TRIBUNAL DE CONTAS DA UNIÃO

Auditoria para elaborar diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD

(Acórdão 1.384/2022-TCU-Plenário, Relatoria Min. Augusto Nardes)

Relatório de *Feedback*

Organização:

Conselho Federal de Medicina

(CFM)

Todas as informações deste documento são consideradas públicas, conforme classificação do item 9.10 do Acórdão 1.384/2022-TCU-Plenário.

Sumário

Lista de Figuras

Lista de Tabelas

1 Introdução

Este relatório apresenta os resultados da organização **CFM** relativos à auditoria realizada pelo TCU entre novembro de 2020 e maio de 2021 para avaliar as ações governamentais e os riscos à proteção de dados pessoais por meio da elaboração de diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à Lei 13.709/2018, denominada Lei Geral de Proteção de Dados (LGPD) (TC 039.606/2020-1; Acórdão 1.384/2022-TCU-Plenário de relatoria do Ministro Augusto Nardes).

Ressalta-se que o TCU fará a divulgação dos resultados desta fiscalização conforme autorização do Plenário, mas, em atendimento ao princípio da transparência, é recomendável que a própria organização tome a iniciativa de também **publicar em seu próprio *site* as informações contidas neste relatório**.

2 Avaliação da adequação à LGPD

O método utilizado para avaliar as organizações foi o de autoavaliação de controles (do inglês *Control Self-Assessment – CSA*), por meio do qual foi disponibilizado um questionário eletrônico para que os gestores preenchessem as respostas que melhor refletiam a situação das respectivas organizações com relação aos controles relacionados à LGPD. Além de permitir que as organizações verificassem quais controles associados à LGPD foram implementados, as questões também devem ser utilizadas como referência para a condução de futuras iniciativas de adequação.

O questionário contemplou 60 questões organizadas em duas perspectivas e nove dimensões (Figura 1). As questões tiveram como referência a própria LGPD e a norma técnica ABNT NBR ISO/IEC 27701:2019 (extensão das normas de segurança da informação ABNT NBR ISO/IEC 27.001 e ABNT NBR ISO/IEC 27.002 para gestão da privacidade da informação).

Figura 1 - Dimensões do questionário

De modo a consolidar os dados obtidos e a possibilitar a comparação das organizações auditadas, no que tange ao nível de adequação à LGPD, um subconjunto de 42 questões foi escolhido para compor um indicador elaborado com o intuito de resumir as respostas fornecidas por cada organização.

O cálculo do indicador considerou as possíveis respostas de cada questão selecionada, atribuindo uma nota numérica a cada uma delas. Assim, as respostas dos tipos "Sim", "Parcialmente" e "Não" correspondem, respectivamente, às notas 1, 0,5 e 0; sendo que o valor do indicador é obtido pela soma das notas obtidas em cada uma das questões dividida por 42. Assim, para cada organização, o valor do indicador pode variar de 0 (nota 0 em todas as questões) a 1 (nota 1 em todas as questões)[1].

A partir dos valores do indicador, foram definidos quatro níveis de adequação à LGPD: "Inexpressivo" (indicador menor ou igual a 0,15), "Inicial" (indicador maior do que 0,15 e menor ou

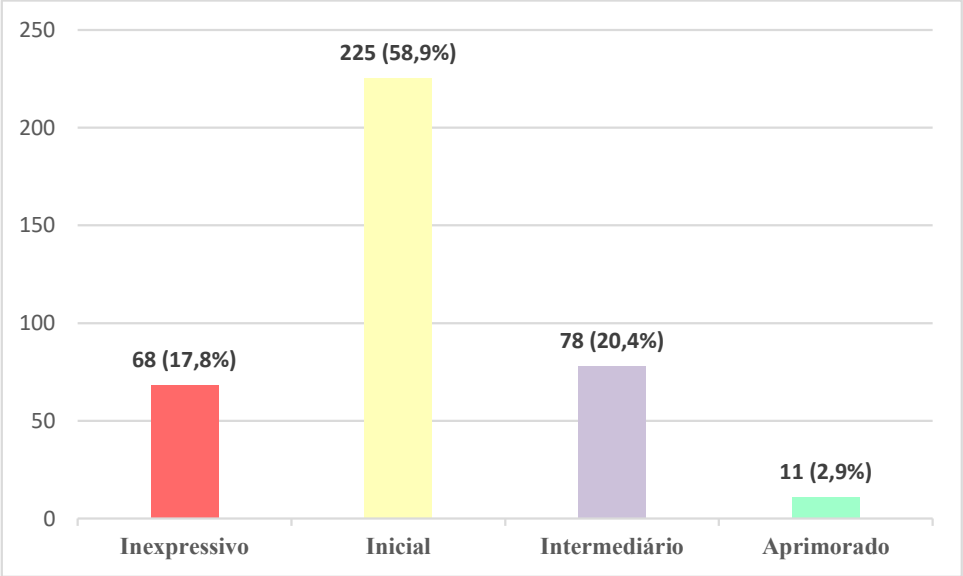
[1] O cálculo do indicador está detalhado na Seção 2.2 do relatório de auditoria.

igual a 0,5), "Intermediário" (indicador maior do que 0,5 e menor ou igual a 0,8) e "Aprimorado" (indicador maior do que 0,8). Assim, conforme o valor do indicador obtido, as organizações foram classificadas em um desses níveis de maturidade.

A organização **CFM** obteve o valor **0,53** para o indicador de adequação, o que corresponde ao nível "**Intermediário**".

O gráfico da Figura 2 apresenta a consolidação da distribuição das 382 organizações em cada nível.

Figura 2 - Distribuição das organizações por níveis de adequação à LGPD



O indicador pode ser desmembrado e também apresentado levando em consideração os valores referentes a cada uma das dimensões do questionário: "Preparação", "Contexto Organizacional", "Liderança", "Capacitação", "Conformidade do Tratamento", "Direitos do Titular", "Compartilhamento de Dados Pessoais", "Violação de Dados Pessoais" e "Medidas de Proteção".

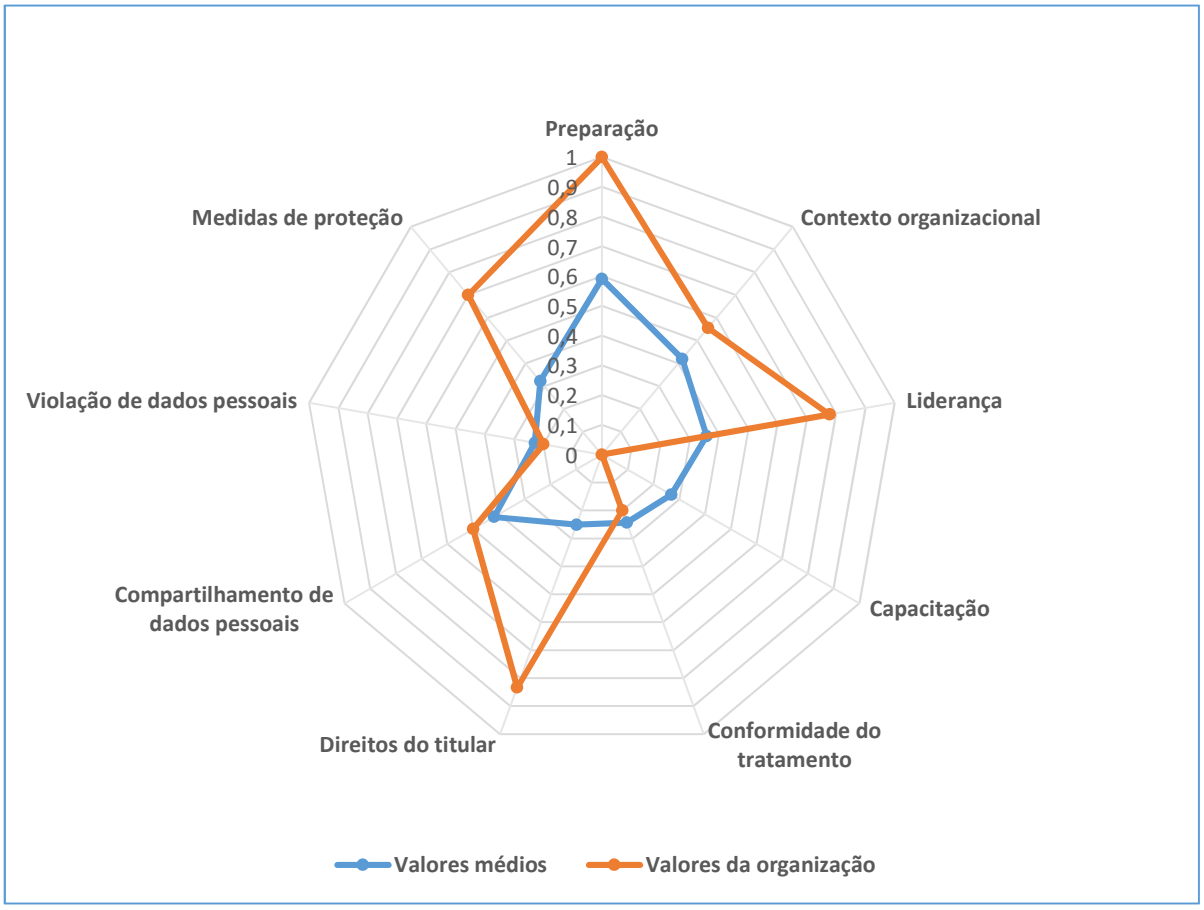
Na Tabela 1 é apresentado um resumo da avaliação da organização contendo os valores de cada dimensão do questionário e do indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

Tabela 1 - Resumo da avaliação da adequação à LGPD

Dimensões do questionário	**Valores da organização**	**Valores médios**
Estruturação para condução da iniciativa de adequação		
Preparação	1,00	0,59
Contexto Organizacional	0,56	0,42
Liderança	0,78	0,36
Capacitação	0,00	0,27
Medidas e controles de proteção de dados pessoais implementados		
Conformidade do Tratamento	0,20	0,24
Direitos do Titular	0,83	0,25
Compartilhamento de Dados Pessoais	0,50	0,42
Violação de Dados Pessoais	0,20	0,23
Medidas de Proteção	0,70	0,32
Indicador de adequação à LGPD	**0,53**	**0,35**

O gráfico da Figura 3 possibilita comparar visualmente os valores dos indicadores em cada dimensão que foram calculados para a organização **CFM** relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 3 - Valores da organização e valores médios por dimensões do questionário



A partir deste diagnóstico, constata-se que a maior parte das organizações ainda está iniciando o processo de adequação à LGPD. Contudo, vale ressalvar que o gráfico individual de cada organização pode ser influenciado pelo porte e pelos objetivos do negócio e que, assim, nem todas as organizações devem estar no mesmo patamar em todas as dimensões.

2.1 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 dimensão abordam aspectos relacionados à identificação e ao planejamento das medidas necessárias à adequação.

Na Tabela 2 são apresentadas as questões desta dimensão que compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

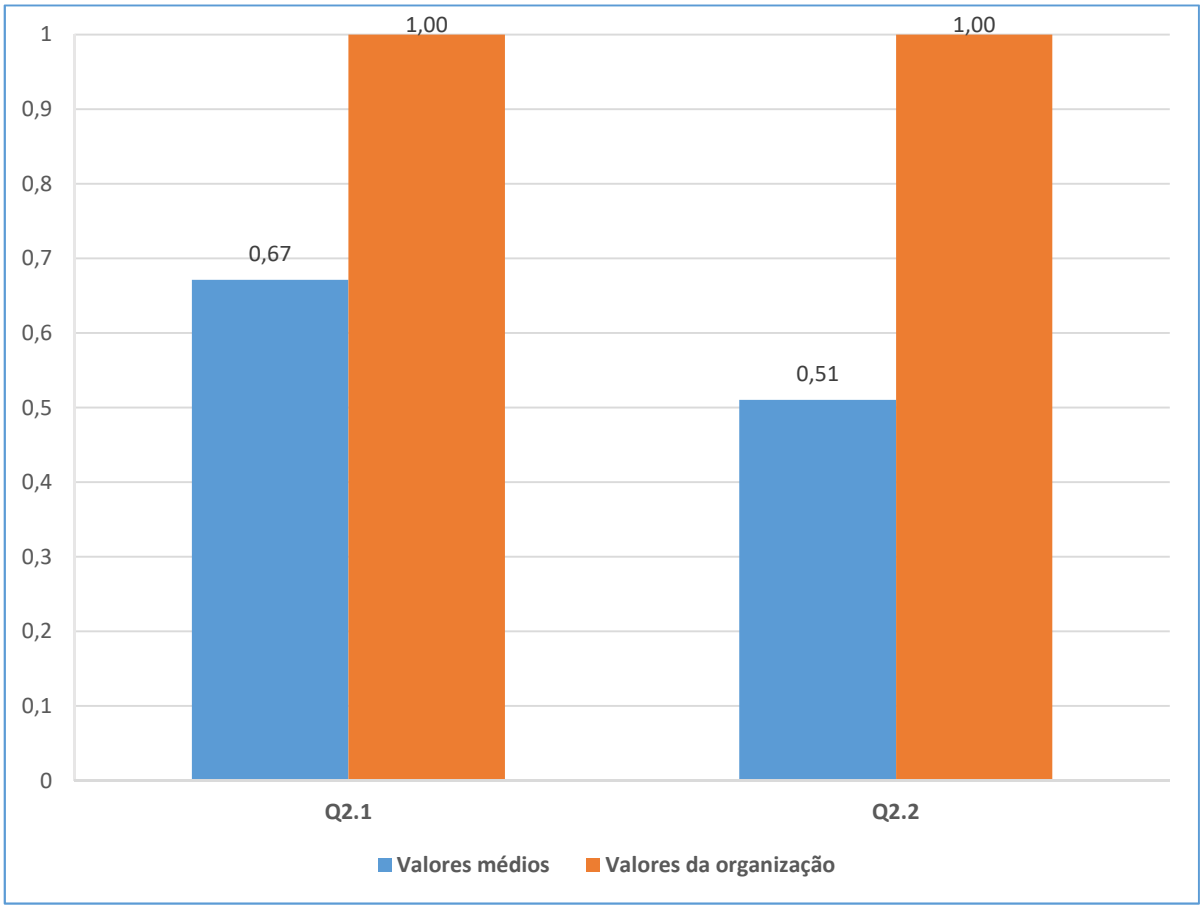
Tabela 2 - Preparação para adequação à LGPD

Questões	Valores da organização	Valores médios
2.1 A organização conduziu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD?	1,00	0,67
2.2 A organização elaborou plano de ação, plano de	1,00	0,51

projeto ou documento similar para direcionar a iniciativa de adequação à LGPD?		

O gráfico da Figura 4 possibilita comparar visualmente os valores das questões desta dimensão que foram calculados para a organização relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 4 - Valores da organização e valores médios na dimensão "Preparação"



2.2 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.

Na Tabela 3 são apresentadas as questões desta dimensão que compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

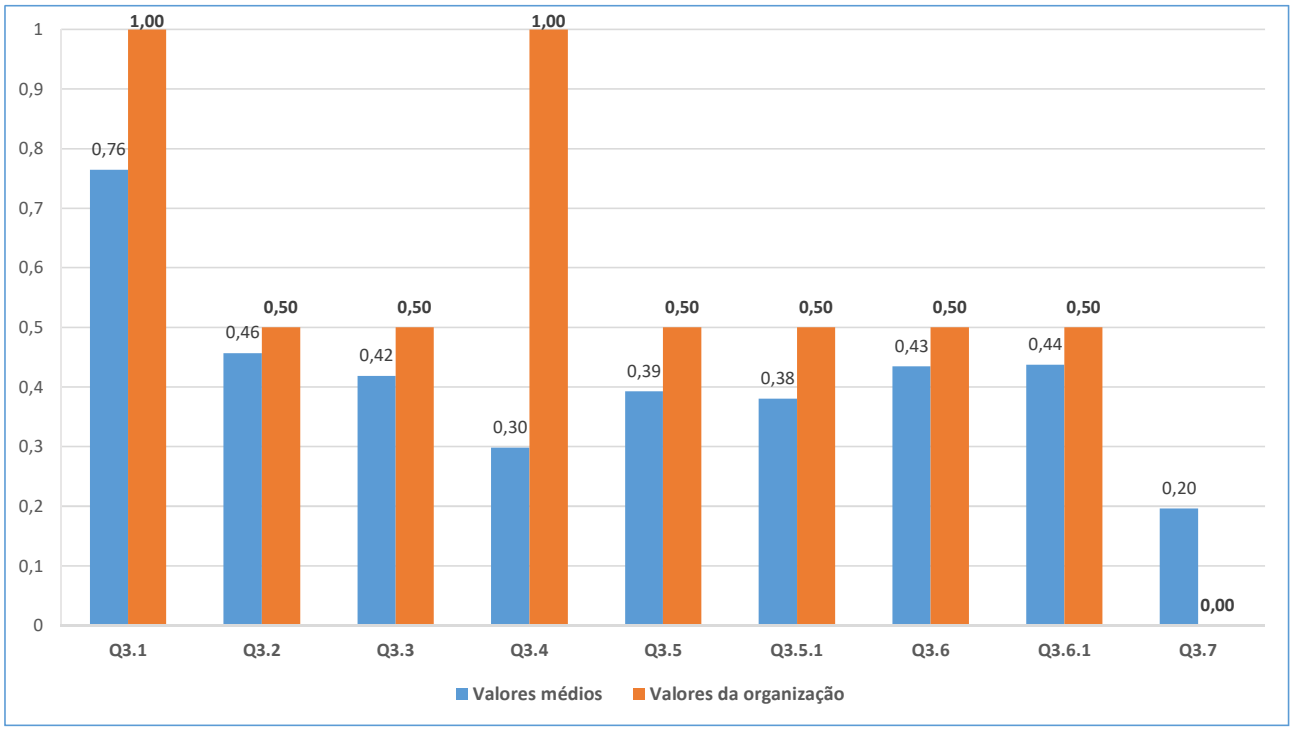
Tabela 3 - Contexto Organizacional

Questões	Valores da organização	Valores médios
3.1 A organização conduziu iniciativa para identificar outros normativos (e.g.: leis, regulamentos e	1,00	0,76

instruções normativas), além da LGPD, que abrangem comandos relacionados à proteção de dados pessoais e que também devem ser respeitados?		
3.2 A organização identificou as categorias de titulares de dados pessoais com os quais se relaciona?	0,50	0,46
3.3 A organização conduziu iniciativa para identificar os operadores que realizam tratamento de dados pessoais em seu nome?	0,50	0,42
3.4 A organização avaliou se há tratamento de dados que envolva controlador conjunto?	1,00	0,30
3.5 A organização identificou os processos de negócio que realizam tratamento de dados pessoais?	0,50	0,39
3.5.1 A organização identificou quem são os responsáveis pelos processos de negócio que realizam tratamento de dados pessoais e que já foram identificados?	0,50	0,38
3.6 A organização identificou quais são os dados pessoais tratados por ela?	0,50	0,43
3.6.1 A organização identificou os locais onde os dados pessoais identificados são armazenados?	0,50	0,44
3.7 A organização avaliou os riscos dos processos de tratamento de dados pessoais que foram identificados?	0,00	0,20

O gráfico da Figura 5 possibilita comparar visualmente os valores das questões desta dimensão que foram calculados para a organização relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 5 - Valores da organização e valores médios na dimensão "Contexto Organizacional"



2.3 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.

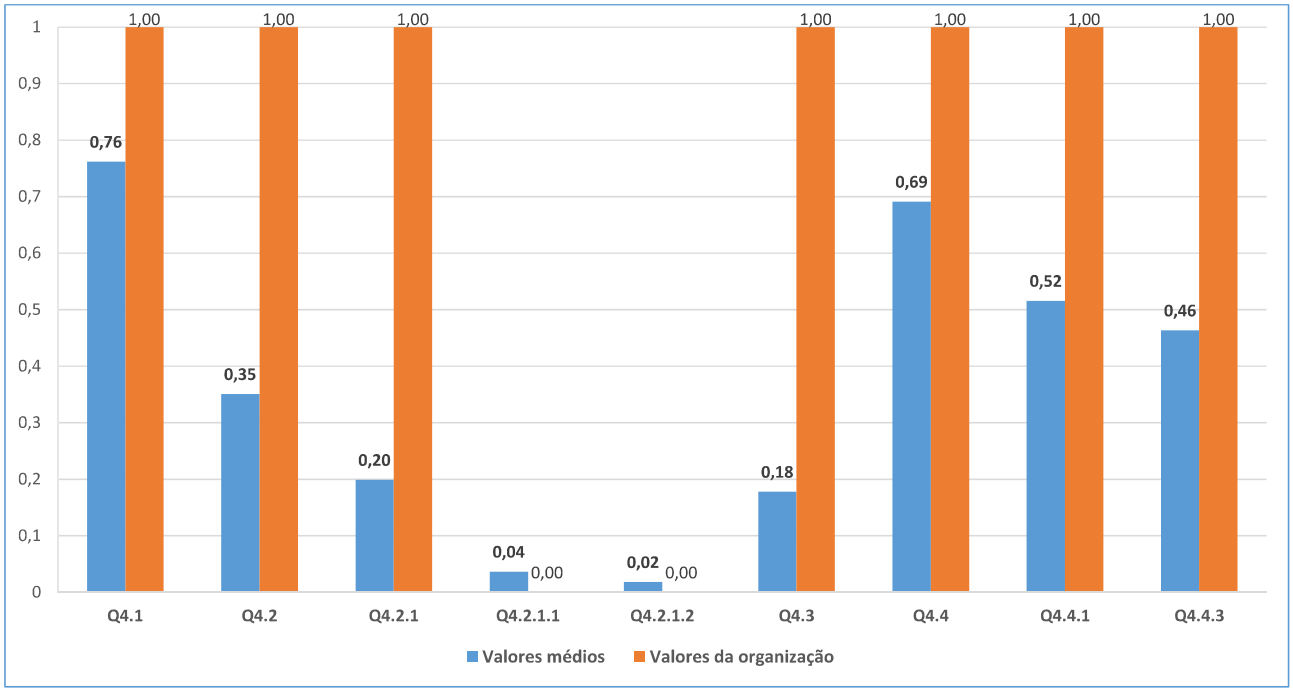
Na Tabela 4 são apresentadas as questões desta dimensão que compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

Tabela 4 - Liderança

Questões	**Valores da organização**	**Valores médios**
4.1 A organização possui Política de Segurança da Informação ou instrumento similar?	1,00	0,76
4.2 A organização possui Política de Classificação da Informação ou instrumento similar?	1,00	0,35
4.2.1 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para a classificação de dados pessoais?	1,00	0,20
4.2.1.1 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para identificar dados pessoais sensíveis e relacionados a crianças e adolescentes?	0,00	0,04
4.2.1.2 A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para identificar dados pessoais de crianças e de adolescentes?	0,00	0,02
4.3 A organização possui Política de Proteção de Dados Pessoais (ou instrumento similar)?	1,00	0,18
4.4 A organização nomeou o encarregado pelo tratamento de dados pessoais?	1,00	0,69
4.4.1 A nomeação do encarregado foi publicada em veículo de comunicação oficial?	1,00	0,52
4.4.3 A identidade e as informações de contato do encarregado foram divulgadas na internet?	1,00	0,46

O gráfico da Figura 6 possibilita comparar visualmente os valores das questões desta dimensão que foram calculados para a organização relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 6 - Valores da organização e valores médios na dimensão "Liderança"



2.4 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.

Na Tabela 5 são apresentadas as questões desta dimensão que compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

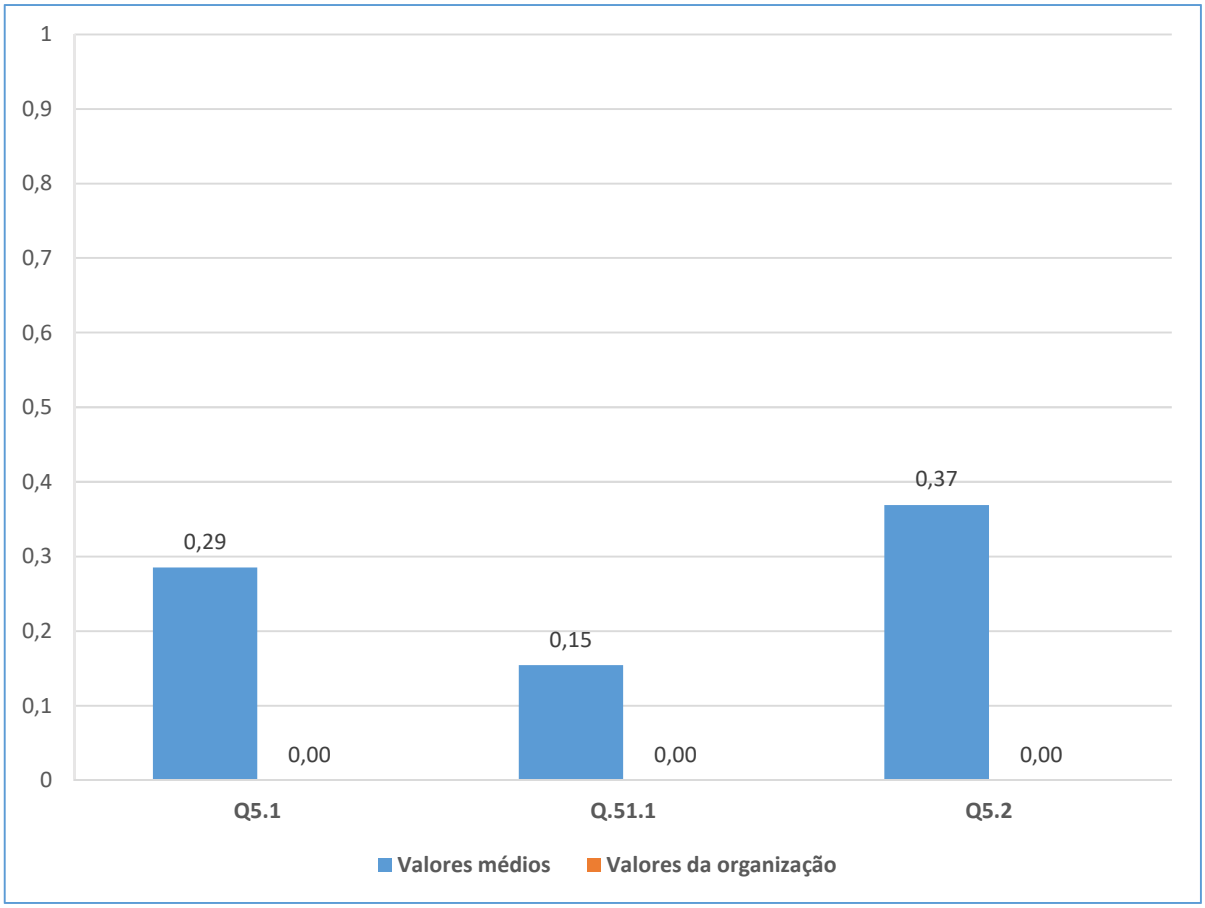
Tabela 5 - Capacitação

Questões	Valores da organização	Valores médios
5.1 A organização possui Plano de Capacitação (ou instrumento similar) que abrange treinamento e conscientização dos seus colaboradores em proteção de dados pessoais?	0,00	0,29
5.1.1 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?	0,00	0,15

5.2. Colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema?	0,00	0,37

O gráfico da Figura 7 possibilita comparar visualmente os valores das questões desta dimensão que foram calculados para a organização relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 7 - Valores da organização e valores médios na dimensão "Capacitação"



2.5 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.

Na Tabela 6 são apresentadas as questões desta dimensão que compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

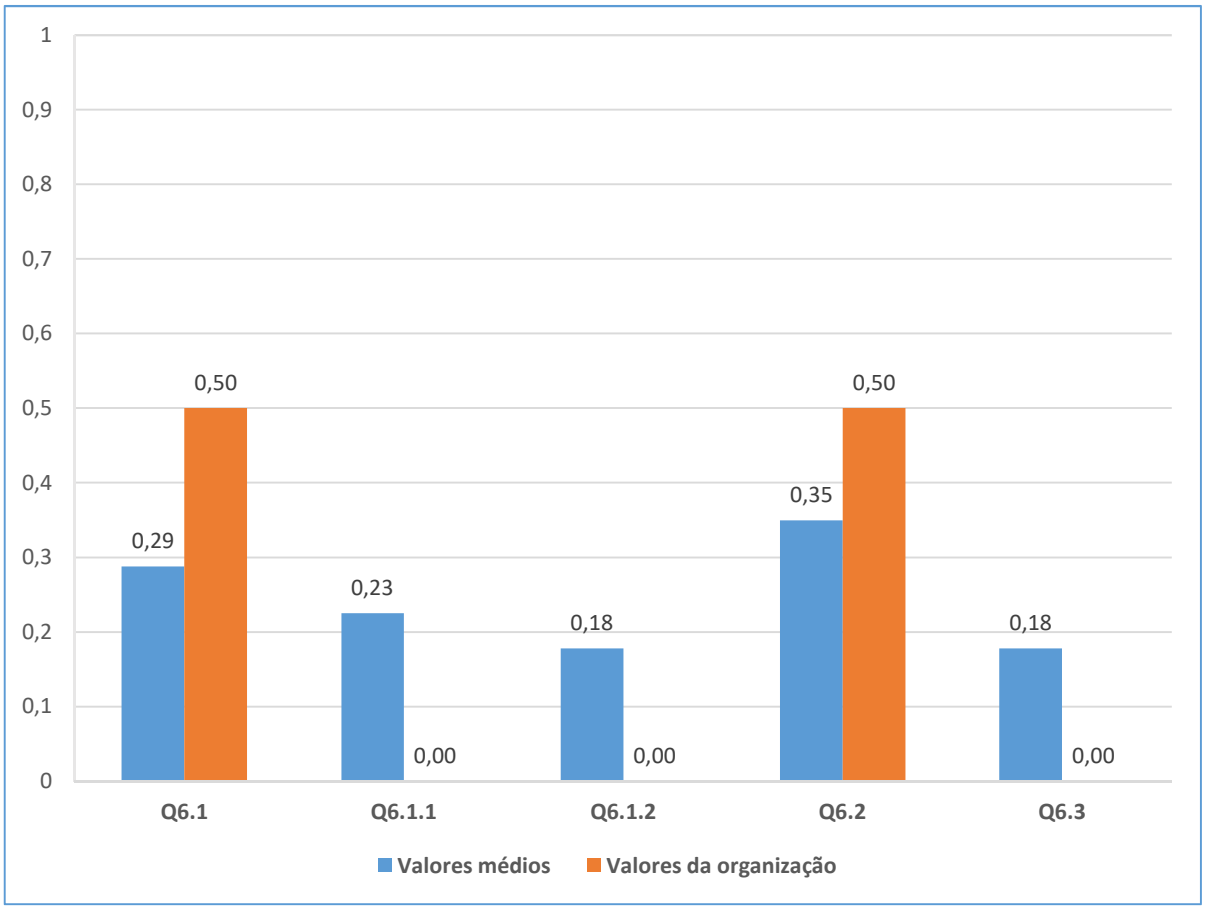
Tabela 6 - Conformidade do Tratamento

Questões	**Valores da**	**Valores**

	organização	médios
6.1 A organização identificou e documentou as finalidades das atividades de tratamento de dados pessoais?	0,50	0,29
6.1.1 A organização avaliou se coleta apenas os dados estritamente necessários para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas?	0,00	0,23
6.1.2 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?	0,00	0,18
6.2 A organização identificou e documentou as bases legais que fundamentam as atividades de tratamento de dados pessoais?	0,50	0,35
6.3 Há um registro (*e.g.*: inventário) instituído para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais?	0,00	0,18

O gráfico da Figura 8 possibilita comparar visualmente os valores das questões desta dimensão que foram calculados para a organização relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 8 - Valores da organização e valores médios na dimensão "Conformidade do Tratamento"



2.6 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.

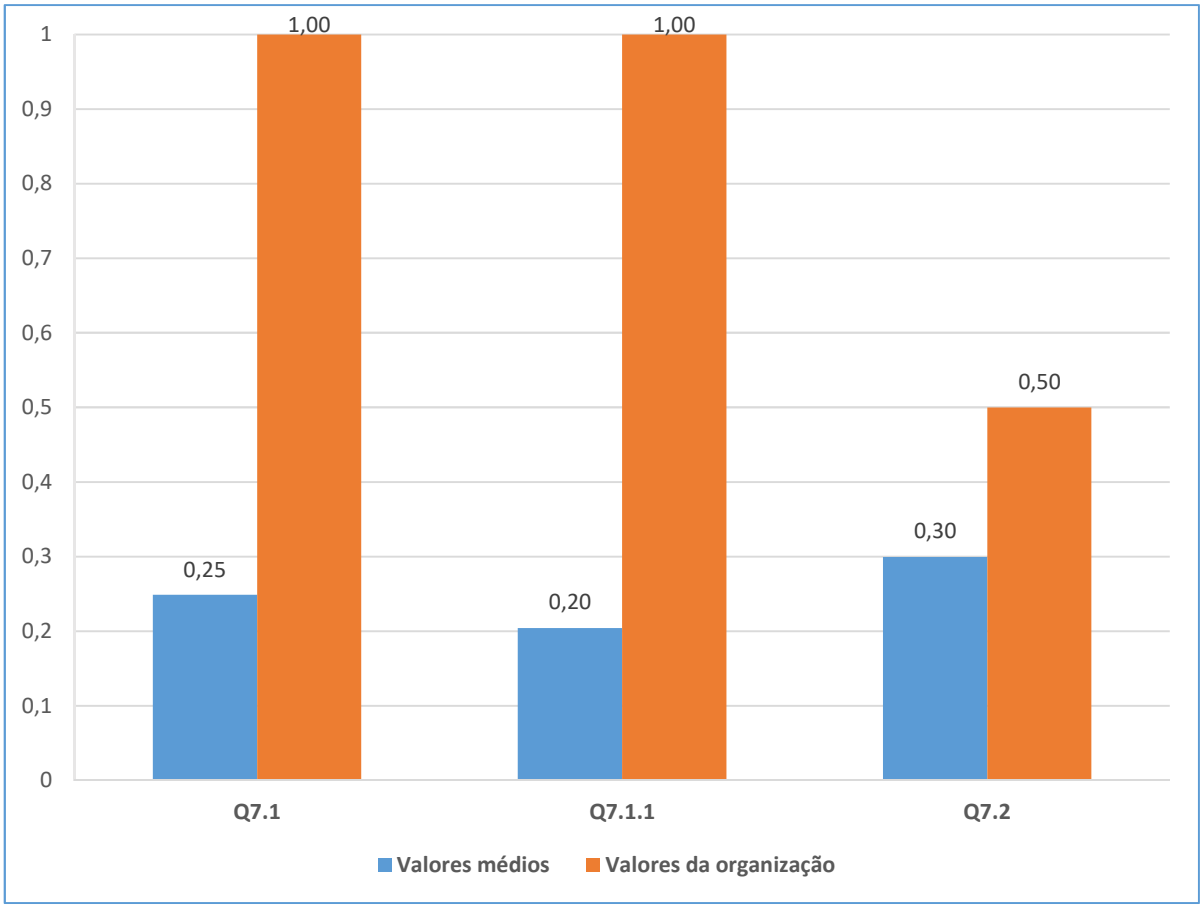
Na Tabela 7 são apresentadas as questões desta dimensão que compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

Tabela 7 - Direitos do Titular

Questões	**Valores da organização**	**Valores médios**
7.1 A organização possui Política de Privacidade (ou instrumento similar)?	1,00	0,25
7.1.1 A Política de Privacidade (ou instrumento similar) está publicada na internet?	1,00	0,20
7.2 Foram implementados mecanismos para atender os direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização?	0,50	0,30

O gráfico da Figura 9 possibilita comparar visualmente os valores das questões desta dimensão que foram calculados para a organização relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 9 - Valores da organização e valores médios na dimensão "Direitos do Titular"



2.7 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.

Na Tabela 8 é apresentada a questão desta dimensão que compõe o indicador de adequação à LGPD, possibilitando comparar o valor da própria organização e o valor médio do conjunto das 382 organizações avaliadas.

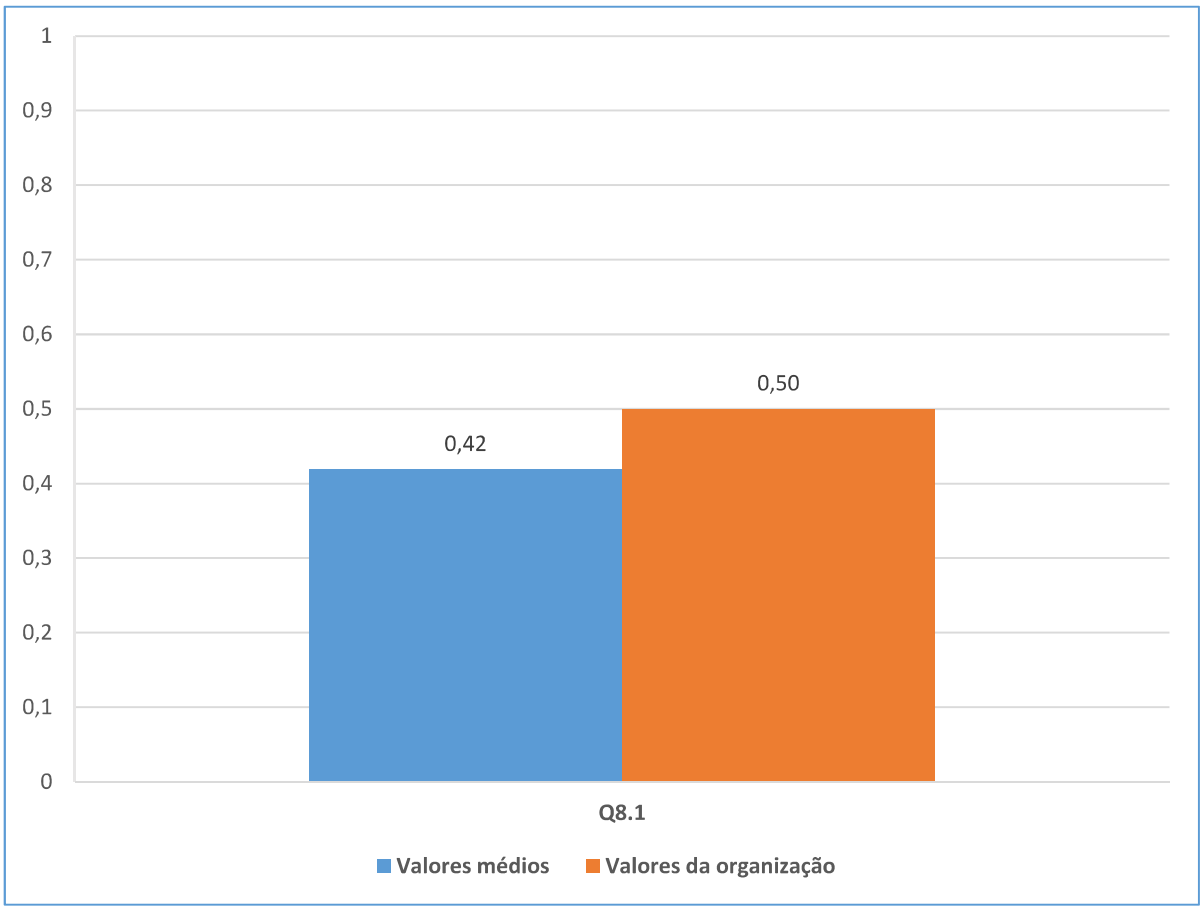
Tabela 8 - Compartilhamento de Dados Pessoais

Questão	Valor da organização	Valor médio
8.1 A organização identificou os dados pessoais que são compartilhados com terceiros?	0,50	0,42

O gráfico da Figura 10 possibilita comparar visualmente o valor da questão desta

dimensão que foi calculado para a organização relativamente ao valor médio calculado ao se considerar o conjunto das 382 organizações avaliadas.

Figura 10 - Valor da organização e valor médio na dimensão "Compartilhamento de Dados Pessoais"



2.8 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.

Na Tabela 9 são apresentadas as questões desta dimensão que compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

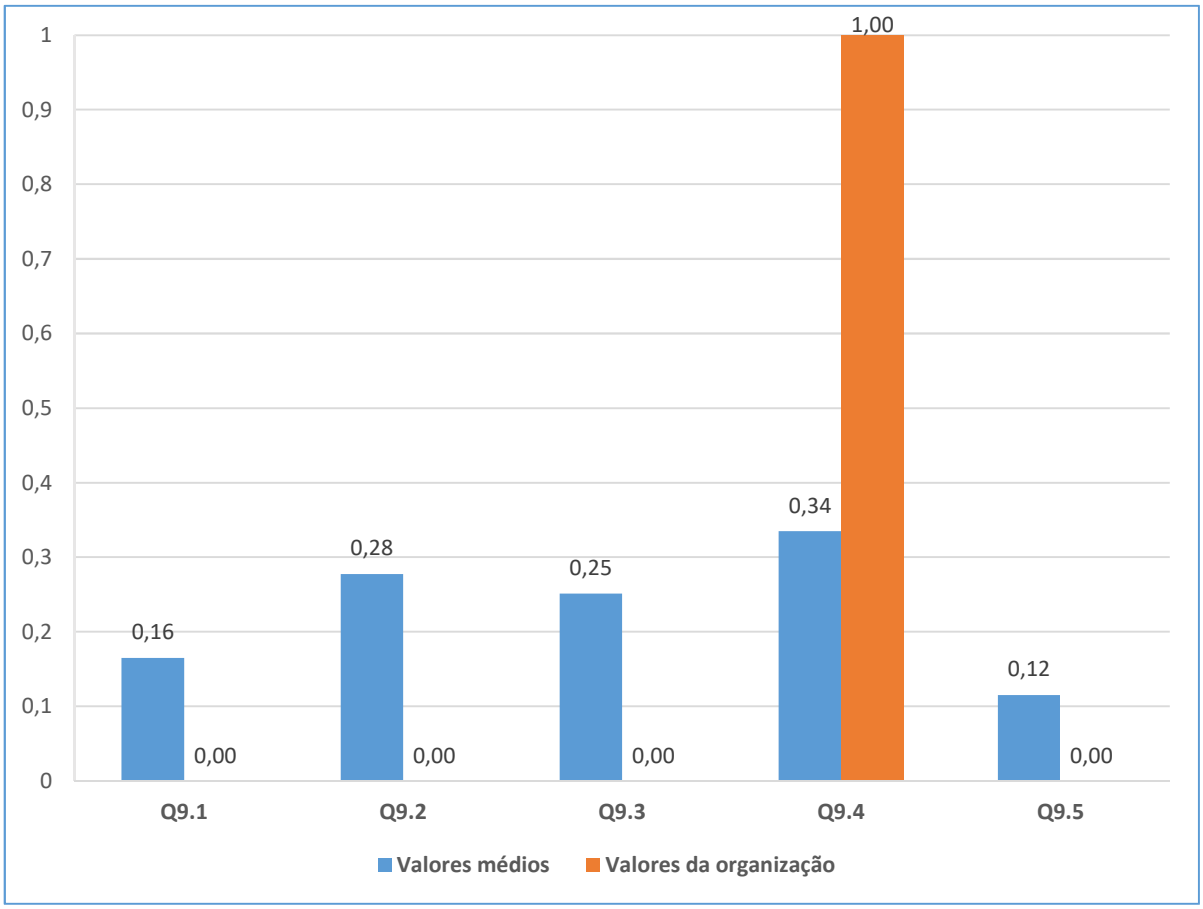
Tabela 9 - Violação de Dados Pessoais

Questões	Valores da organização	Valores médios
9.1 A organização possui Plano de Resposta a Incidentes (ou documento similar) que abrange o tratamento de incidentes que envolvem violação de dados pessoais?	0,00	0,16
9.2 A organização possui sistema para o registro de incidentes de segurança da informação que envolvem violação de dados pessoais?	0,00	0,28

9.3 A organização possui sistema para registro das ações adotadas para solucionar incidentes de segurança da informação que envolvem violação de dados pessoais?	0,00	0,25
9.4 A organização monitora proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais?	1,00	0,34
9.5 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?	0,00	0,12

O gráfico da Figura 11 possibilita comparar visualmente os valores das questões desta dimensão que foram calculados para a organização relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 11 - Valores da organização e valores médios na dimensão "Violação de Dados Pessoais"



2.9 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.

Na Tabela 10 são apresentadas as questões desta dimensão que compõem o indicador de

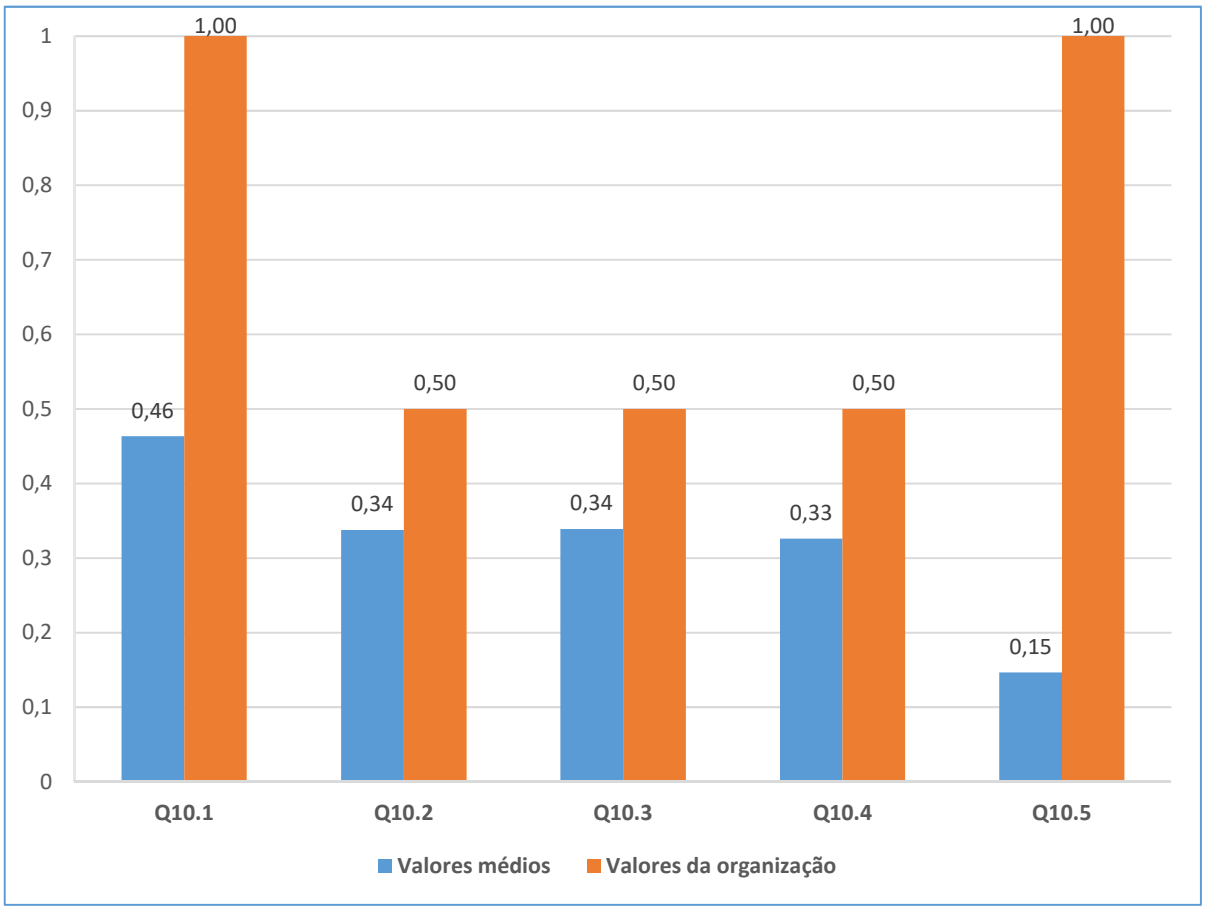
adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas.

Tabela 10 - Medidas de Proteção

Questões	Valores da organização	Valores médios
10.1 A organização é capaz de comprovar que adotou medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais?	1,00	0,46
10.2 A organização implementou processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam tratamento de dados pessoais?	0,50	0,34
10.3 A organização registra eventos das atividades de tratamento de dados pessoais?	0,50	0,34
10.4 A organização utiliza criptografia para proteger os dados pessoais?	0,50	0,33
10.5 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*)?	1,00	0,15

O gráfico da Figura 12 possibilita comparar visualmente os valores das questões desta dimensão que foram calculados para a organização relativamente aos valores médios calculados ao se considerar o conjunto das 382 organizações avaliadas.

Figura 12 - Valores da organização e valores médios na dimensão "Medidas de Proteção"



3 Respostas ao questionário

1. Identificação do respondente

2. Preparação

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

Sim (a organização concluiu 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.

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

Sim

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.

3. Contexto organizacional

3.1 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?

Sim

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.

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

Parcialmente (algumas categorias de titulares de dados pessoais foram identificadas).

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.

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

Parcialmente (a iniciativa ainda está em andamento).

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.

3.3.1 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?

Não aplicável

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.

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

Sim

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).

3.4.1 Caso exista controlador conjunto, 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).

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".

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

Parcialmente (alguns processos de negócio que realizam tratamento de dados pessoais foram identificados).

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.

3.5.1 A organização identificou quem são os responsáveis pelos 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).

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).

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

Parcialmente (alguns dados pessoais tratados pela organização foram identificados).

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.

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

Parcialmente (a organização identificou os locais onde são armazenados alguns dos dados pessoais que já foram identificados).

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.

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

Não

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.

4. Liderança

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

Sim

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.

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

Sim

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.

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

Sim

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.

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

Não

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.

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

Não

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.

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

Sim

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).

4.4 A organização nomeou o encarregado pelo tratamento de dados pessoais?

Sim

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.

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

Sim

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).

4.4.2 Em qual setor da organização está lotado o encarregado?

Jurídico

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.

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

Sim

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.

5. Capacitação

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

Não

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.

5.1.1 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?

Não aplicável

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.

5.2. 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).

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.

6. Conformidade do tratamento

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

Parcialmente (algumas finalidades das atividades de tratamento de dados pessoais foram identificadas e documentadas).

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.

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

Não

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.

6.1.2 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?

Não

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.

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

Parcialmente (as bases legais que fundamentam algumas das atividades de tratamento de dados pessoais da organização foram definidas e documentadas).

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.

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

Não

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.

6.4 A organização elaborou Relatório de Impacto à Proteção de Dados Pessoais?

Não.

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.

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

Não aplicável

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.

7. Direitos do titular

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

Sim

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 clarae 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.

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

Sim

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.

7.1.1.1 Favor informar o endereço da internet (URL) onde a política está publicada:

https://transparencia.cfm.org.br/images/Documentos/IN_CFM_003_2021.pdf

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

Parcialmente (foram implementados mecanismos para atender alguns 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.

8. Compartilhamento de dados pessoais

8.1 A organização identificou os dados pessoais são compartilhados com terceiros?

Parcialmente (alguns dados pessoais que são compartilhados com terceiros 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 7.5.3 e 7.5.4.

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

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

Sim (os compartilhamentos de dados pessoais 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.

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

Sim (a organização registra eventos relacionados à transferência de todos os 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.

8.1.3 Algum caso de compartilhamento envolve transferência internacional de dados pessoais?

Não

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.

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

Não aplicável

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.

9. Violação de dados pessoais

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

Não

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.

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

Não

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.

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

Não

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.

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

Sim

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.

9.5 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?

Não

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.

10. Medidas de proteção

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

Sim

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.

10.2 A organização implementou processo para registro, cancelamento e provisionamento de usuários em 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).

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 observe os princípios de "necessidade de conhecer" e "necessidade de uso".

10.3 A organização registra eventos das atividades de tratamento de dados pessoais?

Parcialmente (a organização registra os eventos de algumas 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).

10.4 A organização utiliza criptografia para proteger os dados pessoais?

Parcialmente (a organização utiliza criptografia para proteger alguns 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.

10.5 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*)?

Sim

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.