Auditoria para avaliar a adequação das organizações públicas federais à LGPD

Data de envio
30/03/2021 17:50:35

1. Identificação do respondente

1. Identificação do respondente

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

1.1 Dados do servidor responsável pela resposta ao questionário: [Nome:]
[redacted]

1.1 Dados do servidor responsável pela resposta ao questionário: [E-mail:]
[redacted]

1.1 Dados do servidor responsável pela resposta ao questionário: [Telefone (com DDD):]
[redacted]

1.1 Dados do servidor responsável pela resposta ao questionário: [Cargo/Função:]
[redacted]

2. Preparação

2. 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.

2.1 A organização conduziu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD?
Parcialmente (a organização iniciou, mas ainda não concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD). [A2]

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

3. Contexto organizacional

3. 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.

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 [Y]

3.2 A organização identificou as categorias de titulares de dados pessoais com os quais se relaciona?
Não (ainda não foi conduzida iniciativa para identificar as categorias de titulares de dados pessoais). [A3]

3.3 A organização conduziu iniciativa para identificar os operadores que realizam tratamento de dados pessoais em seu nome?
Não (ainda não foi conduzida iniciativa para identificar os operadores). [A4]

3.4 A organização avaliou se há tratamento de dados que envolva controlador conjunto?
Não [N]

3.5 A organização identificou os processos de negócio que realizam tratamento de dados pessoais?
Não (ainda não foi conduzida iniciativa para identificar os processos de negócio que realizam tratamento de dados pessoais). [A3]

3.6 A organização identificou quais são os dados pessoais tratados por ela?
Não (a organização não identificou os dados pessoais que são tratados por ela). [A3]

4. Liderança

4. 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.

4.1 A organização possui Política de Segurança da Informação ou instrumento similar?
Sim [Y]

4.1.1 Anexe a Política de Segurança da Informação (ou instrumento similar) da organização:
POSIC_UNIR_2019_V01_base_v4_Final_2029080297.pdf (303KB)

filecount - 4.1.1 Anexe a Política de Segurança da Informação (ou instrumento similar) da organização:
1

4.2 A organização possui Política de Classificação da Informação ou instrumento similar?
Não [N]

4.3 A organização possui Política de Proteção de Dados Pessoais (ou instrumento similar)?
Não [N]

4.4 A organização nomeou o encarregado pelo tratamento de dados pessoais?
Não [N]

5. Capacitação

5. 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.

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 [N]

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). [A3]

6. Conformidade do tratamento

6. Conformidade do tratamento

A organização deve ser capaz de provar que os tratamentos de dados pessoais que realiza são lícitos. Para isso é fundamental demonstrar que os princípios estabelecidos 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.

6.1 A organização identificou e documentou as finalidades das atividades de tratamento de dados pessoais?
Não (as finalidades das atividades de tratamento de dados pessoais ainda não foram identificadas e documentadas). [A3]

6.2 A organização identificou e documentou as bases legais que fundamentam as atividades de tratamento de dados pessoais?
Sim (as bases legais que fundamentam todas as atividades de tratamento de dados pessoais da organização foram definidas e documentadas). [A1]

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

6.4 A organização elaborou Relatório de Impacto à Proteção de Dados Pessoais?
Não. [A3]

7. Direitos do titular

7. Direitos do titular

A organização deve assegurar que os titulares tenham acesso a informações relacionadas ao tratamento de seus dados pessoais. Para isso, a organização deve publicar, de maneira clara e concisa, informações relativas ao tratamento de dados pessoais. A organização também deve estar preparada para atender todos os direitos dos titulares que são elencados na LGPD.

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

7.1 A organização possui Política de Privacidade (ou instrumento similar)?
Não [N]

7.2 Foram implementados mecanismos para atender os 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). [A3]

8. Compartilhamento de dados pessoais

8. 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.

8.1 A organização identificou os dados pessoais são compartilhados com terceiros?
Não (não houve iniciativa para identificar dados pessoais que são compartilhados com terceiros). [A3]

9. Violação de dados pessoais

9. 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.

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 [N]

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

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 [N]

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

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 [N]

10. Medidas de proteção

10. 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.

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

10.2 A organização implementou processo para registro, cancelamento e provisionamento de usuários em 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). [A3]

10.3 A organização registra eventos das atividades de tratamento de dados pessoais?
Não (a organização não registra os eventos de atividades de tratamento de dados pessoais). [A3]

10.4 A organização utiliza criptografia para proteger os dados pessoais?
Sim (a organização utiliza criptografia para proteger todos os dados pessoais). [A1]

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*)?
Não [N]