança e a proteção dos dados e informações que trata. Essa norma traz uma série de medidas com vistas a proteger a confidencialidade, a integridade e a disponibilidade dos dados (*e.g.* definição de responsabilidades para os diferentes atores envolvidos na gestão da nuvem, gerenciamento de identidades e de registros/*logs*, adoção de criptografia), além de abordar a prevenção e a resposta a incidentes de segurança.

As questões desta seção, então, abordam aspectos atinentes à identificação dos dados pessoais que são compartilhados com terceiros, à devida avaliação e adequação dessas operações frente aos critérios previstos na LGPD, em especial nos arts. 26 (finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos/entidades públicos, respeitados, ainda, os princípios de proteção de dados pessoais elencados no art. 6º) e 27 (compartilhamento de dados pessoais com pessoa de direito privado), ao registro dos eventos relacionados a esses compartilhamentos (quais dados foram compartilhados, com quem foram compartilhados e quando foram compartilhados), às transferências internacionais de dados pessoais e ao tratamento de dados pessoais em solução de computação em nuvem.

Referências úteis:

- Lei 13.709/2018, art. 5º, inciso XVI, arts. 26-27 e 30, arts. 33-36 e 39, arts. 44 e 50, § 2º, inciso I, alínea “d” (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm));

- IN GSI/PR 5/2021 (Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da APF), em especial arts. 17 e 18 (https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684 (https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684));

- ABNT NBR ISO/IEC 27701:2019, itens 7.5.1 (Identificando as bases para a transferência de dados pessoais entre jurisdições), 7.5.2 (Países e organizações internacionais para os quais os dados pessoais podem ser transferidos), 7.5.3 (Registros de transferência de dados pessoais) e 7.5.4 (Registro de divulgação de dados pessoais para terceiros);

- Guia Orientativo – Tratamento de dados pessoais pelo Poder Público (https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf (https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf)).

8.1 (TIPO A) Quanto aos compartilhamentos de dados pessoais com terceiros, a organização: *

Favor escolher apenas uma das opções a seguir:

◯ Não se aplica (justificar no campo de comentário)

◯ AINDA NÃO AVALIOU se os realiza ou AINDA NÃO IDENTIFICOU todos os dados eventualmente compartilhados

◯ AVALIOU se há esses compartilhamentos e, nos casos detectados, IDENTIFICOU todos os dados eventualmente compartilhados

◯ IDENTIFICOU todos os dados pessoais compartilhados com terceiros e INICIOU A AVALIAÇÃO desses compartilhamentos, porém ainda não pode atestar que todos estejam em conformidade com os critérios legais (LGPD, arts. 26-27)

◯ IDENTIFICOU todos os dados pessoais compartilhados, AVALIOU os compartilhamentos e ATESTA que todos ESTÃO EM CONFORMIDADE COM OS CRITÉRIOS LEGAIS (LGPD, arts. 26-27), apesar de ainda não manter registro dos eventos relacionados a cada compartilhamento

◯ IDENTIFICOU todos os dados pessoais compartilhados, AVALIOU os compartilhamentos, ATESTA que todos ESTÃO EM CONFORMIDADE COM OS CRITÉRIOS LEGAIS (LGPD, arts. 26-27), DISPONIBILIZA INFORMAÇÕES acerca do uso compartilhado de dados e sua finalidade (art. 9º, inciso V) e MANTÉM REGISTRO DETALHADO dos eventos relacionados a cada compartilhamento, incluindo a identificação de quais dados foram compartilhados, com quem foram compartilhados e quando foram compartilhados

Comente aqui sua escolha:

Help: **Questão TIPO A:**

Esta questão permite a marcação de uma única opção de resposta, sendo que as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação às práticas e aos controles envolvidos. No caso, o respondente deve assinalar qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização.

Além de marcar a opção que melhor reflete a situação da sua organização em relação ao tópico questionado, o gestor **DEVE** complementar textualmente a sua resposta, no respectivo campo de comentário (que aceita texto aberto). Caso marque a opção “Não se aplica”, o gestor deve justificar nesse campo o seu entendimento pela não aplicação daquela medida/controle à sua organização. Caso marque alguma das demais opções de resposta, o gestor deve fornecer nesse campo detalhes que permitam compreender melhor a escolha por aquela opção, considerando o contexto específico da sua organização. Por exemplo, o gestor deve utilizar esse campo para descrever, quando aplicável, datas, períodos, responsáveis, projetos e iniciativas, bem como referenciar artefatos, evidências, atas e outros documentos internos, indicando os respectivos nomes, datas e números de identificação, se houver. A qualquer momento, inclusive após encerrado o prazo para o preenchimento do questionário, os auditores poderão requisitar informações adicionais, bem como o envio desses elementos (artefatos, evidências, atas, documentos) eventualmente mencionados pelo gestor.

8.1.1 (TIPO A) A organização realiza transferência internacional de dados pessoais? *

Só responder essa pergunta sob as seguintes condições:
((Q81.NAOK (/pesquisas/index.php/questionAdministration/view/surveyid/542191/gid/420/qid/10346) == 'A3' or Q81.NAOK (/pesquisas/index.php/questionAdministration/view/surveyid/542191/gid/420/qid/10346) == 'A4' or Q81.NAOK (/pesquisas/index.php/questionAdministration/view/surveyid/542191/gid/420/qid/10346) == 'A5' or Q81.NAOK (/pesquisas/index.php/questionAdministration/view/surveyid/542191/gid/420/qid/10346) == 'A6'))

Favor escolher apenas uma das opções a seguir:

◯ Até o momento, não foi identificada transferência internacional de dados, porém a organização AINDA NÃO AVALIOU TODOS OS CASOS de compartilhamento de dados pessoais

◯ Todos os compartilhamentos foram avaliados e NÃO HÁ transferência internacional de dados

◯ Todos os compartilhamentos foram avaliados e HÁ TRANSFERÊNCIA INTERNACIONAL DE DADOS

Comente aqui sua escolha:

Questão TIPO A:

Esta questão permite a marcação de uma única opção de resposta, sendo que as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação às práticas e aos controles envolvidos. No caso, o respondente deve assinalar qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização.

Além de marcar a opção que melhor reflete a situação da sua organização em relação ao tópico questionado, o gestor **DEVE** complementar textualmente a sua resposta, no respectivo campo de comentário (que aceita texto aberto). Caso marque a opção “Não se aplica”, o gestor deve justificar nesse campo o seu entendimento pela não aplicação daquela

medida/controle à sua organização. Caso marque alguma das demais opções de resposta, o gestor deve fornecer nesse campo detalhes que permitam compreender melhor a escolha por aquela opção, considerando o contexto específico da sua organização. Por exemplo, o gestor deve utilizar esse campo para descrever, quando aplicável, datas, períodos, responsáveis, projetos e iniciativas, bem como referenciar artefatos, evidências, atas e outros documentos internos, indicando os respectivos nomes, datas e números de identificação, se houver. A qualquer momento, inclusive após encerrado o prazo para o preenchimento do questionário, os auditores poderão requisitar informações adicionais, bem como o envio desses elementos (artefatos, evidências, atas, documentos) eventualmente mencionados pelo gestor.

8.1.1.1 (TIPO A) As transferências internacionais de dados pessoais estão de acordo com os princípios, direitos e requisitos previstos na LGPD, em especial no art. 33? *

Só responder essa pergunta sob as seguintes condições:
((Q811.NAOK (/pesquisas/index.php/questionAdministration/view/surveyid/542191/gid/420/qid/10349) == 'A3'))

Favor escolher apenas uma das opções a seguir:

◯ A organização AINDA NÃO AVALIOU os princípios, direitos e requisitos previstos na LGPD, em especial no art. 33, em relação a todos os casos de transferência internacional de dados

◯ Todos os casos de transferência internacional de dados foram avaliados, porém AINDA NÃO ATENDEM integralmente os requisitos legais (LGPD, em especial art. 33)

◯ Todos os casos de transferência internacional de dados foram avaliados e ATENDEM INTEGRALMENTE OS REQUISITOS LEGAIS (LGPD, em especial art. 33)

Comente aqui sua escolha:

Questão TIPO A:

Esta questão permite a marcação de uma única opção de resposta, sendo que as diferentes opções disponíveis refletem um aumento gradativo da maturidade da organização em relação às práticas e aos controles envolvidos. No caso, o respondente deve assinalar qual, dentre as opções disponíveis, melhor reflete a situação atual da sua organização.

Além de marcar a opção que melhor reflete a situação da sua organização em relação ao tópico questionado, o gestor **DEVE** complementar textualmente a sua resposta, no respectivo campo de comentário (que aceita texto aberto). Caso marque a opção “Não se aplica”, o gestor deve justificar nesse campo o seu entendimento pela não aplicação daquela medida/controle à sua organização. Caso marque alguma das demais opções de resposta, o gestor deve fornecer nesse campo detalhes que permitam compreender melhor a escolha por aquela opção, considerando o contexto específico da sua organização. Por exemplo, o gestor deve utilizar esse campo para descrever, quando aplicável, datas, períodos, responsáveis, projetos e iniciativas, bem como referenciar artefatos, evidências, atas e outros documentos internos, indicando os respectivos nomes, datas e números de identificação, se houver. A qualquer

momento, inclusive após encerrado o prazo para o preenchimento do questionário, os auditores poderão requisitar informações adicionais, bem como o envio desses elementos (artefatos, evidências, atas, documentos) eventualmente mencionados pelo gestor.

8.1.2 (TIPO B) Acerca de tratamento de dados pessoais em solução de computação em nuvem (*cloud computing*), a organização: *

Por favor, escolha as opções que se aplicam:

☐ REALIZA O TRATAMENTO DE DADOS PESSOAIS EM NUVEM (ainda que apenas armazenamento)

☐ Avaliou e PODE ASSEGURAR QUE NÃO HÁ ARMAZENAMENTO DE DADOS PESSOAIS EM TERRITÓRIO ESTRANGEIRO

☐ Realizou AVALIAÇÃO DE RISCOS relativamente a esse tratamento, amparada em análise e em relatório de impacto que foram devidamente submetidos à apreciação das instâncias competentes

☐ INCLUIU, NOS INSTRUMENTOS CONTRATUAIS COM OS PROVEDORES DE NUVEM, CLÁUSULAS e mecanismos que garantem, ao menos, o sigilo dos dados no armazenamento e em trânsito, a não transferência dos dados a terceiros, a remoção incondicional dos dados após o término do contrato e a não utilização dos dados, para quaisquer fins, pelo provedor ou por terceiros

☐ NÃO REALIZA NENHUM TRATAMENTO DE DADOS PESSOAIS EM NUVEM

Questão TIPO B:

Esta questão permite a marcação de múltiplas opções de resposta. No caso, o respondente deve marcar todas as opções que são atendidas pela sua organização.

9. Violação de dados pessoais

9. Violação de dados pessoais

Como parte do seu processo de gestão de incidentes de segurança da informação, convém que a organização estabeleça papéis, responsabilidades e procedimentos específicos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança que envolvem a violação de dados pessoais.

Convém, ainda, que a organização possua um sistema de informação de gestão de incidentes próprio/adequado para registrar tanto os incidentes em si quanto o histórico de todas as ações adotadas para solucioná-los/tratá-los, desde a eventual adoção inicial de uma solução de contorno, previamente à atuação para efetivamente analisar e erradicar as causas-raízes do incidente.

Ademais, tendo em vista que a identificação/detecção precoce pode diminuir significativamente os impactos causados por esses incidentes, a organização deve adotar mecanismos para monitorar proativa e continuamente os eventos que podem sinalizar (sinais precursores e indicadores) a ocorrência de incidentes de segurança associados à violação de dados pessoais, de modo que seja capaz de agir rapidamente nesses casos.

Por fim, a organização deve comunicar tanto à Autoridade Nacional de Proteção de Dados (ANPD) quanto ao(s) próprio(s) titular(es) de dados a ocorrência de incidente de segurança da informação que possa acarretar risco ou dano relevante a estes últimos. Essa notificação deve ser feita no prazo de 3 (três) dias úteis e mencionar, entre outras coisas: a descrição da natureza e da categoria dos dados pessoais afetados; as informações sobre os titulares afetados, incluindo seu número e a discriminação de crianças, adolescentes e idosos, se houver; a indicação das medidas técnicas e de segurança adotadas para a proteção dos dados, antes e após o incidente; os riscos relacionados ao incidente; as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares; a data da ocorrência do incidente e a de seu conhecimento pelo controlador; os dados do encarregado; a descrição do incidente, incluindo sua causa. Caso a organização não encaminhe a comunicação tempestivamente, deverá expor, também, os motivos que levaram à demora (Resolução CD/ANPD 15/2024, art. 6º).

A questão desta seção, então, aborda aspectos atinentes à identificação, ao registro e ao tratamento/resposta a incidentes de segurança da informação que envolvem a violação de dados pessoais, bem como à existência de mecanismos e procedimentos padronizados para notificação da ANPD e dos titulares de dados envolvidos nos casos de incidentes que possam representar risco ou causar dano relevante aos titulares.

Referências úteis:

- Lei 13.709/2018, arts. 48 e 50, § 2º, inciso I, alínea “g” (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm));

- Resolução CD/ANPD 15/2024 (Regulamento de Comunicação de Incidente de Segurança), em especial arts. 6º-10 (https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024 (https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024));

- ABNT NBR ISO/IEC 27701:2019, itens 6.13.1.1 (Responsabilidades e procedimentos), 6.13.1.4 (Avaliação e decisão dos eventos de segurança da informação) e 6.13.1.5 (Resposta aos incidentes de segurança da informação).

9.1 (TIPO B) A organização: *

Por favor, escolha as opções que se aplicam:

☐ Elaborou e mantém atualizado PLANO DE RESPOSTA A INCIDENTES (ou documento similar), sendo que abordou nesse documento questões específicas relacionadas ao tratamento/resposta a incidentes de segurança da informação que envolvem violação de dados pessoais

☐ REGISTRA TODOS OS INCIDENTES de segurança da informação que envolvem violação de dados pessoais em sistema próprio/adequado a esse propósito

☐ Sempre registra no sistema próprio/adequado a esse propósito TODAS AS AÇÕES QUE FORAM ADOTADAS PARA TRATAR/RESPONDER AO INCIDENTE de segurança da informação que envolve violação de dados pessoais, incluindo a eventual adoção de solução de contorno em um primeiro momento

☐ MONITORA PROATIVA E CONTINUAMENTE a ocorrência de eventos (sinais precursores e indicadores) que podem ser associados a incidentes de segurança da informação que envolvem violação de dados pessoais

☐ Estabeleceu e executa PROCEDIMENTOS PADRONIZADOS PARA COMUNICAR À ANPD E AO TITULAR DE DADOS a ocorrência de incidente de segurança da informação que possa acarretar risco ou dano relevante ao(s) titular(es)

☐ AINDA NÃO ATENDE NENHUM dos itens anteriores

Questão TIPO B:

Esta questão permite a marcação de múltiplas opções de resposta. No caso, o respondente deve marcar todas as opções que são atendidas pela sua organização.

9.1.1 Anexe o Plano de Resposta a Incidentes (ou documento similar) da organização:

Só responder essa pergunta sob as seguintes condições:
A resposta foi na questão ' [Q91]' (9.1 (TIPO B) A organização:)

Kindly attach the aforementioned documents along with the survey

Só é aceito o *upload* de um único arquivo no formato PDF, com tamanho máximo de 20MB.

10. Medidas de proteção

10. Medidas de proteção

A organização deve adotar amplas medidas de segurança, técnicas e administrativas com vistas a proteger os dados pessoais que trata de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46), sobretudo, se houver, os dados pessoais sensíveis (que envolvem origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico) e os dados pessoais de crianças e de adolescentes.

Para isso, convém, inclusive, que a organização defina claramente papéis, responsabilidades e procedimentos voltados à proteção desses dados e implemente controles específicos que sejam capazes de mitigar riscos que possam resultar em violações de privacidade. Entre tais controles, pode-se citar a definição de processo formal para registro e cancelamento de usuários nos sistemas que realizam tratamento de dados pessoais, de modo a viabilizar a atribuição dos direitos de acesso adequados nesses sistemas. O mesmo deve ser feito com o processo de provisionamento para conceder ou revogar os direitos de acesso, os quais devem observar os princípios de "necessidade de conhecer" (o colaborador só deve ter permissão para acessar informações que necessita para desempenhar suas tarefas) e "necessidade de uso" (o colaborador só deve ter permissão para acessar recursos de TI [*e.g.* equipamentos, aplicações, procedimentos, salas] que necessita para desempenhar suas tarefas).

Adicionalmente, convém que a organização registre e monitore os eventos (*logs*) relacionados às atividades de tratamento de dados pessoais, de forma que seja possível identificar por quem, quando e quais dados pessoais foram acessados. Nos casos em que ocorrerem mudanças nos dados, também deve ser registrada a ação realizada (*e.g.* inclusão, alteração ou exclusão). Convém, ainda, que a organização faça uso de soluções criptográficas para proteger de acessos indevidos os dados pessoais armazenados (em repouso) e quando estes estiverem trafegando (em trânsito), seja na rede interna da organização ou mesmo na Internet (durante o envio para um servidor na nuvem, por exemplo).

A organização também deve fornecer aos seus colaboradores diretrizes e orientações a respeito do uso de técnicas e ferramentas tecnológicas capazes de anonimizar, pseudonimizar, ocultar, mascarar e/ou tarjar dados pessoais, em especial no que se refere a temas transversais e comuns das organizações públicas (*e.g.* licitações, contratos, gestão de recursos humanos), o que atua para evitar a negação indevida de pedidos de acesso solicitados com base na LAI, com prejuízo à transparência das informações e ao controle social da Administração Pública.

Por fim, a organização deve assegurar que seus processos e sistemas sejam projetados, desde a concepção, de forma que os tratamentos de dados pessoais associados estejam limitados ao que é estritamente necessário para o alcance das finalidades pretendidas (*Privacy by Design* e *Privacy by Default*).

A questão desta seção, então, aborda aspectos atinentes à implementação de controles adequados para proteger os dados pessoais e mitigar o risco de violação, a exemplo da restrição e do rastreamento das atividades e dos acessos aos sistemas que realizam o tratamento desses dados, da utilização de criptografia para evitar acessos indevidos (seja aos

dados armazenados ou mesmo em trânsito), do uso de técnicas e ferramentas de mascaramento/ocultação/tarjamento de dados pessoais e da concepção de processos e sistemas que estejam conformes com a LGPD.

Referências úteis:

- Lei 12.527/2011, arts. 3º e 7º, § 2º, arts. 10-14, e arts. 31 e 40 (https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm (https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm));

- Lei 13.709/2018, art. 13, § 4º, arts. 44 e 46, em especial § 2º, e arts. 49 e 50, § 2º, inciso I, alíneas “c” e "d" (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm));

- Decreto 7.724/2012, arts. 11-20, 55, 57, 58, inciso III, e arts. 67 e 68 (https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm (https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm));

- Portaria Normativa CGU 71/2023 (Aprova enunciados referentes à aplicação da Lei nº 12.527, de 18 de novembro de 2011), em especial Enunciado 12 (https://www.in.gov.br/en/web/dou/-/portaria-normativa-cgu-n-71-de-10-de-abril-de-2023-477406468 (https://www.in.gov.br/en/web/dou/-/portaria-normativa-cgu-n-71-de-10-de-abril-de-2023-477406468));

- ABNT NBR ISO/IEC 27002:2013, item 6.1 (Organização interna), em especial item 6.1.1 (Responsabilidades e papéis pela segurança da informação);

- ABNT NBR ISO/IEC 27701:2019, itens 6.6.2.1 (Registro e cancelamento de usuário), 6.6.2.2 (Provisionamento para acesso de usuário), 6.7 (Criptografia), 6.9.4.1 (Registros de eventos [logs]) e 7.4 (*Privacy by Design* e *Privacy by Default*).

10.1 (TIPO B) A organização: *

Por favor, escolha as opções que se aplicam:

☐ Disponibiliza aos colaboradores FERRAMENTA/SOLUÇÃO TECNOLÓGICA PARA REALIZAÇÃO DO MASCARAMENTO/OCULTAÇÃO/TARJAMENTO em documentos de interesse coletivo ou geral que contenham dados pessoais;

☐ Possui NORMA(S) INTERNA(S) que orientam os colaboradores quanto à obrigatoriedade do uso de MASCARAMENTO/OCULTAÇÃO/TARJAMENTO em documentos de interesse coletivo ou geral que contenham dados pessoais, de modo a possibilitar dar acesso a tais documentos sem comprometer esses dados;

☐ Utiliza criptografia para proteger os dados pessoais quando estes estão em trânsito na rede interna da organização ou na Internet, ou seja, a chamada CRIPTOGRAFIA DE PONTA-A-PONTA

☐ Utiliza criptografia para proteger os dados pessoais quando estes estão em repouso, ou seja, a chamada CRIPTOGRAFIA DE ARMAZENAMENTO

☐ Adota medidas para assegurar que seus processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD (PRIVACY BY DESIGN E PRIVACY BY DEFAULT)

☐ AINDA NÃO ATENDE NENHUM dos itens anteriores

☐ É capaz de comprovar que ADOTA AMPLAS MEDIDAS DE SEGURANÇA, TÉCNICAS E ADMINISTRATIVAS aptas a proteger os dados pessoais que trata, tendo, inclusive, definido e atribuído papéis, responsabilidades e procedimentos específicos com esse propósito

☐ Implementou PROCESSO FORMAL PARA REGISTRO, CANCELAMENTO E PROVISIONAMENTO DE USUÁRIOS nos sistemas que realizam tratamento de dados pessoais

☐ REGISTRA E MONITORA EVENTOS (LOGS) relacionados às atividades de tratamento de dados pessoais

Questão TIPO B:

Esta questão permite a marcação de múltiplas opções de resposta. No caso, o respondente deve marcar todas as opções que são atendidas pela sua organização.

11. Questões finais

11. Questões finais

OBSERVAÇÃO 1: Ao gestor, é relevante compreender cada uma das nove dimensões avaliadas nesta auditoria (Preparação; Contexto organizacional; Liderança; Capacitação; Conformidade do tratamento; Direitos do titular; Compartilhamento de dados pessoais; Violação

de dados pessoais; e Medidas de proteção), bem como as subpráticas específicas que foram questionadas no bojo de cada uma dessas dimensões. Deste modo, o gestor pode se programar para, ao longo dos próximos meses/anos, implementar na sua organização as medidas e controles faltantes, frisando-se que o questionário não contempla todas as medidas e controles possíveis de serem implementados para a adequação das organizações à LGPD.

OBSERVAÇÃO 2: A ação do controle interno/auditoria interna é muito importante para que as leis, as normas gerais e as normas internas sejam efetivamente observadas, bem como para avaliar riscos em relação aos processos de trabalho da organização. No âmbito do Poder Executivo federal, as instâncias do sistema de controle interno, nos órgãos estrito senso, são as Assessorias Especiais de Controle Interno (AECI) e, nos outros tipos de organizações, são as auditorias internas, conforme estabelecem o Decreto 3.591/2000 (https://www.planalto.gov.br/ccivil_03/decreto/d3591.htm (https://www.planalto.gov.br/ccivil_03/decreto/d3591.htm)) e as Instruções Normativas CGU 3/2017 (https://repositorio.cgu.gov.br/handle/1/33409 (https://repositorio.cgu.gov.br/handle/1/33409)) e 13/2020 (https://repositorio.cgu.gov.br/handle/1/44989 (https://repositorio.cgu.gov.br/handle/1/44989)).

Q11.1 (TIPO B) Nos últimos 3 (três) anos, a instância do “sistema de controle interno governamental” da organização realizou avaliação relacionada com o tema:

Por favor, escolha as opções que se aplicam:

☐ PROTEÇÃO DE DADOS PESSOAIS (Lei Geral de Proteção de Dados Pessoais – LGPD)

☐ TRANSPARÊNCIA DA GESTÃO relativa às informações de interesse coletivo ou geral (Lei de Acesso à Informação – LAI)

☐ AINDA NÃO FOI REALIZADA AVALIAÇÃO DE NENHUM DESSES TEMAS (LGPD ou LAI)

Questão TIPO B:

Esta questão permite a marcação de múltiplas opções de resposta. No caso, o respondente deve marcar todas as opções que são atendidas pela sua organização.

No caso de ente público estadual, municipal ou federal de outro Poder que não o Executivo, favor responder em relação à instância que desempenha o papel de controle interno/auditoria interna da organização, ou que mais se aproxima desse papel.

Q11.2 (texto aberto) Por favor, registre aqui os principais desafios, deficiências e pontos de atenção relacionados à adequação da sua organização à LGPD, bem como quaisquer outras considerações, comentários ou críticas que considerar pertinentes:

Por favor, coloque sua resposta aqui:

ATENÇÃO:

CONFIRA TODAS AS SUAS RESPOSTAS ANTES DE CLICAR NO BOTÃO "ENVIAR".

Caso ainda exista alguma pendência ou dúvida, utilize a opção "Retomar mais tarde" (localizada no canto superior direito da página) para salvar as respostas fornecidas até então. Desse modo, até 12/7/2024 (sexta-feira), por meio do mesmo código de acesso (*token*: {TOKEN:TOKEN}), é possível retornar para alterar ou complementar as respostas fornecidas.

Ao final, depois do envio, aparecerá, na página de confirmação, uma opção para salvar/imprimir as respostas. Entretanto, alertamos que **ESSA OPÇÃO SÓ APARECE NESSE MOMENTO** e não será possível acessar o questionário após o dia 12/7/2024 para ver ou imprimir as respostas enviadas.

Esta Corte de Contas agradece a sua participação.
12/07/2024 – 23:59

Enviar questionário
Obrigado por ter preenchido o questionário.