O TCE-RJ, por meio da Coordenadoria Setorial de Auditoria em Políticas de Tecnologia da Informação (CAS-TI), está realizando auditoria para avaliar a adequação das entidades e órgãos públicos do Estado do Rio de Janeiro em relação à Lei 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD).

O questionário desta auditoria é um instrumento de coleta de dados sobre as medidas implementados para assegurar a conformidade com a LGPD e deve ser preenchido pelas entidades e órgãos auditados.

<u>Observações importantes:</u>

1) O questionário não contempla todos os controles possíveis de serem implementados para a adequação das organizações à LGPD.

2) Há questões que abrangem controles que podem não ser aplicáveis a algumas organizações, devido ao contexto, ao porte ou aos objetivos institucionais.

3) As questões tiveram como referência a própria legislação, normas e boas práticas, principalmente a ABNT NBR ISO/IEC 27.701/2019 (extensão da ABNT NBR ISO/IEC 27.001 e ABNT NBR ISO/IEC 27.002 para gestão da privacidade da informação - Requisitos e diretrizes).

4) O presente questionário se baseia em trabalho desenvolvido pelo TCU (processo TCU n° 039.606/2020-1) com mesmo propósito, de modo a viabilizar a comparação dos dados a serem obtidos pelas respectivas auditorias.

5) O questionário envolve a solicitação de informações e, em casos pontuais, solicita o envio de arquivos para evidenciarem as respostas fornecidas. É importante destacar que o envio dos arquivos é obrigatório. A não inclusão de arquivos, quando solicitado, impedirá o respondente de avançar para o próximo grupo de questões.

6) Ressalta-se que as evidências documentais que não foram solicitadas pelo presente questionário deverão ser armazenadas e mantidas para futura verificação do TCE-RJ.

7) Aconselha-se que o questionário seja preenchido assim que recebido, pois solicitações de esclarecimentos (que devem ser encaminhadas para o e-mail auditoria_lgpd@tcerj.tc.br) podem não ser respondidas tempestivamente caso a solicitação seja enviada em data próxima ao limite de entrega do questionário, devido ao elevado volume de dúvidas que costumam ser enviadas nesse período.

8) 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) estiverem preenchidas. O botão "Sair e

Seção A: Seção A - Preparação

Antes de iniciar o processo de adequação à LGPD, a organização deve adotar medidas para construir um ambiente propício para o sucesso da iniciativa.

As questões desta seção abordam aspectos relacionados à identificação e ao planejamento das medidas necessárias à adequação.

A1. A organização conduziu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD?

Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I. ABNT NBR ISO/IEC 27.701/2019, item 5.4.

A organização deve conduzir iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD. Um exemplo de iniciativa pode ser a instituição de comitê ou grupo de trabalho. É importante que a iniciativa conte com o apoio ou, até mesmo, com a participação direta da alta direção da organização. Ademais, convém que sejam envolvidas pessoas pertencentes a unidades que exercem atividades relevantes para o tratamento de dados pessoais (e.g.: Segurança da Informação, Tecnologia da Informação, Direito, Auditoria/Conformidade e Ouvidoria). Um exemplo de artefato que pode ser produzido pela iniciativa é o plano de ação.

- [ ] Sim (a organização concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD).
- [x] Parcialmente (a organização iniciou, mas ainda não concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD).
- [ ] Não

A2. A organização elaborou plano de ação, plano de projeto ou documento similar para direcionar a iniciativa de adequação à LGPD?

Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I. ABNT NBR ISO/IEC 27.701/2019, item 5.4.

A organização deve documentar informações relacionadas aos objetivos da iniciativa de adequação e às ações necessárias para alcançá-los.

- [x] Sim
- [ ] Não

A3. Anexe o plano de ação, plano de projeto ou documento similar que foi elaborado pela organização:

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

Seção B: Seção B - Contexto Organizacional

Para alcançar os resultados pretendidos pela iniciativa de adequação à LGPD, a organização deve avaliar questões internas e externas que são relevantes para atingir os objetivos.

As questões desta seção abordam aspectos relacionados à identificação de normativos correlatos à proteção de dados pessoais que devem ser respeitados pela organização, à identificação das partes interessadas e à análise dos dados pessoais tratados pela organização e dos processos organizacionais que tratam esses dados.

B1. A organização conduziu iniciativa para identificar outros normativos (e.g.: leis, regulamentos e instruções normativas), além da LGPD, que abrangem comandos relacionados à proteção de dados pessoais e que também devem ser respeitados?

Referência(s): ABNT NBR ISO/IEC 27.701/2019, item 5.2.1.

Além da LGPD, há outros normativos que abordam o tratamento de dados pessoais e que também devem ser respeitados por determinadas organizações. O Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Consolidação das Leis Trabalhistas (CLT), a Lei de Acesso à Informação e a Lei 13.787/2018 (que dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente) são alguns exemplos desses normativos.

- [x] Sim
- [ ] Não

B2. A organização identificou as categorias de titulares de dados pessoais com os quais se relaciona?

Referência(s): Lei 13.709/2018, art. 5º, inciso V. ABNT NBR ISO/IEC 27.701/2019, itens 6.5.2 e 7.2.8.

Convém que a organização identifique as partes interessadas que possuem interesses ou responsabilidades associados ao tratamento de dados pessoais, o que pode abranger, por exemplo: titulares de dados pessoais, operadores e controladores conjuntos. O titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Os titulares podem ser enquadrados em diferentes categorias como: cidadão, cliente, servidor público, representante de fornecedor e terceirizado.

- [ ] Sim (todas as categorias de titulares de dados pessoais foram identificadas)
- [ ] Parcialmente (algumas categorias de titulares de dados pessoais foram identificadas)
- [x] Não (ainda não foi conduzida iniciativa para identificar as categorias de titulares de dados pessoais)

B3. A organização conduziu iniciativa para identificar os operadores que realizam tratamento de dados pessoais em seu nome?

Referência(s): Lei 13.703/2018, art. 5º, incisos VI e VII. ABNT NBR ISO/IEC 27.701/2019, item 5.2.2.

Convém que a organização identifique as partes interessadas que possuem interesses ou responsabilidades associados ao tratamento de dados pessoais, o que pode abranger, por exemplo: titulares de dados pessoais, operadores e controladores conjuntos. O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Este, por sua vez, é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

- [ ] Sim (a iniciativa foi concluída e todos os operadores foram identificados)
- [ ] Sim (a iniciativa foi concluída e a organização constatou que não há operadores que realizam tratamentos de dados pessoais em seu nome)
- [x] Parcialmente (a iniciativa ainda está em andamento)
- [ ] Não (ainda não foi conduzida iniciativa para identificar os operadores)

B4. A organização adequou os contratos firmados com os operadores identificados de forma a estabelecer suas responsabilidades e papéis com relação à proteção de dados pessoais?

Referência(s): Lei 13.709/2018, art. 39; arts. 42-46. ABNT NBR ISO/IEC 27.701/2019, item 7.2.6.

O controlador deve ter contrato firmado com os operadores de dados pessoais para assegurar que estes adotem medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais que são compartilhados com eles.

- [ ] Sim (A organização adequou todos os contratos firmados com os operadores que foram identificados)
- [ ] Parcialmente (A organização adequou os contratos firmados com alguns operadores que foram identificados)
- [x] Não (A organização não adequou os contratos firmados com os operadores que foram identificados)

B5. A organização já realizou uma adequação dos instrumentos convocatórios que estão sendo elaborados, estabelecendo responsabilidades e papéis dos operadores com relação à proteção de dados pessoais?

Referência(s): Lei 13.709/2018, art. 39; arts. 42-46. ABNT NBR ISO/IEC 27.701/2019, item 7.2.6.

O controlador deve ter contrato firmado com os operadores de dados pessoais para assegurar que estes adotem medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais que são compartilhados com eles.

- [ ] Sim
- [x] Não

B6. A organização avaliou se há tratamento de dados que envolva controlador conjunto?

Referência(s): Lei 13.709/2018, art. 5º, inciso VI; art. 7º, § 5º. ABNT NBR ISO/IEC 27.701/2019, itens 5.2.2 e 7.2.7.

Convém que a organização identifique as partes interessadas que possuem interesses ou responsabilidades associados ao tratamento de dados pessoais, o que pode abranger, por exemplo: titulares de dados pessoais, operadores e controladores conjuntos. O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Por sua vez, controlador conjunto é o controlador de dados pessoais que determina os propósitos e as formas do tratamento de dados pessoais junto com outro(s) controlador(es).

- [ ] Sim
- [x] Não

B7. Caso exista controlador conjunto, os papéis e responsabilidades de cada um dos controladores estão definidos em contrato, acordo de cooperação ou instrumento similar?

Referência(s): Lei 13.709/2018, arts. 42-45. ABNT NBR ISO/IEC 27.701/2019, item 7.2.7.

É conveniente que a organização estabeleça formalmente os papéis e as responsabilidades de cada controlador caso haja controlador conjunto. Caso não haja tratamento de dados que envolva controlador conjunto, assinale a alternativa "não se aplica".

- [ ] Sim (os papéis e responsabilidades de cada um dos controladores estão definidos em contrato, acordo de cooperação ou instrumento similar)
- [ ] Parcialmente (há acordo de cooperação ou instrumento similar firmado, mas nem todos os papéis e responsabilidades de cada um dos controladores estão definidos)
- [ ] Não (os papéis e responsabilidades de cada um dos controladores não estão definidos em contrato, acordo de cooperação ou instrumento similar)
- [ ] Não se aplica (não há relação da organização com controlador conjunto)

B8. A organização identificou os processos de negócio que realizam tratamento de dados pessoais?

Referência(s): Lei 13.709/2018, art. 37. ABNT NBR ISO/IEC 27.701/2019, item 7.2.8.

O tratamento de dados pessoais envolve toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

- Sim (todos os processos de negócio que realizam tratamento de dados pessoais foram identificados) ☐
- Parcialmente (alguns processos de negócio que realizam tratamento de dados pessoais foram identificados) ☒
- Não (ainda não foi conduzida iniciativa para identificar os processos de negócio que realizam tratamento de dados pessoais) ☐

B9. A organização identificou quem são os responsáveis pelos processos de negócio que realizam tratamento de dados pessoais que já foram identificados?

Referência(s): Lei 13.709/2018, art. 37. ABNT NBR ISO/IEC 27.701/2019, item 7.2.8.

Os responsáveis pelo tratamento de dados pessoais podem abranger, por exemplo, pessoas, departamentos, operadores e controlador(es) conjunto(s).

- Sim (a organização identificou os responsáveis por todos os processos de negócio que realizam tratamento de dados pessoais e que já foram identificados) ☐
- Parcialmente (a organização identificou os responsáveis por alguns dos processos de negócio que realizam tratamento de dados pessoais e que já foram identificados) ☒
- Não (a organização não identificou os responsáveis pelos processos de negócio que realizam tratamento de dados pessoais e que já foram identificados) ☐

B10. A organização identificou quais são os dados pessoais tratados por ela?

Referência(s): Lei 13.709/2018, art. 5º, inciso I; art. 37. ABNT NBR ISO/IEC 27.701/2019, itens 6.5.2 e 7.2.8.

O dado pessoal é uma informação relacionada à pessoa natural identificada ou identificável, como nome, RG e CPF.

- Sim (todos os dados pessoais tratados pela organização foram identificados) ☐
- Parcialmente (alguns dados pessoais tratados pela organização foram identificados) ☒
- Não (a organização não identificou os dados pessoais que são tratados por ela) ☐

B11. A organização identificou os locais onde os dados pessoais identificados são armazenados?

Referência(s): Lei 13.709/2018, art. 5º, inciso I; art. 37. ABNT NBR ISO/IEC 27.701/2019, itens 6.5.1 e 7.2.8.

Os dados pessoais podem ser armazenados em ativos de TI (e.g.: servidor de arquivos, nuvem, dispositivo USB, storage, fita de backup) ou em arquivos físicos (e.g.: pastas e armários). As organizações também devem identificar o local (endereço) onde se encontram os dados.

- Sim (a organização identificou os locais onde são armazenados todos os dados pessoais que já foram identificados) ☐
- Parcialmente (a organização identificou os locais onde são armazenados alguns dos dados pessoais que já foram identificados) ☒
- Não (a organização não identificou os locais onde são armazenados os dados pessoais que já foram identificados) ☐

B12. A organização avaliou os riscos dos processos de tratamento de dados pessoais que foram identificados?

Critério(s): Lei 13.709/2018, art. 50, § 1º e § 2º, inciso I, alínea "d". ABNT NBR ISO/IEC 27.701/2019, item 5.4.1.2.

A organização deve avaliar os riscos associados aos processos que realizam tratamento de dados pessoais. Essa avaliação auxilia a organização a compreender as consequências e as probabilidades dos riscos para direcionar a definição de quais processos devem ser priorizados na iniciativa de adequação à LGPD.

- Sim ☐
- Não ☒

Seção C: Seção C - Liderança

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

A existência e a elaboração de políticas relacionadas à proteção de dados pessoais e a nomeação de um encarregado que tenha autonomia para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) são fundamentais para o processo de adequação.

As questões desta seção são relacionadas à nomeação do encarregado e à existência de políticas que buscam assegurar a segurança das informações e a proteção dos dados pessoais.

C1. A organização possui Política de Segurança da Informação ou instrumento similar?

Referência(s): Lei 13.709/2018, art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, itens 5.3.2 e 6.2.

Uma Política de Segurança da Informação estabelece a abordagem da organização para gerenciar os objetivos de segurança da informação. A referida política deve ser aprovada pela alta direção e estar de acordo com os requisitos de negócio e com leis e regulamentações aplicáveis.

- [x] Sim
- [ ] Não

C2. Anexe a Política de Segurança da Informação (ou instrumento similar) da organização:

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

C3. A organização possui Política de Classificação da Informação ou instrumento similar?

Referência(s): Lei 13.709/2018, art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, item 6.5.2.

Uma Política de Classificação da Informação deve fornecer diretrizes para assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.

- [ ] Sim
- [x] Não

C4. A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para a classificação de dados pessoais?

Referência(s): Lei 13.709/2018, art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, item 6.5.2.

A Política de Classificação da Informação deve considerar a classificação de dados pessoais para viabilizar a identificação de quais desses dados são tratados pela organização, o que é importante para direcionar a implementação de controles adequados para a proteção de dados pessoais.

- [ ] Sim
- [ ] Não

C5. A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para identificar dados pessoais sensíveis e relacionados a crianças e adolescentes?

Referência(s): Lei 13.709/2018, art. 5º, inciso II; art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, item 6.5.2.2.

O dado pessoal sensível é o dado pessoal sobre 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, quando vinculado a uma pessoa natural.

A LGPD demanda que sejam adotados cuidados específicos para o tratamento de dados pessoais sensíveis.

- [ ] Sim
- [ ] Não

C6. A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para identificar dados pessoais de crianças e de adolescentes?

Referência(s): Lei 13.709/2018, art. 14; art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, item 6.5.2.2.

A LGPD demanda que sejam adotados cuidados específicos para o tratamento de dados pessoais de crianças e de adolescentes.

Sim ☐

Não ☐

C7. Anexe a Política de Classificação da Informação (ou instrumento similar) da organização:

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

C8. A organização possui Política de Proteção de Dados Pessoais (ou instrumento similar)?

Referência(s): Lei 13.709/2018, art. 46; art. 50, § 2º, inciso I, alíneas "a" e "d". ABNT NBR ISO/IEC 27.701/2019, itens 6.2.1.

A Política de Proteção de Dados Pessoais deve estar alinhada com a Política de Segurança da Informação e com a Política de Classificação da Informação e provê apoio e comprometimento da organização para alcançar a conformidade com os normativos de proteção de dados pessoais.

A Política de Proteção de Dados Pessoais pode ser definida e publicada em documento específico ou incluída no texto da Política de Segurança da Informação já existente.

Vale ressaltar que a Política de Proteção de Dados Pessoais não se confunde com a Política de Privacidade. Enquanto a primeira é voltada para o público interno da organização, a segunda é direcionada para o público externo (e.g.: titulares de dados pessoais).

Sim ☐

Não ☒

C9. Anexe a Política de Proteção de Dados Pessoais (ou documento similar) da organização:

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

C10. A organização nomeou o encarregado pelo tratamento de dados pessoais?

Referência(s): Lei 13.709/2018, art. 5º, inciso VIII; art. 41. IN SGD/ME 117/2020. ABNT NBR ISO/IEC 27.701/2019, item 6.3.1.

O encarregado é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

O termo DPO (Data Protection Officer) é comumente utilizado para se referir ao encarregado.

Convém que o encarregado possua, além de profundo conhecimento da Lei 13.709/2018, conhecimentos relativos a temas como: Direito, Governança Corporativa, Gestão de Riscos, Tecnologia da Informação e Segurança da Informação.

Sim ☐

Não ☒

C11. A nomeação do encarregado foi publicada em veículo de comunicação oficial?

Referência(s): Lei 13.709/2018, art. 5º, inciso VIII; art. 41. IN SGD/ME 117/2020, art 2º. ABNT NBR ISO/IEC 27.701/2019, item 6.3.1.

A organização deve designar oficialmente o encarregado. Diante disso, é conveniente que a nomeação do encarregado seja publicada em veículo de comunicação oficial como o Diário Oficial da União (DOU).

Sim ☐

Não ☐

C12. Anexe a publicação da nomeação do encarregado de dados

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

C13. Em qual setor da organização está lotado o encarregado?

Referência(s): Lei 13.709/2018, art. 5º, inciso VIII; art. 41. IN SGD/ME 117/2020, art 1º, § 1º, inciso II. ABNT NBR ISO/IEC 27.701/2019, item 6.3.1.

O encarregado deve ser independente e ter liberdade para reportar à alta administração. É recomendável que o encarregado não faça parte de um setor no qual possa haver conflito de interesses.

- [ ] Tecnologia da Informação
- [ ] Jurídico
- [ ] Ouvidoria
- [ ] Auditoria/Controle Interno (compliance)
- [ ] Terceiro / Serviço Contratado
- [ ] Outros

Outros

C14. A identidade e as informações de contato do encarregado foram divulgadas na internet?

Referência(s): Lei 13.709/2018, art. 5º, inciso VIII; art. 41, § 1º. IN SGD/ME 117/2020, art 2º. ABNT NBR ISO/IEC 27.701/2019, item 6.3.1.

A identidade e as informações de contato (e.g.: e-mail, telefone) do encarregado devem ser divulgadas publicamente, preferencialmente no sítio eletrônico da organização.

- [ ] Sim
- [ ] Não

C15. Favor informar o endereço da internet (URL) onde foram divulgadas as informações de contato do encarregado

Seção D: Seção D - Capacitação

A organização deve conduzir iniciativas para conscientizar e capacitar os colaboradores em proteção de dados pessoais.

A conscientização é importante para que os colaboradores conheçam as políticas organizacionais relacionadas à proteção de dados pessoais e para que reconheçam como suas ações são importantes para a preservação da privacidade dos titulares.

As ações de capacitação devem considerar diferentes níveis de envolvimento dos colaboradores no tema, de forma que aqueles que ocupam funções com responsabilidades essenciais relacionadas à proteção de dados pessoais recebam treinamento diferenciado, além do nível básico fornecido aos demais.

Nesta seção são abordadas questões para avaliar o planejamento e a realização de ações de conscientização e de capacitação.

D1. A organização possui Plano de Capacitação (ou instrumento similar) que abrange treinamento e conscientização dos seus colaboradores em proteção de dados pessoais?

Referência(s): ABNT NBR ISO/IEC 27.701/2019, itens 5.5.2, 5.5.3 e 5.5.4.

É conveniente que a organização elabore um Plano de Capacitação que determine as competências necessárias para os recursos humanos envolvidos em atividades que realizam o tratamento de dados pessoais. O Plano de Capacitação deve mapear as lacunas de conhecimento associadas ao tema, bem como planejar ações de treinamento para redução dessas lacunas.

Ademais, é necessário que todas as pessoas da organização estejam cientes da importância do tema proteção de dados pessoais e dos impactos que podem ser causados devido à violação desses dados. Diante disso, é importante que o plano de capacitação também contemple ações de conscientização. Nada impede que a organização elabore um plano de conscientização apartado de um plano de treinamento.

- [ ] Sim
- [x] Não

D2. O Plano de Capacitação (ou instrumento similar) considera que pessoas que exercem funções com responsabilidades essenciais relacionadas à proteção de dados pessoais devem receber treinamento diferenciado?

Referência(s): ABNT NBR ISO/IEC 27.701/2019, itens 5.5.2, 5.5.3 e 5.5.4.

Por exemplo, recursos humanos envolvidos em atividades críticas relacionadas ao tratamento de dados pessoais devem receber treinamento além do nível básico fornecido aos demais colaboradores.

- [ ] Sim
- [ ] Não

D3. Anexe o Plano de Capacitação (ou instrumento similar) da organização.

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

D4. Colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema?

Referência(s): ABNT NBR ISO/IEC 27.701/2019, itens 5.5.2, 5.5.3 e 5.5.4.

Diante da vigência da LGPD, é conveniente que os colaboradores envolvidos diretamente em atividades que realizam o tratamento de dados pessoais já tenham participado de treinamentos correlatos ao tema.

- [ ] Sim (todos os colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema)
- [x] Parcialmente (alguns colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema)
- [ ] Não (nenhum dos colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema)

Seção E: Seção E - 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 pela LGPD são seguidos e que os tratamentos são fundamentados em, ao menos, uma das bases legais descritas na legislação.

Nesta seção são abordadas questões para avaliar se os tratamentos estão em conformidade com alguns dos princípios e se estão fundamentados em alguma base legal. Também será avaliado se a organização possui um registro para documentar detalhes das atividades de tratamento.

E1. A organização identificou e documentou as finalidades das atividades de tratamento de dados pessoais?

Referência(s): Lei 13.709/2018, art. 6º, inciso I. ABNT NBR ISO/IEC 27.701/2019, item 7.2.1.

As atividades de tratamento de dados pessoais devem ter propósitos legítimos, específicos, explícitos e informados ao titular. A organização deve assegurar que os titulares de dados pessoais entendam a(s) finalidade(s) pelas quais os seus dados pessoais são tratados.

- Sim (todas as finalidades das atividades de tratamento de dados pessoais foram identificadas e documentadas). ☐
- Parcialmente (algumas finalidades das atividades de tratamento de dados pessoais foram identificadas e documentadas). ☒
- Não (as finalidades das atividades de tratamento de dados pessoais ainda não foram identificadas e documentadas). ☐

E2. A organização avaliou se coleta apenas os dados estritamente necessários para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?

Referência(s): Lei 13.709/2018, art. 6º, incisos II e III. ABNT NBR ISO/IEC 27.701/2019, item 7.4.1.

Os dados pessoais coletados devem se limitar ao que é estritamente necessário para cumprir com as finalidades de tratamento.

- Sim ☐
- Não ☒

E3. A organização 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?

Referência(s): Lei 13.709/2018, art. 40. ABNT NBR ISO/IEC 27.701/2019, item 7.4.7.

A organização não deve reter dados pessoais por tempo maior do que o estritamente necessário.

- Sim ☐
- Não ☒

E4. A organização publica na internet as informações sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para o tratamento de dados pessoais?

- Sim ☐
- Não ☒

E5. Favor informar o endereço (URL) onde estão publicadas essas informações sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para o tratamento de dados pessoais.

E6. A organização identificou e documentou as bases legais que fundamentam as atividades de tratamento de dados pessoais?

Referência(s): Lei 13.709/2018 art. 7º. ABNT NBR ISO/IEC 27.701/2019, item 7.2.2.

A organização deve determinar e documentar as bases legais que fundamentam as atividades de tratamento de dados pessoais. As bases legais são relacionadas no art. 7º da Lei 13.709/2018: consentimento; cumprimento de obrigação legal ou regulatória; execução de políticas públicas pela Administração Pública; estudos por órgão de pesquisa; execução de contrato; exercício regular de direitos em processo judicial, administrativo ou arbitral; proteção da vida ou da incolumidade física; tutela da saúde; interesse legítimo; e proteção do crédito.

- Sim (as bases legais que fundamentam todas as atividades de tratamento de dados pessoais da organização foram definidas e documentadas). ☐
- Parcialmente (as bases legais que fundamentam algumas das atividades de tratamento de dados pessoais da organização foram definidas e documentadas). ☒
- Não (nenhuma base legal que fundamenta as atividades de tratamento de dados pessoais da organização foi definida e documentada). ☐

E7. Há um registro (e.g.: inventário) instituído para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais?

Referência(s): Lei 13.709/2018, art. 37. ABNT NBR ISO/IEC 27.701/2019, item 7.2.8.

Uma maneira de reter os registros das características das atividades de tratamento de dados pessoais é por meio de um inventário, o qual pode contemplar, por exemplo: finalidade do tratamento; base legal que fundamenta o tratamento; descrição das categorias dos titulares de dados pessoais envolvidos no tratamento; dados pessoais coletados; tempo de retenção dos dados; local de armazenamento dos dados; responsável pelo processo de tratamento; e medidas de segurança adotadas.

- Sim ☐
- Não ☒

E8. Anexe o arquivo que representa o registro das atividades de tratamento de dados pessoais (e.g.: inventário).

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

E9. A organização elaborou Relatório de Impacto à Proteção de Dados Pessoais?

Referência(s): Lei 13.709/2018, art. 5º, inciso XVII; art. 38. ABNT NBR ISO/IEC 27.701/2019, item 7.2.5.

O Relatório de Impacto à Proteção de Dados Pessoais é uma documentação do controlador que contempla a descrição dos processos de tratamento de dados pessoais que podem gerar riscos aos titulares e das medidas adotadas para tratamento desses riscos.

O relatório deve 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 da organização quanto às medidas, salvaguardas e mecanismos de mitigação de riscos.

- Sim (a organização elaborou Relatório de Impacto à Proteção de Dados Pessoais que abrange TODOS os processos de tratamento de dados pessoais que podem gerar riscos aos titulares) ☐
- Sim (a organização elaborou Relatório de Impacto à Proteção de Dados Pessoais que abrange ALGUNS processos de tratamento de dados pessoais que podem gerar riscos aos titulares) ☐
- Não ☒
- Não se aplica (a organização não executa processo de tratamento de dados pessoais que pode gerar riscos às liberdades civis e aos direitos fundamentais dos titulares) ☐

E10. A organização implementou controles para mitigar os riscos identificados por meio da elaboração do Relatório de Impacto de Proteção de Dados Pessoais?

Referência(s): Lei 13.709/2018, art. 5º, inciso XVII; art. 38. ABNT NBR ISO/IEC 27.701/2019, item 7.2.5.

A organização deve adotar medidas para tratar os riscos identificados por meio da avaliação de impacto sobre a proteção de dados pessoais.

Sim (a organização implementou controles para mitigar todos os riscos identificados por meio da elaboração do Relatório de Impacto de Proteção de Dados Pessoais) ☐

Parcialmente (a organização implementou controles para mitigar alguns riscos identificados por meio da elaboração do Relatório de Impacto de Proteção de Dados Pessoais) ☐

Não (a organização não implementou controles para mitigar os riscos identificados por meio da elaboração do Relatório de Impacto de Proteção de Dados Pessoais) ☐

Seção F: Seção F - 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.

Nesta seção são abordadas questões relacionadas à elaboração da política de privacidade e ao atendimento dos direitos dos titulares.

F1. A organização possui Política de Privacidade (ou instrumento similar)?

Referência(s): Lei 13.709/2018, art. 6º, inciso VI; art. 9º; art. 23, inciso I; art. 50, inciso I, alíneas "a", "d" e "e". ABNT NBR ISO/IEC 27.701/2019, itens 7.3.2 e 7.3.3.

A Política de Privacidade deve documentar e comunicar aos titulares de dados pessoais, de maneira clara e concisa, informações relativas ao tratamento de seus dados pessoais. A LGPD exemplifica informações que devem constar no referido artefato: as finalidades dos tratamentos; as formas e as durações dos tratamentos; a identificação e os dados de contato do controlador; as informações acerca do uso compartilhado de dados; as responsabilidades dos agentes que realizam os tratamentos; e os direitos do titular. Além disso, o Poder Público deve informar as hipóteses em que, no exercício de suas competências, realiza tratamento de dados pessoais, fornecendo informações sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades. O termo "Aviso de Privacidade" é comumente utilizado para se referir à Política de Privacidade.

Sim ☐

Não ☒

F2. A Política de Privacidade (ou instrumento similar) está publicada na internet?

Referência(s): Lei 13.709/2018, art. 6º, inciso VI; art. 9º; art. 50, inciso I, alínea "e". ABNT NBR ISO/IEC 27.701/2019, item 7.3.3.

A Política de Privacidade deve ser publicada em local facilmente acessível pelos titulares de dados pessoais. Além de fornecer acesso à política no momento da coleta dos dados pessoais, convém que a organização forneça acesso ao artefato de forma permanente no sítio institucional.

Sim ☐

Não ☐

F3. Favor informar o endereço da internet (URL) onde a política está publicada.

F4. Anexe a Política de Privacidade (ou instrumento similar) da organização.

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

F5. Foram implementados mecanismos para atender os direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização?

Referência(s): Lei 13.709/2018, art. 17-22. ABNT NBR ISO/IEC 27.701/2019, item 7.3.

Quando aplicável, a organização deve atender aos direitos dos titulares estabelecidos no art.18 da LGPD como, por exemplo: confirmação da existência de tratamento; acesso aos dados; e correção de dados.

- [ ] Sim (foram implementados mecanismos para atender todos os direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização)
- [x] Parcialmente (foram implementados mecanismos para atender alguns direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização)
- [ ] Não (não foram implementados mecanismos para atender os direitos dos titulares elencados no art. 18 da LGPD)

F6. A organização ao efetuar o tratamento de dados pessoais no exercício de suas competências legais ou execução de políticas públicas dá publicidade sobre a finalidade e a forma como o dado será tratado?

Referência(s): Lei 13.709/2018, art. 6º, Incisos I e VI / art. 23, Inciso I.

O tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

Sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

- [ ] Sim
- [x] Não

Seção G: Seção G - Compartilhamento de Dados Pessoais

A organização deve documentar detalhes relacionados ao compartilhamento de dados pessoais com terceiros.

A realização de compartilhamento demanda a adoção de controles adequados para mitigar riscos que possam comprometer a proteção dos dados pessoais. Diante disso, a LGPD defende que as precauções a serem adotadas entre as partes envolvidas no compartilhamento sejam formalizadas em contrato e que cuidados especiais devem ser adotados no caso de transferência internacional desses dados.

Nesta seção são abordadas questões relacionadas à identificação dos dados pessoais que são compartilhados, ao registro de eventos correlatos aos compartilhamentos e à transferência internacional de dados pessoais.

G1. A organização identificou os dados pessoais que são compartilhados com terceiros?

Referência(s): Lei 13.709/2018, art. 5º, inciso XVI; arts. 26-27; art. 39. ABNT NBR ISO/IEC 27.701/2019, item 7.5.3 e 7.5.4.

É conveniente que a organização tenha documentado quais os dados pessoais que são compartilhados com terceiros.

- [ ] Sim (os dados pessoais que são compartilhados com terceiros foram identificados)
- [ ] Parcialmente (alguns dados pessoais que são compartilhados com terceiros foram identificados)
- [x] Não (não houve iniciativa para identificar dados pessoais que são compartilhados com terceiros)
- [ ] Não se aplica (a organização não realiza compartilhamento de dados pessoais com terceiros)

G2. Os compartilhamentos de dados pessoais identificados estão em conformidade com os critérios estabelecidos na LGPD?

Referência(s): Lei 13.709/2018, art. 5º, inciso XVI; arts. 26-27; art. 39. ABNT NBR ISO/IEC 27.701/2019, item 7.5.3 e 7.5.4.

Os compartilhamentos de dados pessoais devem respeitar os critérios estabelecidos na LGPD. Diante disso, os casos de compartilhamento devem ser avaliados para que sejam efetuados os devidos ajustes.

O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal e respeitar os princípios elencados no art. 6º da LGPD.

Ademais, há a necessidade de que os contratos e convênios que impliquem uso compartilhado, transferência ou comunicação de dados pessoais com entidades privadas sejam objeto de comunicação à ANPD.

- [ ] Sim (os compartilhamentos de dados pessoais estão em conformidade com os critérios estabelecidos na LGPD)
- [ ] Parcialmente (alguns compartilhamentos de dados pessoais estão em conformidade com os critérios estabelecidos na LGPD)
- [ ] Não (os compartilhamentos de dados pessoais não estão em conformidade com os critérios estabelecidos na LGPD).

G3. A organização registra eventos relacionados à transferência dos dados pessoais que são compartilhados com terceiros e que foram identificados?

Referência(s): Lei 13.709/2018, art. 5º, inciso XVI; arts. 26-27; art. 39. ABNT NBR ISO/IEC 27.701/2019, item 7.5.4.

É conveniente que a organização tenha registros de quais dados foram compartilhados, com quem foram compartilhados e quando foram compartilhados.

- [ ] Sim (a organização registra eventos relacionados à transferência de todos os dados pessoais que são compartilhados com terceiros e que foram identificados)
- [ ] Parcialmente (a organização registra eventos relacionados à transferência de alguns dados pessoais que são compartilhados com terceiros e que foram identificados)
- [ ] Não (a organização não registra eventos relacionados à transferência dos dados pessoais que são compartilhados com terceiros e que foram identificados)

G4. Algum caso de compartilhamento envolve transferência internacional de dados pessoais?

Referência(s): Lei 13.709/2018, arts 33-36. ABNT NBR ISO/IEC 27.701/2019, item 7.5.1 e 7.5.2.

A LGPD relaciona os casos nos quais é permitida a transferência internacional de dados pessoais. Diante disso, é conveniente que a organização identifique os casos em que isso ocorre para avaliar se estão em conformidade com as hipóteses estabelecidos na lei.

- [ ] Sim
- [ ] Não

G5. As transferências internacionais de dados pessoais estão de acordo com os casos previstos na LGPD?

Referência(s): Lei 13.709/2018, arts. 33-36. ABNT NBR ISO/IEC 27.701/2019, item 7.5.2.

A organização deve avaliar se a transferência internacional de dados pessoais se enquadra em um dos casos previstos no art. 33 da LGPD.

- [ ] Sim
- [ ] Não

Seção H: Seção H - Violação de Dados Pessoais

A organização deve gerenciar incidentes de segurança da informação que envolvem a violação de dados pessoais.

Nesta seção são abordadas questões relacionadas à identificação, ao registro e ao tratamento de incidentes de violação de dados pessoais. Também será avaliado se a organização dispõe de mecanismo para notificar a Autoridade Nacional de Proteção de Dados e os titulares nos casos de incidentes que possam acarretar risco ou dano relevante aos titulares.

H1. A organização possui Plano de Resposta a Incidentes (ou documento similar) que abrange o tratamento de incidentes que envolvem violação de dados pessoais?

Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I, alínea "g". ABNT NBR ISO/IEC 27.701/2019, item 6.13.1.1.

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

Sim ☐

Não ☒

H2. Anexe o Plano de Resposta a Incidentes (ou documento similar) da organização.

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

H3. A organização possui sistema para o registro de incidentes de segurança da informação que envolvem violação de dados pessoais?

Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I, alínea "g". ABNT NBR ISO/IEC 27.701/2019, item 6.13.1.1.

Convém que a organização possua um sistema de informação de gestão de incidentes que viabiliza o tratamento de casos que envolvem violação de dados pessoais. Essa gestão inclui o registro dos incidentes.

Sim ☐

Não ☒

H4. A organização possui sistema para registro das ações adotadas para solucionar incidentes de segurança da informação que envolvem violação de dados pessoais?

Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I, alínea "g". ABNT NBR ISO/IEC 27.701/2019, item 6.13.1.5.

Convém que a organização possua sistema para o registro das ações adotadas para solucionar os incidentes que envolvem violação de dados pessoais. O tratamento de incidentes pode envolver, primeiramente, a adoção de solução de contorno para, posteriormente, haver análise e erradicação da causa.

Sim ☐

Não ☒

H5. A organização monitora proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais?

Referência(s): Lei 13.709/2018, art. 50, § 2º, inciso I, alínea "g". ABNT NBR ISO/IEC 27.701/2019, itens 6.13.1.4 e 6.13.1.5.

Convém que a organização adote mecanismo para monitorar proativamente os eventos de segurança da informação que são associados à violação de dados pessoais para adotar medidas necessárias caso ocorram. A identificação precoce de incidentes pode diminuir significativamente os impactos causados por eles.

Sim ☒

Não ☐

H6. A organização estabeleceu procedimentos para comunicar à Autoridade Nacional de Proteção de Dados e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares?

Referência(s): Lei 13.709/2018, art. 48. ABNT NBR ISO/IEC 27.701/2019, item 6.13.1.5.

A organização deve comunicar à ANPD e ao titular a ocorrência de incidente de segurança da informação que possa acarretar risco ou dano relevante aos titulares. A notificação deve ser feita em prazo razoável e mencionar, no mínimo: a descrição da natureza dos dados pessoais afetados; as informações sobre os titulares envolvidos; a indicação das medidas técnicas e de segurança adotadas para a proteção dos dados; os riscos relacionados ao incidente; e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. Caso a organização não encaminhe a comunicação tempestivamente, deverá ser exposto, também, os motivos que levaram à demora.

Sim ☐

Não ☒

Seção I: Seção I - Medidas de Proteção

A organização deve adotar medidas de segurança, técnicas e administrativas, para proteger os dados pessoais. Para isso, convém que sejam implementados controles capazes de mitigar riscos que possam resultar em violação da privacidade.

Nesta seção serão abordadas questões relacionadas à implementação de controles para restringir e rastrear o acesso a dados pessoais e à avaliação de impacto sobre a proteção de dados pessoais.

I1. A organização é capaz de comprovar que adotou medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais?

Referência(s): Lei 13.709/2018, art. 46. ABNT NBR ISO/IEC 27.002/2013, item 6.1.

A organização deve 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.

Sim ☐

Não ☒

I2. A organização implementou processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais?

Referência(s): Lei 13.709/2018, art. 46. ABNT NBR ISO/IEC 27.701/2019, itens 6.6.2.1 e 6.6.2.2.

Convém que a organização defina processo formal para registro e cancelamento de usuários para viabilizar a atribuição dos direitos de acesso aos sistemas que realizam tratamento de dados pessoais. O mesmo deve ser feito com o processo de provisionamento para conceder ou revogar os direitos de acesso dos usuários nesses sistemas. Convém que a concessão de direitos de acesso observem os princípios de "necessidade de conhecer" e "necessidade de uso".

Sim (a organização implementou processo formal para registro, cancelamento e provisionamento de usuários em todos os sistemas que realizam tratamento de dados pessoais) ☐

Parcialmente (a organização implementou processo formal para registro, cancelamento e provisionamento de usuários em alguns sistemas que realizam tratamento de dados pessoais) ☒

Não (a organização não implementou processo formal para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais) ☐

I3. A organização registra eventos das atividades de tratamento de dados pessoais?

Referência(s): Lei 13.709/2018, art. 46. ABNT NBR ISO/IEC 27.701/2019, item 6.9.4.1.

Convém que a organização registre os eventos (logs) das 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 ocorrem mudanças nos dados, também deve ser registrada a ação realizada (e.g.: inclusão, alteração ou exclusão).

Sim (a organização registra os eventos de todas as atividades de tratamento de dados pessoais) ☐

Parcialmente (a organização registra os eventos de algumas atividades de tratamento de dados pessoais) ☒

Não (a organização não registra os eventos de atividades de tratamento de dados pessoais) ☐

I4. A organização utiliza criptografia para proteger os dados pessoais?

Referência(s): Lei 13.709/2018, art. 46; art. 50, § 2º, inciso I, alínea "c". ABNT NBR ISO/IEC 27.701/2019, item 6.7.

A utilização de criptografia pode proteger a confidencialidade, a autenticidade e/ou a integridade da informação. Por exemplo, devido à criticidade dos dados sensíveis, a adoção de mecanismos para criptografá-los em trânsito e no armazenamento pode mitigar riscos associados à violação de dados pessoais.

Sim (a organização utiliza criptografia para proteger todos os dados pessoais) ☐

Parcialmente (a organização utiliza criptografia para proteger alguns dados pessoais) ☐

Não (a organização não utiliza criptografia para proteger os dados pessoais) ☒

I5. A organização adotou medidas para assegurar que processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD (*Privacy by Design e Privacy by Default*)?

Referência(s): Lei 13.709/2018, art. 46, § 2º. ABNT NBR ISO/IEC 27.701/2019, item 7.4.

A organização deve assegurar que os processos e sistemas sejam projetados de forma que os tratamentos de dados pessoais estejam limitados ao que é estritamente necessário para alcance da finalidade pretendida.

Sim ☐

Não ☒

Seção J: Seção J - Informações Complementares

J1. O Órgão possui cargos/áreas/especialidades próprios para a área de TI?

Sim ☒

Não ☐

J2. O Órgão possui e atualiza estudo de quantitativo de pessoal necessário para a execução das atividades da área de TI?

Sim ☐

Não ☒

J3. Qual o quantitativo da força de trabalho da área de TI do Órgão?

Considere servidores efetivos, requisitados, temporários e terceirizados.

Para terceirizados, considere apenas os com regime de dedicação exclusiva de mão de obra.

Os serviços terceirizados com regime de dedicação exclusiva de mão de obra são aqueles em que o modelo de execução contratual exige, dentre outros requisitos, que: I. Os empregados da contratada fiquem à disposição nas dependências da contratante para a prestação dos serviços; II. A contratada não compartilhe os recursos humanos e materiais disponíveis de uma contratação para execução simultânea de outros contratos; III. A contratada possibilite a fiscalização pela contratante quanto à distribuição, controle e supervisão dos recursos humanos alocados aos seus contratos.

3	1	.	0	0	0	0	0	0	0

J4. Qual o quantitativo de servidores efetivos que compõe força de trabalho de TI do Órgão?

Não considerar servidores requisitados de outros Órgãos.

2	1	.	0	0	0	0	0	0	0

J5. Qual o quantitativo de servidores efetivos do Órgão que atua na área de TI desempenhando tarefas de gestão, tais como planejamento, coordenação, supervisão e controle, e/ou atividades estratégicas?

Considere os profissionais que executam esses papéis, independemente de possuírem função comissionada.

Exemplos de atividades estratégicas: governança e segurança da informação.

7	.	0	0	0	0	0	0	0	0

J6. Qual o quantitativo de profissionais não efetivos do Órgão que atua na área de TI desempenhando tarefas de gestão, tais como planejamento, coordenação, supervisão e controle, e/ou atividades estratégicas?

Considere "profissionais não efetivos" os que executam esses papéis e não são servidores efetivos do Órgão, tais como requisitados, temporários, exclusivamente comissionados ou terceirizados.

Considere os profissionais que executam esses papéis, independemente de possuírem função comissionada.

Exemplos de atividades estratégicas: governança e segurança da informação.

2	.	0	0	0	0	0	0	0	0

J7. O Órgão contratou algum serviço de consultoria para auxiliar em sua adequação à LGPD?

Serviço de consultoria pode ser para auxiliar o órgão na criação de um plano de ação para implementação da LGPD, para mapeamento de processos de negócios que tratam dados pessoais, para a realização de ações de capacitação e treinamento, entre outros possíveis tipos de consultoria sobre o tema LGPD.

Sim ☐

Não ☒

J8. Informe o processo administrativo referente a contratação da consultoria.

J9. O Órgão estabeleceu ato normativo próprio visando recepcionar a lei do Governo Digital, Lei n.º 14.129/2021, que dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública ?

Sim (O município já publicou ano normativo próprio referente à lei de Governo Digital) ☐

Não (O município ainda não possui normativo próprio, mas já possui comissão formalmente instituída para tratar do tema) ☐

Não (O município ainda não adotou qualquer medida para publicar ato próprio sobre a lei de Governo Digital) ☒

J10. Anexe a Lei municipal (ou outro instrumento) publicado para recepcionar a Lei do Governo Digital

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

J11. Anexe a portaria (ou outro instrumento) publicada, que instituiu a comissão municipal para tratar da Lei de Governo Digital no município

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

J12. O município publicou algum normativo visando a implementação da LGPD?

O normativo pode ser lei municipal, decreto ou qualquer outro tipo de instrumento publicado.

Sim ☐

Não ☒

J13. Anexe o normativo publicado pelo município que trata da implementação da LGPD

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

Seção K: Seção K - Conclusão

K1. Há informações prestadas neste questionário classificadas como não públicas?

Sim ☐

Não ☒

K2. Favor informar as informações classificadas como não públicas, com as devidas justificativas, bem como o endereço eletrônico no qual se encontra o respectivo instrumento de classificação da informação.

K3. Considera que o questionário usado nessa auditoria de conformidade pode contribuir para a adequação do Órgão à LGPD?

Sim ☒

Parcialmente ☐

Não ☐

K4. Comentários

Utilize o espaço para registrar suas considerações acerca da auditoria, incluindo críticas às questões, alertas para situações especiais não contempladas ou qualquer outra contribuição que considere válida. Tais comentários permitirão análise mais adequada dos dados encaminhados e melhorias para os próximos questionários.

Esta auditoria trouxe execelente referências para o planejamento de execuções de ações envolvendo à LGPD.

K5. Estou ciente que não será possível realizar ajustes nas respostas após clicar no botão "Enviar".

Caso ainda exista alguma pendência ou dúvida, utilize a opção "Retomar mais tarde" no canto superior direito da página para salvar as respostas fornecidas até então.

Ao final, depois do envio, vai aparecer, na página de confirmação, uma opção para imprimir o questionário com as respostas.

Sim ☒

Atenção

Alertamos que a opção de impressão do questionário só aparece nesse momento e não é possível acessar depois para ver ou imprimir as respostas enviadas.

Utilize o link abaixo, e em seguida a opção Exportar para queXML PDF, depois salve o arquivo PDF gerado, tendo em vista que o órgão deve publicar este documento em seu sítio eletrônico.