TRIBUNAL DE CONTAS DA UNIÃO

Auditoria sobre a implementação dos dispositivos da Lei Geral de Proteção de Dados Pessoais (LGPD) na União (TC 009.980/2024-5)

(Acórdão 1.372/2025-TCU-Plenário, Relatoria Min. Walton Alencar Rodrigues)

Relatório de *Feedback*

Organização:

Petróleo Brasileiro S.A.

(PETROBRAS)

Área Temática:

Outra

Todas as informações deste documento são consideradas públicas, conforme classificação do item 9.4 do Acórdão 1.372/2025-TCU-Plenário.

Sumário

Lista de Figuras

Lista de Tabelas

1 Introdução

Este relatório apresenta os resultados da organização **Petróleo Brasileiro S.A. (PETROBRAS)** relativos à auditoria realizada pelo TCU entre maio e setembro de 2024 para avaliar os controles implementados pelas organizações públicas federais para adequação à Lei 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais – LGPD (TC 009.980/2024-5; Acórdão 1372/2025-TCU-Plenário, de relatoria do Ministro Walton Alencar Rodrigues).

Ressalta-se que o TCU divulgará os resultados desta fiscalização conforme autorização do Plenário. Em todo caso, em atendimento ao princípio da transparência, recomenda-se que a própria organização também **publique em seu sítio institucional as informações contidas neste relatório**.

2 Avaliação da adequação à LGPD

O método utilizado para avaliar as organizações foi o de autoavaliação de controles internos (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 atual do respectivo ente com relação à implementação de medidas de adequação à LGPD, solicitando-se, adicionalmente, o envio das evidências correspondentes. Além de permitir que as organizações verificassem quais controles associados à LGPD foram implementados, as questões avaliadas também podem ser utilizadas como referência para a condução de futuras iniciativas de adequação, inclusive por parte dos próprios gestores e/ou das unidades de controle/auditoria interno/a das organizações.

As perguntas do questionário tiveram como referências principais a própria LGPD (Lei 13.709/2018), a Lei 12.527/2011 (Lei de Acesso à Informação – LAI), a norma técnica ABNT NBR ISO/IEC 27701:2019 ("Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes"), além de outros normativos (*e.g.* IN SGD/ME 117/2020 [Dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais na APF], IN GSI/PR 5/2021 [Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da APF]) e documentos elaborados pela Autoridade Nacional de Proteção de Dados – ANPD (Resolução CD/ANPD 15/2024 [Regulamento de Comunicação de Incidente de Segurança], "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado", "Guia Orientativo – Tratamento de dados pessoais pelo Poder Público").

Desconsiderando-se a parte inicial (identificação do respondente) e as questões que demandavam anexar documentos, o questionário contemplou, no total, 16 questões e, assim como a auditoria anterior (TC 039.606/2020-1), foi estruturado em torno de duas perspectivas e nove dimensões (Figura 1). Algumas das questões só eram mostradas de forma condicionada às respostas do gestor em perguntas anteriores.

Figura 1 - Questionário da Auditoria LGPD 2024 - Duas perspectivas e nove dimensões

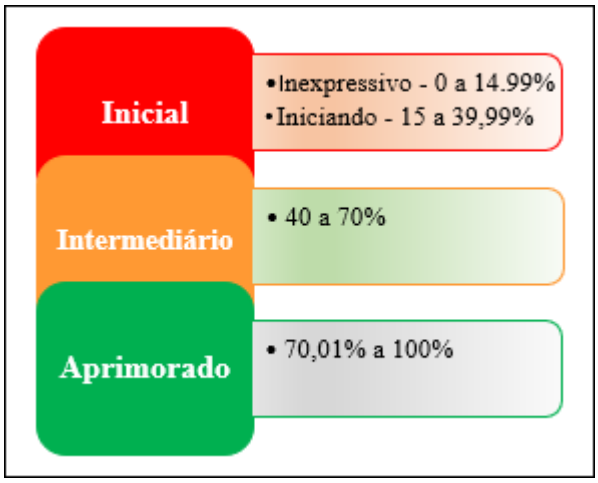
De modo a consolidar os dados obtidos e a possibilitar comparações entre as diferentes organizações auditadas, no que tange ao nível de adequação à LGPD, foi elaborada fórmula matemática para, com base nas respostas fornecidas por cada órgão/entidade, calcular um "indicador de adequação à LGPD" (iLGPD), entre 0 e 100%, o qual representa, em última instância, o grau de implementação das medidas de adequação avaliadas na auditoria. A metodologia de cálculo desse indicador é resumida na Tabela 1.

Tabela 1 - Resumo da metodologia de cálculo do indicador de adequação à LGPD (iLGPD)

Aspecto	Regra adotada
Questões do "Tipo A" (resposta única)	Notas (arredondadas) atribuídas a partir da aplicação de escala gradativa com taxa exponencial de 0.35
Questões do "Tipo B" (múltiplas respostas)	Notas (arredondadas) atribuídas a partir da aplicação de escala linear simples
Subindicadores de cada dimensão (iPrep, iOrg, iLid, iCap, iConf, iDir, iComp, iResp e iProt)	A nota do subindicador corresponde à nota da respectiva questão, à exceção da dimensão "Direitos do titular", cujo subindicador recebe a fórmula: iDir = 0,4*Q7.1 + 0,6*Q7.2
Indicador de adequação à LGPD	iLGPD = (iPrep + iOrg + iLid*2 + iCap*1,5 + iConf*2 + iDir*2 + iComp*2 + iResp*1,5 + iProt*2) / 15

A partir do cálculo do iLGPD (valor entre 0 e 100%), foram definidos quatro níveis/faixas de adequação à LGPD: "Inexpressivo" ($0 \leq$ iLGPD $< 15\%$), "Iniciando" ($15\% \leq$ iLGPD $< 40\%$), "Intermediário" ($40\% \leq$ iLGPD $\leq 70\%$) e "Aprimorado" ($70\% <$ iLGPD $\leq 100\%$) (Figura 2).

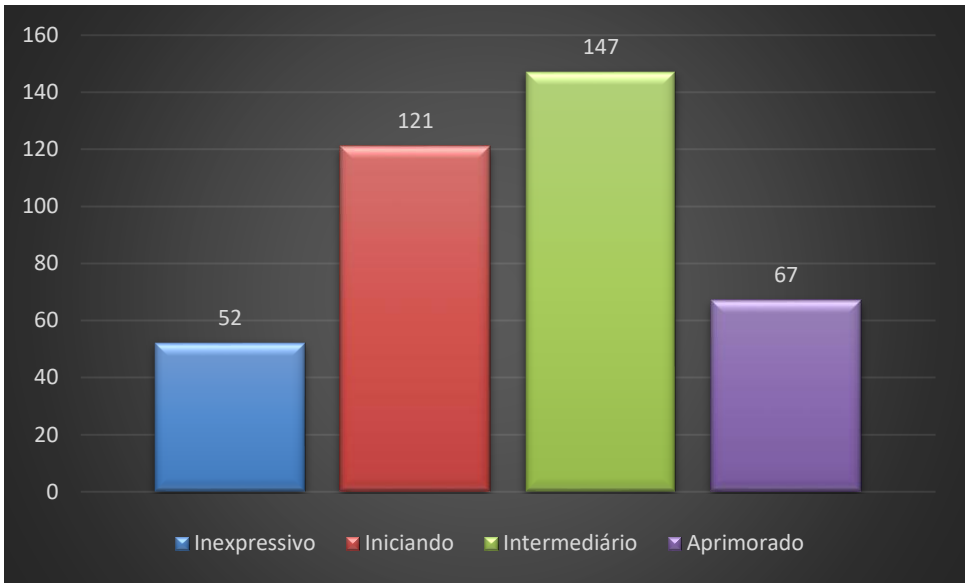
Figura 2 - Quatro níveis/faixas de adequação à LGPD



A organização **PETROBRAS** obteve o valor **88,78%** para o respectivo indicador de adequação à LGPD, o que corresponde, então, ao nível "**Aprimorado**".

O gráfico da **Erro! Fonte de referência não encontrada.** apresenta a distribuição das 387 organizações em cada um dos quatro níveis de adequação.

Figura 3 - Distribuição das 387 organizações por níveis de adequação à LGPD



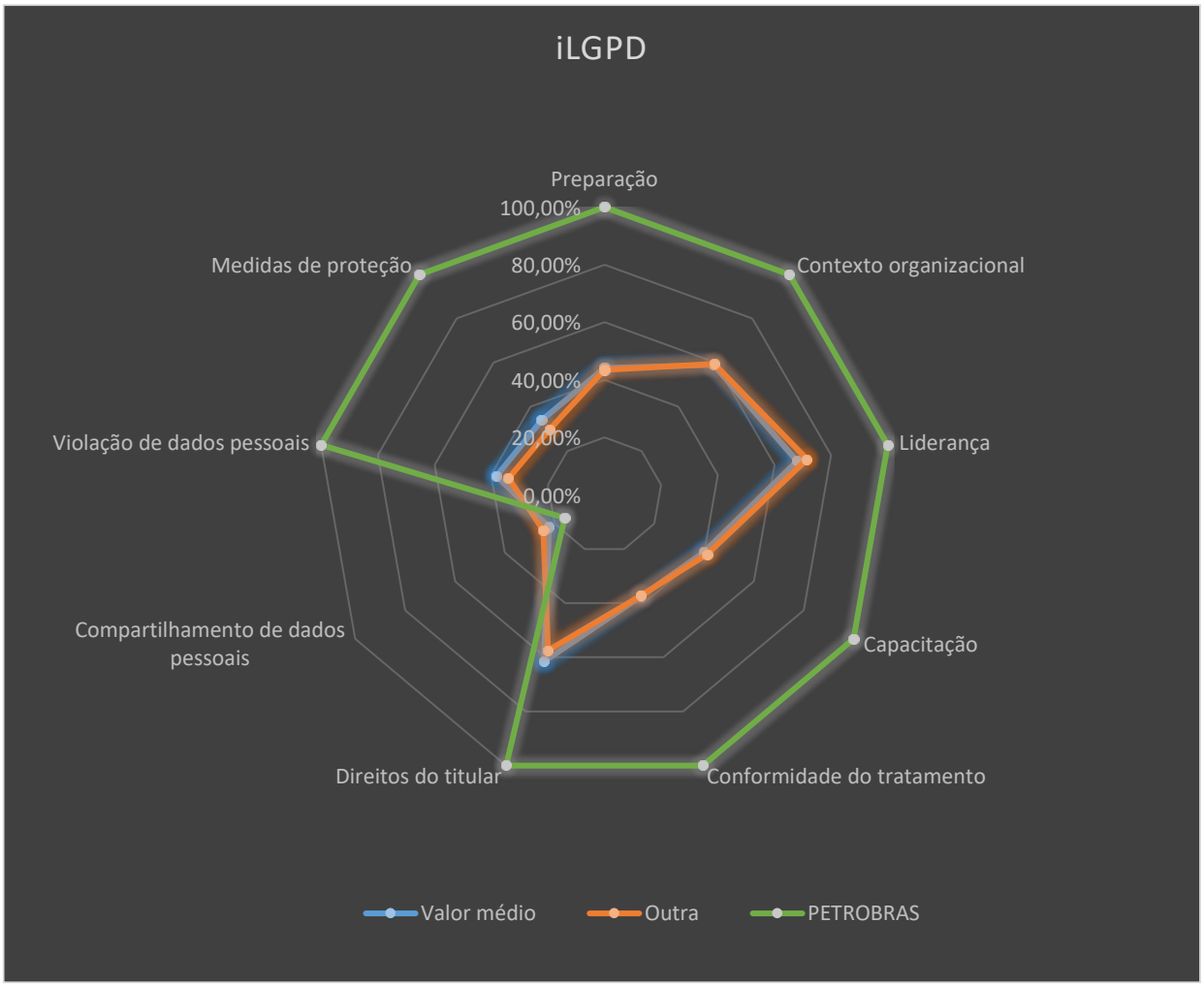
O iLGPD pode ser desmembrado e apresentado levando-se em consideração os valores referentes a cada uma das nove dimensões do questionário: "Preparação", "Contexto Organizacional", "Liderança", "Capacitação", "Conformidade do Tratamento", "Direitos do Titular", "Compartilhamento de Dados Pessoais", "Violação de Dados Pessoais" e "Medidas de Proteção". A Tabela 2, então, apresenta um resumo da avaliação da organização **PETROBRAS** contendo os valores dos subindicadores relativos a cada dimensão do questionário, bem como do indicador geral de adequação à LGPD, possibilitando comparar os valores da própria organização com os valores médios das organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

Tabela 2 - Resumo da avaliação da adequação à LGPD

Dimensão do questionário	**PETROBRAS**	**Outra**	**Valores médios das 387 organizações**
Preparação (iPrep)	100,00%	43,44%	44,14%
Contexto Organizacional (iOrg)	100,00%	59,40%	59,00%
Liderança (iLid)	100,00%	71,47%	68,04%
Capacitação (iCap)	100,00%	41,26%	39,87%
Conformidade do Tratamento (iConf)	100,00%	37,18%	37,44%
Direitos do Titular (iDir)	100,00%	57,49%	61,51%
Compartilhamento de Dados Pessoais (iComp)	15,92%	24,52%	22,30%
Violação de Dados Pessoais (iResp)	100,00%	33,87%	38,14%
Medidas de Proteção (iProt)	100,00%	29,67%	33,95%
Indicador de adequação à LGPD (iLGPD)	**88,79%**	**43,75%**	**44,44%**

O gráfico da Figura 4 possibilita comparar visualmente os valores dos subindicadores relativos a cada uma das nove dimensões que foram calculados para a organização **Petróleo Brasileiro S.A.** com os valores médios calculados para as organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

Figura 4 - Valores do(a) **PETROBRAS** e valores médios por dimensão 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 estarão nos mesmos patamares em todas as dimensões.

2.1 Preparação (subindicador iPrep)

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

A questão desta dimensão, do "Tipo A" (resposta única), aborda aspectos relacionados à identificação, ao planejamento e à concretização de medidas preparatórias necessárias à adequação.

Questão 2.1 (TIPO A): A organização conduziu iniciativas para identificar, planejar e executar medidas preparatórias com vistas a se adequar à LGPD?
A1) Não se aplica
A2) Não (a organização não realizou medidas preparatórias com vistas a se adequar à LGPD)
A3) A organização iniciou, mas ainda não concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD

A4) A organização concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD (possui plano de ação, plano de projeto ou documento similar para direcionar os esforços nesse sentido), porém ainda não formalizou normativo interno relacionado à proteção e à privacidade de dados
A5) A organização concluiu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD e já publicou uma política (ou documento similar) que considera os princípios e aspectos gerais relacionados ao tratamento de dados
A6) A organização já mapeou seus principais processos de tratamento de dados (natureza, escopo, finalidade, benefícios, probabilidade e gravidade dos riscos associados) e publicou normativos internos que tratam dos aspectos mais importantes relacionados à proteção e à privacidade de dados, porém ainda não possui um programa de governança em privacidade de dados implementado
A7) A organização já mapeou todos os processos de tratamento de dados (natureza, escopo, finalidade, benefícios, probabilidade e gravidade dos riscos associados), publicou normativos internos que tratam dos temas proteção e privacidade de dados de forma abrangente e possui programa de governança em privacidade de dados implementado, periodicamente monitorado/avaliado e atualizado continuamente

Das opções disponíveis, a organização **PETROBRAS** assinalou "**A7**".

O gráfico da Figura 5 possibilita comparar visualmente os valores do subindicador relativo à dimensão "Preparação" (iPrep) que foram calculados para o(a) **PETROBRAS** com os valores médios calculados para as organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

Figura 5 - Dimensão "Preparação" (iPrep) - Valor do(a) **PETROBRAS** e valores médios

2.2 Contexto Organizacional (subindicador iOrg)

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.

A questão desta dimensão, do "Tipo B" (múltiplas respostas), aborda aspectos relacionados ao mapeamento dos normativos correlatos à proteção de dados pessoais que devem ser respeitados pela organização, à identificação das partes interessadas e às análises dos diferentes tipos de dados pessoais tratados pela organização e dos processos organizacionais que realizam o tratamento desses dados.

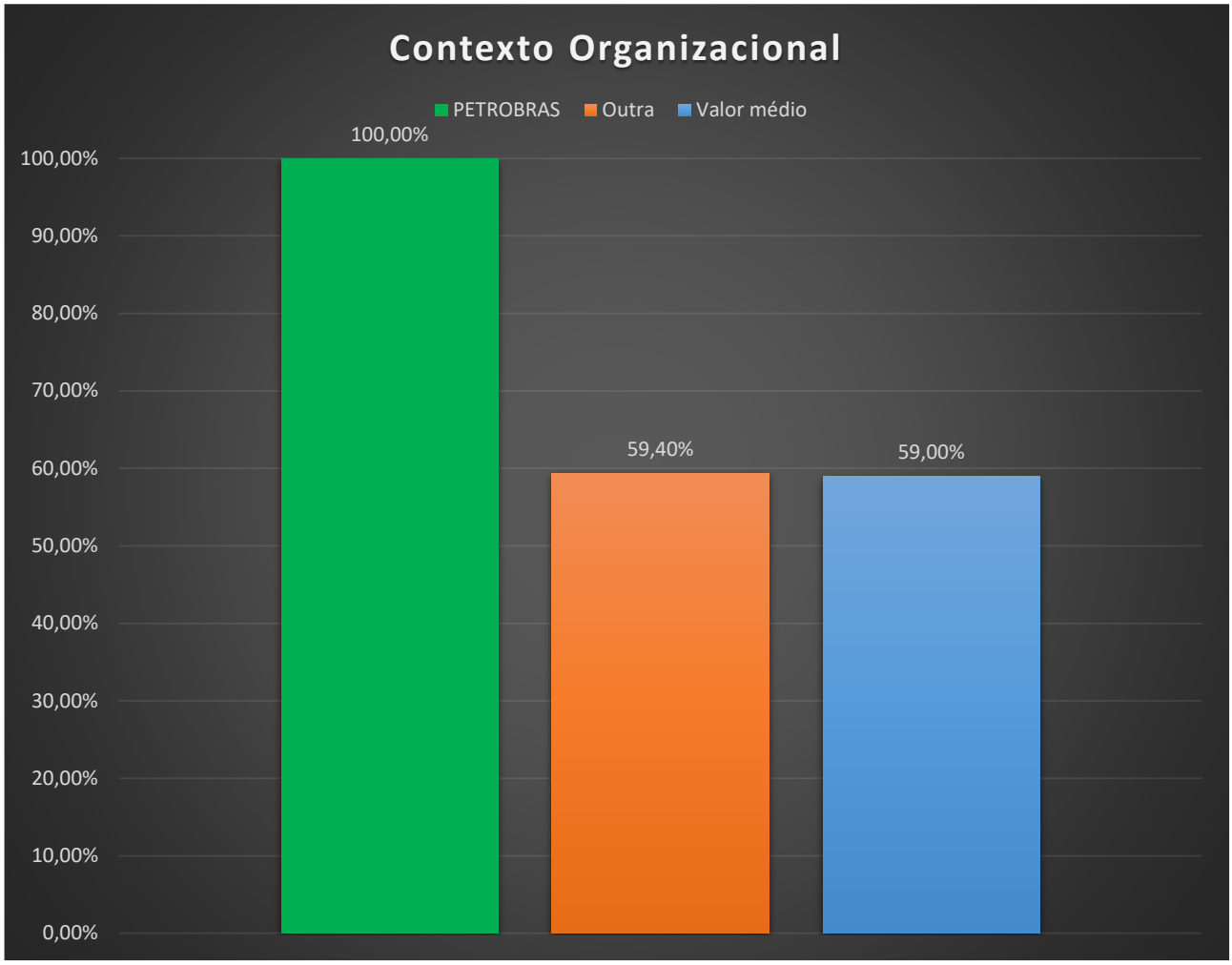
A Tabela 3 apresenta os diferentes itens avaliados na questão desta dimensão, os quais compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização com os valores médios das organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

Tabela 3 - Dimensão "Contexto Organizacional" (iOrg) - Respostas e valor do(a) **PETROBRAS** e valores médios

Questão 3.1 (TIPO B): A organização conduziu iniciativa com vistas a identificar:	**PETROBRAS implementou esta medida?**	**Percentual de Outra que implementou esta medida**	**Percentual das 387 organizações que implementou esta medida**
outros normativos, além da LGPD	Sim	77,33%	76,49%
as diferentes categorias de titulares de dados pessoais com os quais se relaciona	Sim	57,33%	66,63%
os operadores que realizam tratamento de dados pessoais em seu nome	Sim	58,67%	58,40%
se há tratamento de dados que envolva controlador conjunto	Sim	33,33%	35,92%
e adequar os instrumentos contratuais firmados com os operadores e os controladores conjuntos identificados	Sim	61,33%	62,27%
os processos de negócio que realizam tratamento de dados pessoais e os respectivos responsáveis	Sim	62,67%	54,78%
os dados pessoais tratados pela organização	Sim	70,67%	71,06%
os locais de armazenamento dos dados pessoais tratados pela organização	Sim	62,67%	65,37%
e avaliar os riscos associados aos processos de tratamento de dados pessoais que foram identificados	Sim	50,67%	41,09%
a organização ainda não conduziu iniciativa com vistas a identificar qualquer dos objetos mencionados nos itens anteriores	Não	10,67%	10,34%
Subindicador iOrg	**100,00%**	**59,40%**	**59,00%**

O gráfico da Figura 6 possibilita comparar visualmente os valores do subindicador relativo à dimensão "Contexto Organizacional" (iOrg) que foram calculados para o(a) **PETROBRAS** com os valores médios calculados para as organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

Figura 6 - Dimensão "Contexto Organizacional" (iOrg) - Valor do(a) **PETROBRAS** e valores médios



2.3 Liderança (subindicador iLid)

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

A elaboração e a ampla divulgação de políticas relacionadas à proteção de dados pessoais, bem como a nomeação de um encarregado pelo tratamento de dados pessoais (normalmente chamado de DPO, do inglês *Data Protection Officer*), com autonomia para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD, são ações fundamentais para o processo de adequação à LGPD.

A questão desta dimensão, do "Tipo B" (múltiplas respostas), aborda aspectos relacionados à nomeação do encarregado e à formalização de políticas que busquem assegurar a segurança das informações e a proteção dos dados pessoais.

A Tabela 4 apresenta os diferentes itens avaliados na questão desta dimensão, os quais compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização com os valores médios das organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

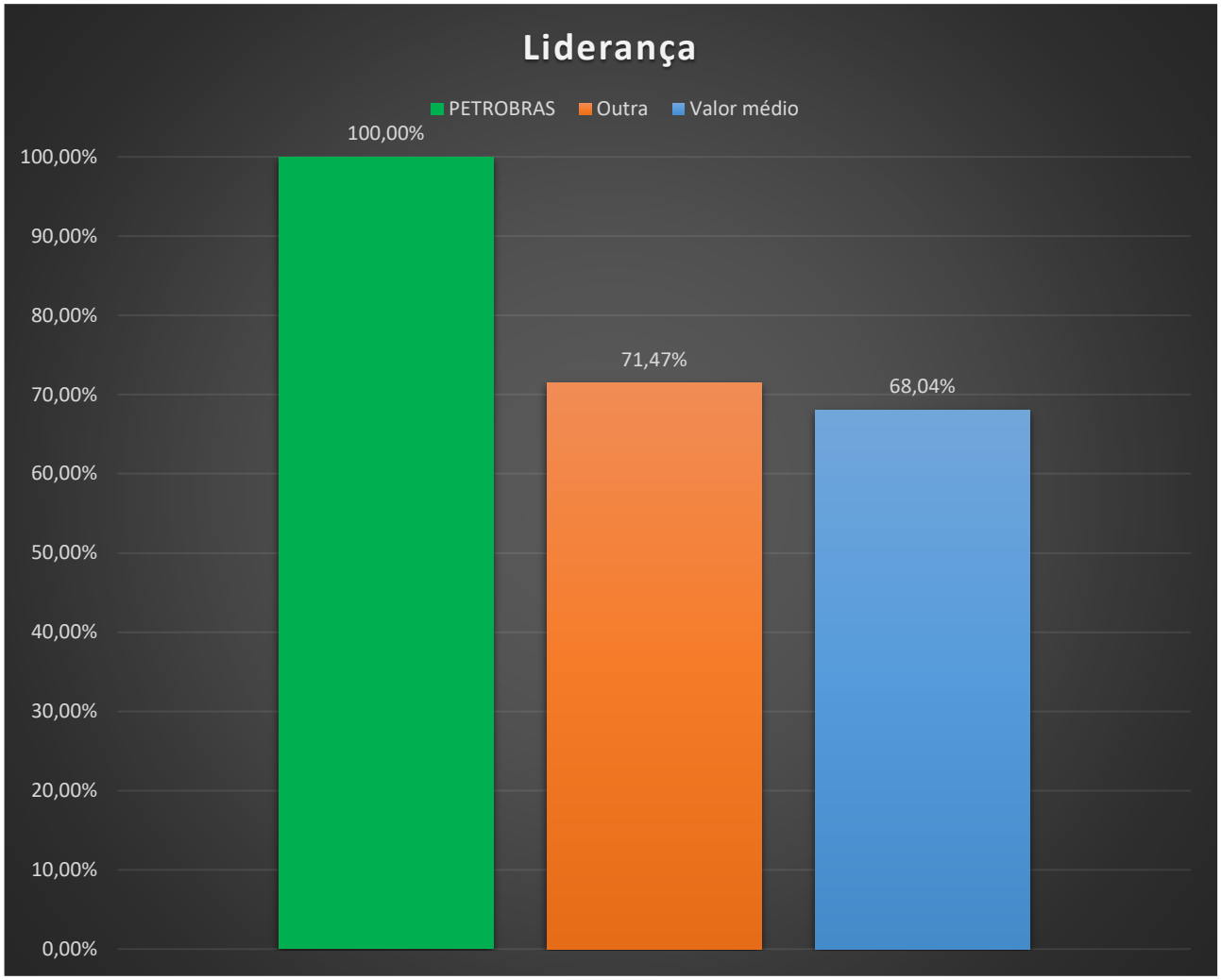
Tabela 4 - Dimensão "Liderança" (iLid) - Respostas e valor do(a) **PETROBRAS** e valores médios

Questão 4.1 (TIPO B): A organização:	**PETROBRAS implementou esta medida?**	**Percentual de Outra que implementou esta medida**	**Percentual das 387 organizações que implementou esta medida**
instituiu formalmente e mantém atualizada política de segurança da informação	Sim	88,00%	79,33%
instituiu formalmente e mantém atualizada política de classificação da informação	Sim	36,00%	30,23%
instituiu formalmente e mantém atualizada política de proteção de dados pessoais	Sim	48,00%	57,11%
nomeou o encarregado pelo tratamento de dados pessoais (*Data Protection Officer* – DPO)*	Sim	93,33%	87,60%
divulga em seu sítio eletrônico institucional a identidade e as informações de contato do encarregado pelo tratamento de dados pessoais*	Sim	90,67%	84,24%
ainda não atende nenhum dos itens	Não	2,67%	6,20%
Subindicador iLid	**100,00%**	**71,47%**	**68,04%**

*Nesta questão, foi atribuída a pontuação de 30% ao item relativo à nomeação do DPO e, consequentemente, apenas 10% ao último item (divulgação dos dados do DPO no sítio da organização). As três primeiras opções pontuaram 20% cada, normalmente.

O gráfico da Figura 7 possibilita comparar visualmente os valores do subindicador relativo à dimensão "Liderança" (iLid) que foram calculados para o(a) **PETROBRAS** com os valores médios calculados para as organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

Figura 7 - Dimensão "Liderança" (iLid) - Valor do(a) **PETROBRAS** e valores médios



2.4 Capacitação (subindicador iCap)

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

A conscientização é importante para que os colaboradores conheçam a legislação, bem como as políticas e normativos institucionais relacionados à proteção de dados pessoais, e para que reconheçam como suas decisões e ações podem afetar a preservação da privacidade dos titulares de dados.

As ações de capacitação devem considerar diferentes níveis de envolvimento dos colaboradores no tema, de forma que aquelas pessoas envolvidas em atividades críticas relacionadas ao tratamento de dados pessoais e que ocupam funções com responsabilidades essenciais relacionadas à proteção de dados pessoais recebam treinamento diferenciado, além do nível básico fornecido aos demais colaboradores.

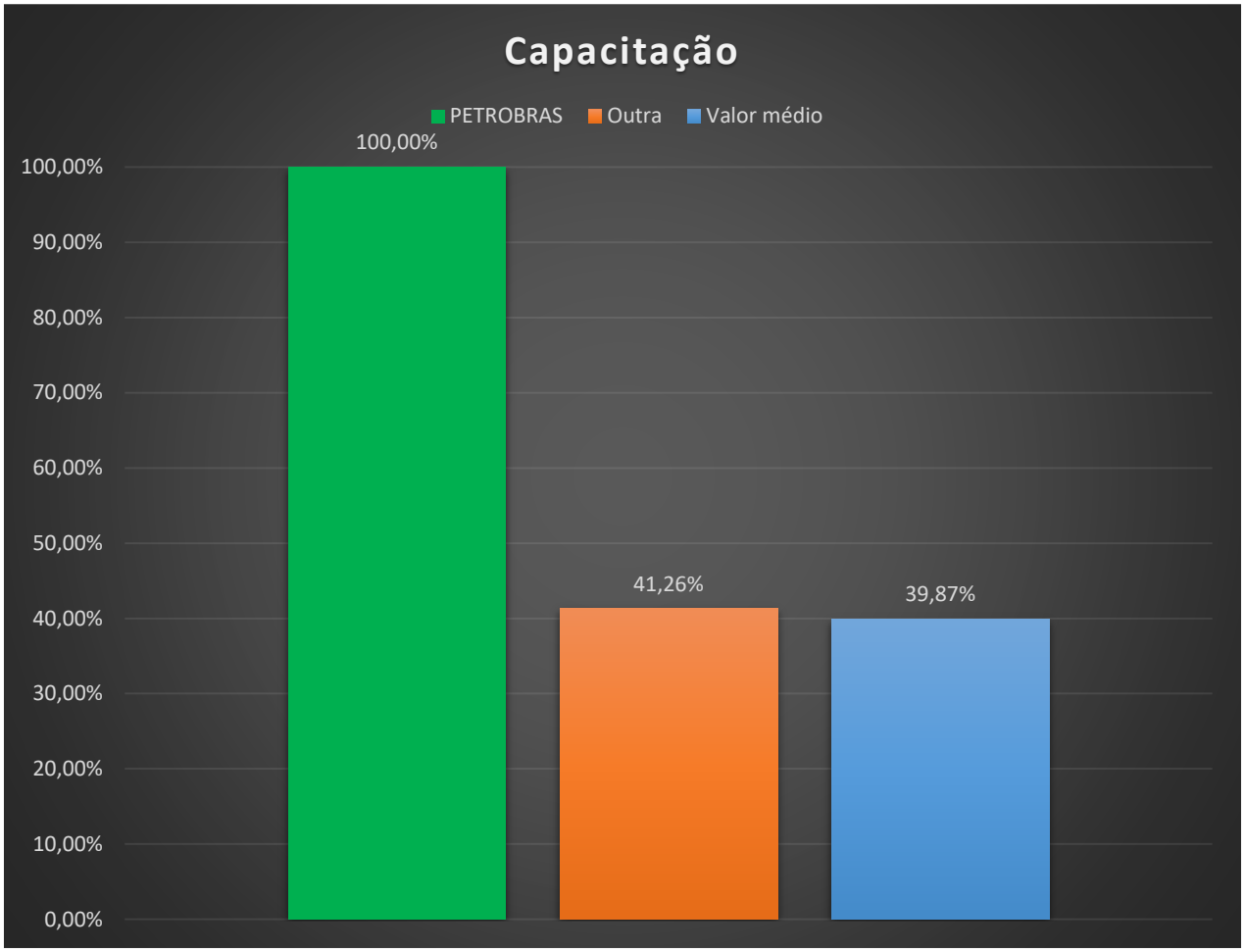
As questões desta dimensão, então, abordam aspectos atinentes à avaliação, ao planejamento e à realização de ações de capacitação relacionadas à privacidade e à proteção de dados pessoais, bem como à necessidade de harmonizar a LGPD e a LAI. Esta dimensão contemplou as questões 5.1, do "Tipo A" (resposta única), e 5.2, do "Tipo B" (múltiplas respostas), sendo que esta última não foi utilizada para composição do iLGPD.

Questão 5.1 (TIPO A): Acerca da capacitação dos seus colaboradores em proteção de dados pessoais, a organização:
A1) Não se aplica
A2) Não possui PLANO DE CAPACITAÇÃO (ou instrumento similar) e seus colaboradores ainda não realizaram treinamento em proteção de dados pessoais
A3) Não possui PLANO DE CAPACITAÇÃO (ou instrumento similar), mas colaboradores específicos já realizaram treinamento em proteção de dados pessoais
A4) Possui PLANO DE CAPACITAÇÃO (ou instrumento similar) e, apesar de este não contemplar a temática de proteção de dados pessoais de maneira específica, já realizou treinamento abrangente (não direcionado apenas a determinados colaboradores) nessa área
A5) Possui PLANO DE CAPACITAÇÃO (ou instrumento similar), contemplou nesse documento a temática de proteção de dados pessoais e já realizou treinamento da maioria dos colaboradores nessa área
A6) Possui PLANO DE CAPACITAÇÃO (ou instrumento similar), contemplou nesse documento a temática de proteção de dados pessoais, incluindo a necessidade de treinamento diferenciado para as pessoas que exercem funções com responsabilidades essenciais quanto à proteção de dados pessoais, e já realizou treinamento de todos os colaboradores nessa área

Das opções disponíveis na questão 5.1, a organização **PETROBRAS** assinalou "**AO06**".

O gráfico da Figura 8 possibilita comparar visualmente os valores do subindicador relativo à dimensão "Capacitação" (iCap) que foram calculados para o(a) **PETROBRAS** com os valores médios calculados para as organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

Figura 8 - Dimensão "Capacitação" (iCap) - Valor do(a) **PETROBRAS** e valores médios



A Tabela 5 apresenta os diferentes itens avaliados na questão 5.2, possibilitando comparar os valores da própria organização com os valores médios das organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

Tabela 5 - Dimensão "Capacitação" (Questão 5.2) - Respostas do(a) **PETROBRAS** e valores médios

Questão 5.2 (TIPO B): Acerca das ações de capacitação em proteção de dados pessoais realizadas nos últimos 3 (três) anos, a organização:	**PETROBRAS implementou esta medida?**	**Percentual de Outra que implementou esta medida**	**Percentual das 387 organizações que implementou esta medida**
levou em consideração a necessidade de complementar a capacitação dos participantes nesses treinamentos com conteúdo sobre transparência da gestão relativa às informações de interesse coletivo ou geral	Sim	34,67%	38,50%
efetivamente capacitou no tema transparência da gestão relativa às informações de interesse coletivo ou geral (LAI) mais de 50% dos colaboradores que receberam treinamento em proteção de dados pessoais	Não	13,33%	11,89%
ofereceu ação de capacitação que tenha abordado conjuntamente, de forma integrada, LGPD e LAI	Sim	36,00%	38,76%
orientou os participantes nesses treinamentos, mesmo que *a posteriori*, sobre a necessidade de observarem os enunciados da CGU divulgados por meio da Portaria Normativa CGU 71/2023	Não	13,33%	14,73%

orientou os participantes nesses treinamentos, mesmo que *a posteriori*, sobre a necessidade de observarem as diretrizes e orientações publicadas pela CGU por meio do "Parecer sobre acesso à informação para atender ao despacho presidencial de 1º de janeiro de 2023"	Não	13,33%	11,37%
não atendeu nenhum dos itens anteriores	Não	32,00%	27,91%

2.5 Conformidade do Tratamento (subindicador iConf)

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 do art. 6º da LGPD são seguidos e que os tratamentos são fundamentados em, ao menos, uma das bases legais descritas na legislação.

A questão desta dimensão, do "Tipo B" (múltiplas respostas), aborda aspectos atinentes à conformidade das atividades de tratamento de dados pessoais realizadas pela organização frente a alguns dos princípios da LGPD, inclusive se esses tratamentos estão fundamentados em alguma base legal. Também é avaliado se a organização mantém registro das operações de tratamento de dados pessoais que realiza.

A Tabela 6 apresenta os diferentes itens avaliados na questão desta dimensão, os quais compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização com os valores médios das organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

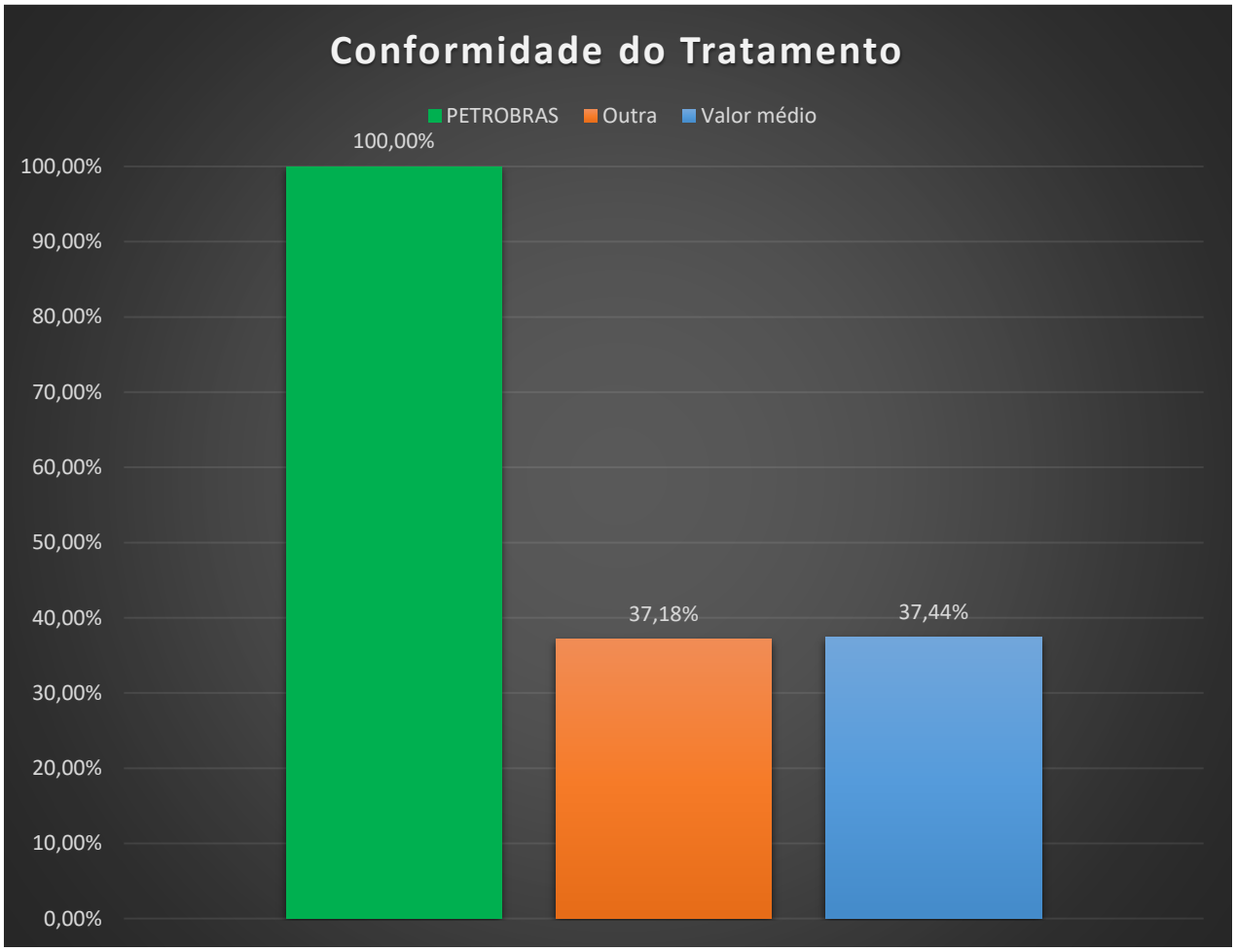
Tabela 6 - Dimensão "Conformidade do Tratamento" (iConf) - Respostas e valor do(a) **PETROBRAS** e valores médios

Questão 6.1 (TIPO B): A organização:	**PETROBRAS implementou esta medida?**	**Percentual de Outra que implementou esta medida**	**Percentual das 387 organizações que implementou esta medida**
identificou e documentou as finalidades de todas as suas principais atividades de tratamento de dados pessoais	Sim	48,00%	49,10%
avaliou se coleta apenas os dados estritamente necessários	Sim	40,00%	40,83%
avaliou se os dados pessoais são retidos/armazenados durante o tempo estritamente necessário	Sim	36,00%	33,59%
identificou e documentou as bases legais que fundamentam todas as suas principais atividades de tratamento de dados pessoais	Sim	42,67%	50,65%
possui registro(s) (*e.g.* inventário[s] de dados pessoais) instituído(s) para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais	Sim	44,00%	44,44%
catalogou no(s) registro(s)/inventário(s) de dados pessoais informações que abrangem todas as suas principais atividades de tratamento de dados pessoais	Sim	37,33%	39,02%
mantém registro das operações de tratamento de dados pessoais que realiza	Sim	28,00%	30,23%
já elaborou algum RIPD (Relatório de Impacto à Proteção de Dados Pessoais)	Sim	33,33%	27,65%

já implementou controles para mitigar os riscos identificados por meio da elaboração de RIPD	Sim	25,33%	21,45%
ainda não atende nenhum dos itens anteriores	Não	33,33%	32,30%
Subindicador iConf	**100,00%**	**37,18%**	**37,44%**

O gráfico da Figura 9 possibilita comparar visualmente os valores do subindicador relativo à dimensão "Conformidade do Tratamento" (iConf) que foram calculados para o(a) **PETROBRAS** com os valores médios calculados para as organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

Figura 9 - Dimensão "Conformidade do Tratamento" (iConf) - Valor do(a) **PETROBRAS** e valores médios



2.6 Direitos do Titular (subindicador iDir)

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

As questões desta dimensão, então, abordam aspectos atinentes à elaboração da Política de Privacidade e ao atendimento dos direitos do titular de dados pessoais. Esta dimensão contemplou as questões 7.1, do "Tipo A" (resposta única), e 7.2, do "Tipo B" (múltiplas respostas).

Questão 7.1 (TIPO A): A organização elaborou e divulga em seu sítio eletrônico institucional Política de Privacidade (ou instrumento similar)?
A1) Não se aplica
A2) A organização NÃO ELABOROU POLÍTICA DE PRIVACIDADE (ou instrumento similar)
A3) A organização ELABOROU A POLÍTICA DE PRIVACIDADE (ou instrumento similar), MAS NÃO A DIVULGA em seu sítio eletrônico institucional
A4) A organização ELABOROU A POLÍTICA DE PRIVACIDADE (ou instrumento similar) E A DIVULGA em seu sítio eletrônico institucional

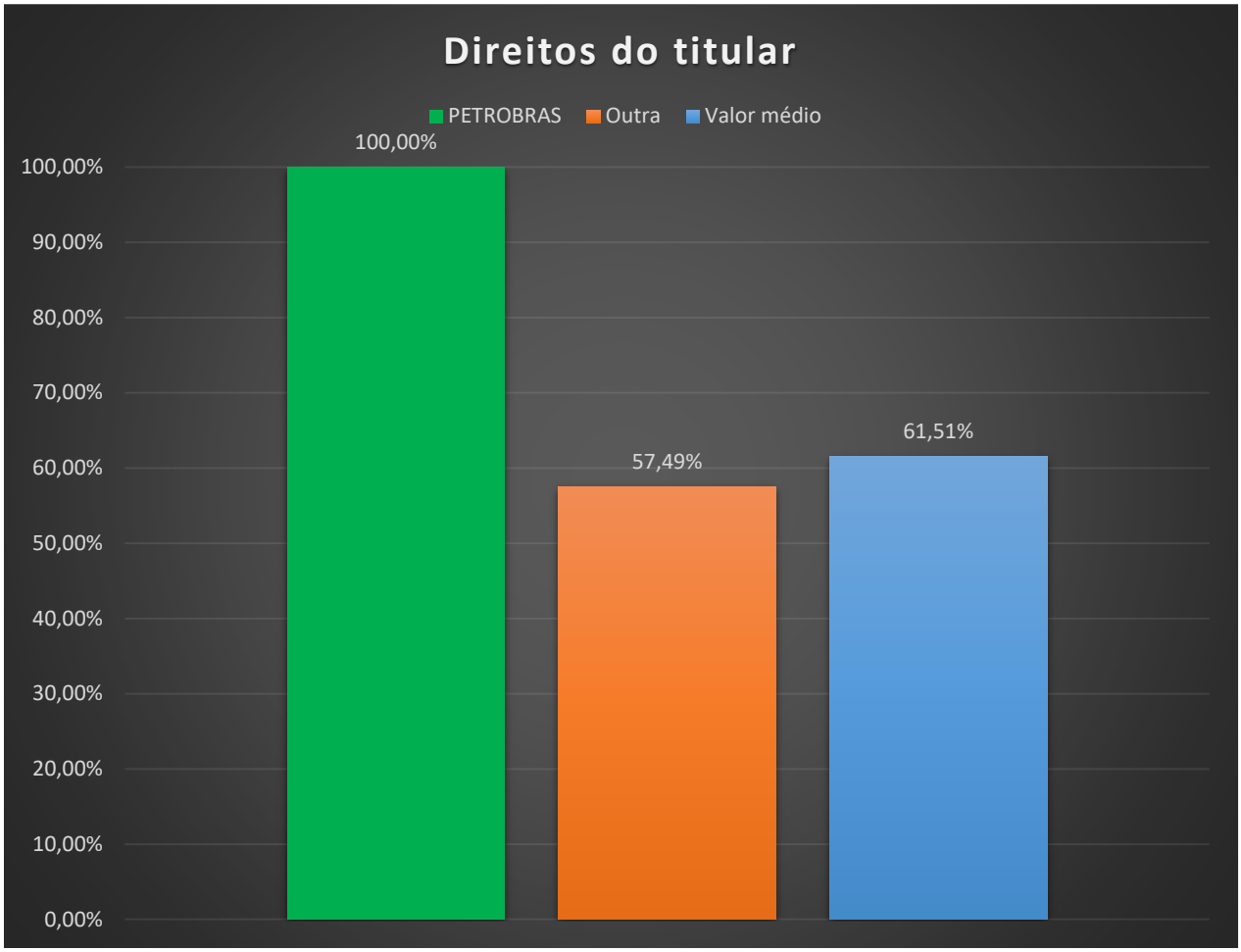
Das opções disponíveis na questão 7.1, a organização **PETROBRAS** assinalou "**AO04**".

Questão 7.2 (TIPO A): Foram implementados mecanismos para atender os direitos dos titulares aplicáveis à organização, relacionados à obtenção de informações sobre o tratamento dos dados, de modo geral (LGPD, art. 9º), bem como sobre os seus dados específicos e o respectivo tratamento (art. 18)?
A1) Não se aplica
A2) Não foram implementados mecanismos para atender direitos dos titulares (LGPD, arts. 9º e 18)
A3) Foram implementados mecanismos para atender alguns dos direitos dos titulares (LGPD, arts. 9º e 18), mas não todos
A4) Foram implementados mecanismos para atender todos os direitos dos titulares (LGPD, arts. 9º e 18) aplicáveis à organização

Das opções disponíveis na questão 7.2, a organização **PETROBRAS** assinalou "**AO04**".

O gráfico da Figura 10 possibilita comparar visualmente os valores do subindicador relativo à dimensão "Direitos do Titular" (iDir) que foram calculados para o(a) **PETROBRAS** com os valores médios calculados para as organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

Figura 10 - Dimensão "Direitos do Titular" (iDir) - Valor do(a) **PETROBRAS** e valores médios



2.7 Compartilhamento de Dados Pessoais (subindicador iComp)

A organização deve identificar, avaliar e documentar detalhes relacionados aos compartilhamentos de dados pessoais com terceiros, tendo em vista que a realização de compartilhamento de dados pessoais demanda a adoção de controles adequados com vistas a mitigar os riscos que possam comprometer a segurança e a proteção desses dados.

Diante disso, a LGPD defende 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 eventual transferência internacional desses dados.

As questões desta dimensão, então, abordam aspectos atinentes à identificação dos dados pessoais que são compartilhados com terceiros, à devida avaliação e adequação dessas operações frente aos critérios previstos na LGPD, ao registro dos eventos relacionados a esses compartilhamentos, às transferências internacionais de dados pessoais e ao tratamento de dados pessoais em solução de computação em nuvem. Esta dimensão contemplou as questões 8.1, 8.1.1 e 8.1.1.1, todas do "Tipo A" (resposta única), e 8.1.2, do "Tipo B" (múltiplas respostas), sendo que apenas a primeira foi utilizada para composição do iLGPD.

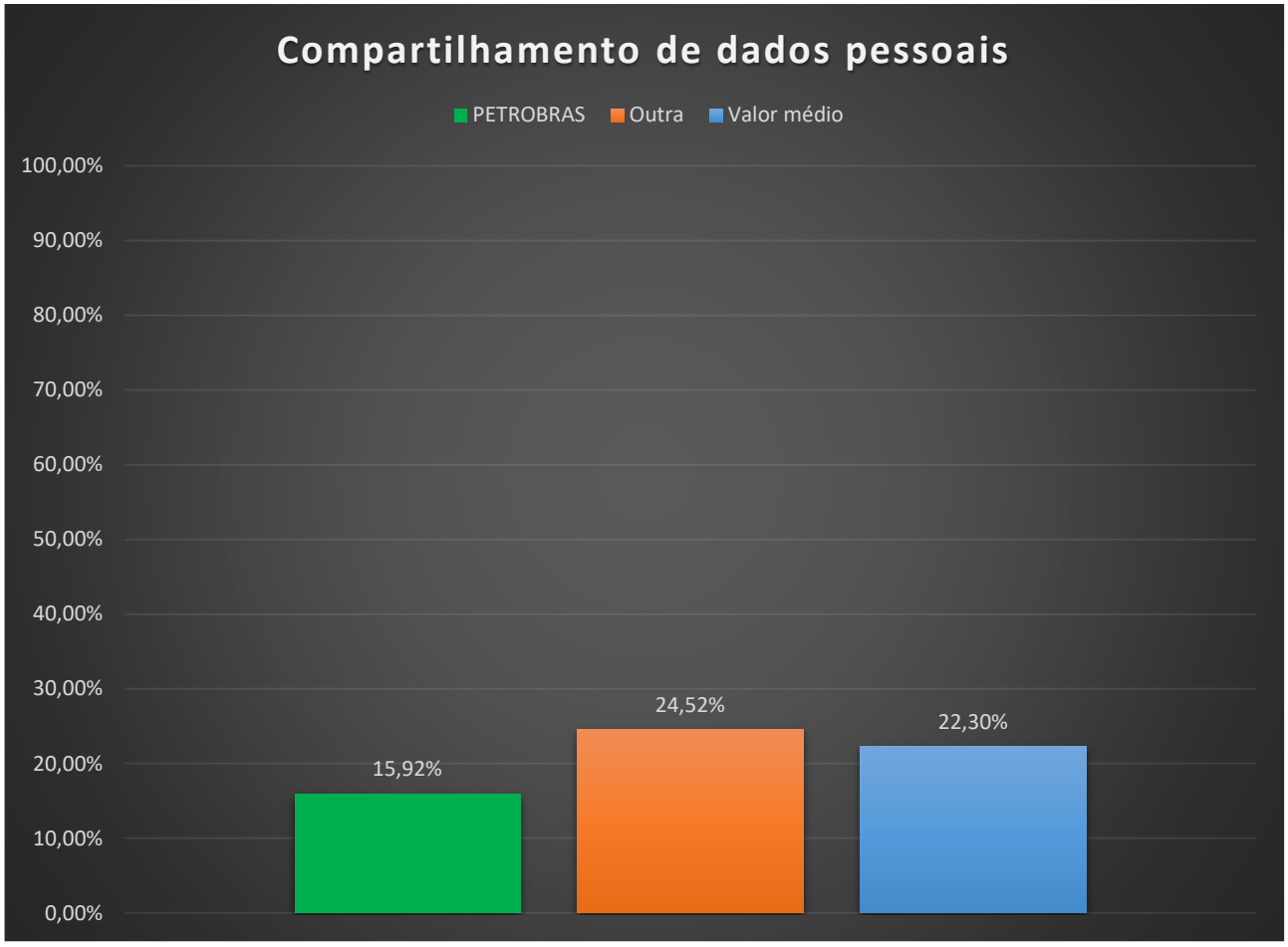
Tendo em vista que nem todas as organizações realizam transferência internacional de dados pessoais, as respostas às questões 8.1.1 e 8.1.1.1 foram excluídas deste relatório de *feedback*.

Questão 8.1 (TIPO A): Quanto aos compartilhamentos de dados pessoais com terceiros, a organização:
A1) Não se aplica
A2) AINDA NÃO AVALIOU se os realiza ou AINDA NÃO IDENTIFICOU todos os dados eventualmente compartilhados
A3) AVALIOU se há esses compartilhamentos e, nos casos detectados, IDENTIFICOU todos os dados eventualmente compartilhados
A4) IDENTIFICOU todos os dados pessoais compartilhados com terceiros e INICIOU A AVALIAÇÃO desses compartilhamentos, porém ainda não pode atestar que todos estejam em conformidade com os critérios legais (LGPD, arts. 26-27)
A5) IDENTIFICOU todos os dados pessoais compartilhados, AVALIOU os compartilhamentos e ATESTA que todos ESTÃO EM CONFORMIDADE COM OS CRITÉRIOS LEGAIS (LGPD, arts. 26-27), apesar de ainda não manter registro dos eventos relacionados a cada compartilhamento
A6) IDENTIFICOU todos os dados pessoais compartilhados, AVALIOU os compartilhamentos, ATESTA que todos ESTÃO EM CONFORMIDADE COM OS CRITÉRIOS LEGAIS (LGPD, arts. 26-27), DISPONIBILIZA INFORMAÇÕES acerca do uso compartilhado de dados e sua finalidade (art. 9º, inciso V) e MANTÉM REGISTRO DETALHADO dos eventos relacionados a cada compartilhamento, incluindo a identificação de quais dados foram compartilhados, com quem foram compartilhados e quando foram compartilhados

Das opções disponíveis na questão 8.1, a organização **PETROBRAS** assinalou "**A3**".

O gráfico da Figura 11 possibilita comparar visualmente os valores do subindicador relativo à dimensão "Compartilhamento de Dados Pessoais" (iComp) que foram calculados para o(a) **PETROBRAS** com os valores médios calculados para as organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

Figura 11 - Dimensão "Compartilhamento de Dados Pessoais" (iComp) - Valor do(a) **PETROBRAS** e valores médios



A Tabela 7 apresenta os diferentes itens avaliados na questão 8.1.2, possibilitando comparar o valor da própria organização com os valores médios das organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

Tabela 7 - Dimensão "Compartilhamento de Dados Pessoais" (Questão 8.1.2) - Respostas do(a) **PETROBRAS** e valores médios

Questão 8.1.2 (TIPO B): Acerca de tratamento de dados pessoais em solução de computação em nuvem (*cloud computing*), a organização:	**PETROBRAS implementou esta medida?**	**Percentual de Outra que implementou esta medida**	**Percentual das 387 organizações que implementou esta medida**
realiza o tratamento de dados pessoais em nuvem (ainda que apenas armazenamento)	Sim	50,67%	57,88%
avaliou e pode assegurar que não há armazenamento de dados pessoais em território estrangeiro	Não	32,00%	21,45%
realizou avaliação de riscos relativamente a esse tratamento, amparada em análise e em relatório de impacto que foram devidamente submetidos à apreciação das instâncias competentes	Sim	9,33%	9,30%
incluiu, nos instrumentos contratuais com os provedores de nuvem, cláusulas e mecanismos que instituem precauções quanto à proteção dos dados	Sim	44,00%	47,55%

não realiza nenhum tratamento de dados pessoais em nuvem	Não	38,67%	27,91%

2.8 Violação de Dados Pessoais (subindicador iResp)

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

A questão desta dimensão, do "Tipo B" (múltiplas respostas), aborda aspectos relacionados à identificação, ao registro e ao tratamento/resposta a incidentes de segurança da informação que envolvem a violação de dados pessoais, bem como à existência de mecanismos e procedimentos padronizados para notificação da ANPD e dos titulares de dados envolvidos nos casos de incidentes.

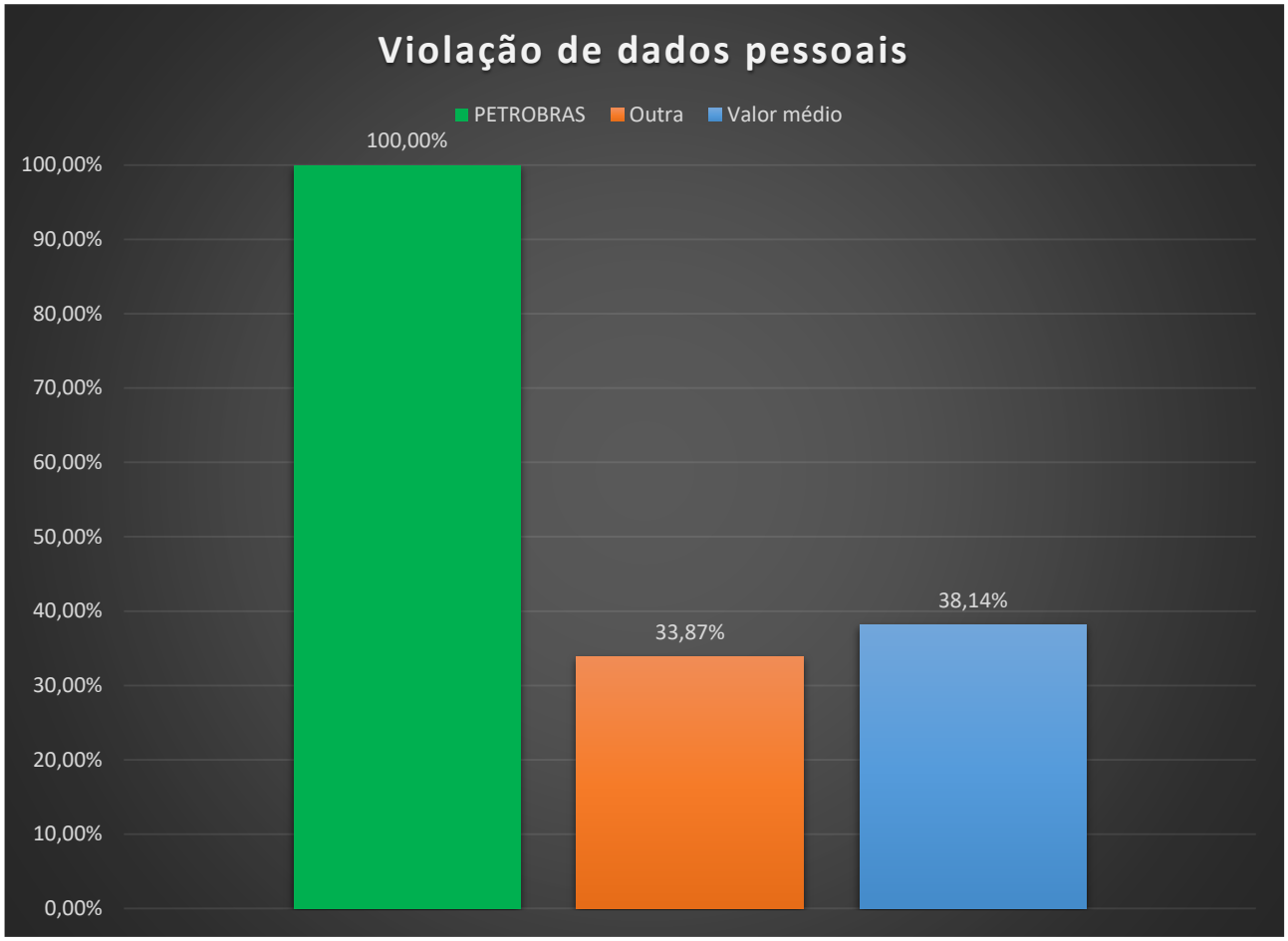
A Tabela 8 apresenta os diferentes itens avaliados na questão desta dimensão, os quais compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização com os valores médios das organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

Tabela 8 - Dimensão "Violação de Dados Pessoais" (iResp) - Respostas e valor do(a) **PETROBRAS** e valores médios

Questão 9.1 (TIPO B): A organização:	**PETROBRAS implementou esta medida?**	**Percentual de Outra que implementou esta medida**	**Percentual das 387 organizações que implementou esta medida**
elaborou e mantém atualizado plano de resposta a incidentes	Sim	30,67%	32,82%
registra todos os incidentes de segurança da informação que envolvem violação de dados pessoais em sistema próprio/adequado	Sim	38,67%	42,12%
sempre registra no sistema próprio/adequado a esse propósito todas as ações que foram adotadas para tratar/responder ao incidente	Sim	33,33%	34,11%
monitora proativa e continuamente a ocorrência de eventos que podem ser associados a incidentes de segurança da informação	Sim	34,67%	46,25%
estabeleceu e executa procedimentos padronizados para comunicar à ANPD e ao titular de dados a ocorrência de incidente de segurança da informação	Sim	32,00%	35,40%
ainda não atende nenhum dos itens anteriores	Não	38,67%	32,82%
Subindicador iResp	**100,00%**	**33,87%**	**38,14%**

O gráfico da Figura 12 possibilita comparar visualmente os valores do subindicador relativo à dimensão "Violação de Dados Pessoais" (iResp) que foram calculados para o(a) **PETROBRAS** com os valores médios calculados para as organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

Figura 12 - Dimensão "Violação de Dados Pessoais" (iResp) - Valor do(a) **PETROBRAS** e valores médios



2.9 Medidas de Proteção (subindicador iProt)

A organização deve adotar medidas de segurança, técnicas e administrativas com vistas a proteger os dados pessoais que trata de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Para isso, convém que a organização defina claramente papéis, responsabilidades e procedimentos voltados à proteção desses dados e implemente controles capazes de mitigar riscos que possam resultar em violações da privacidade.

A questão desta dimensão, do "Tipo B" (múltiplas respostas), aborda aspectos relacionados à implementação de controles adequados para proteger os dados pessoais e mitigar o risco de violação, a exemplo da restrição e do rastreamento das atividades e dos acessos aos sistemas que realizam o tratamento desses dados, da utilização de criptografia, do uso de técnicas e ferramentas de mascaramento/tarjamento de dados pessoais e da concepção de processos e sistemas que estejam conformes com a LGPD.

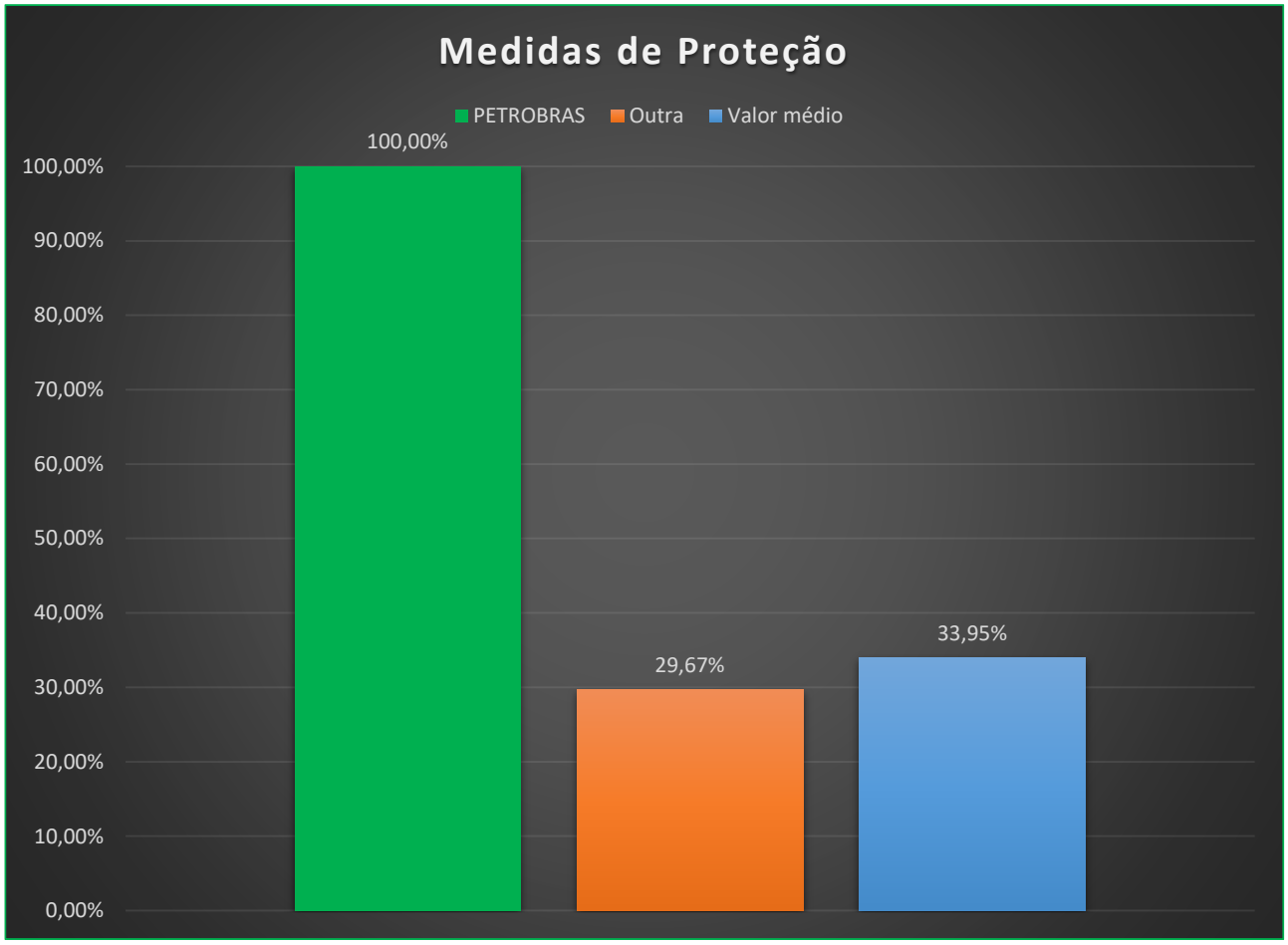
A Tabela 9 apresenta os diferentes itens avaliados na questão desta dimensão, os quais compõem o indicador de adequação à LGPD, possibilitando comparar os valores da própria organização com os valores médios das organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

Tabela 9 - Dimensão "Medidas de Proteção" (iProt) - Respostas e valor do(a) **PETROBRAS** e valores médios

Questão 10.1 (TIPO B): A organização:	**PETROBRAS implementou esta medida?**	**Percentual de Outra que implementou esta medida**	**Percentual das 387 organizações que implementou esta medida**
é capaz de comprovar que adota amplas medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais que trata	Sim	29,33%	34,11%
implementou processo formal para registro, cancelamento e provisionamento de usuários nos sistemas que realizam tratamento de dados pessoais	Sim	38,67%	41,34%
registra e monitora eventos (logs) relacionados às atividades de tratamento de dados pessoais	Sim	28,00%	37,98%
utiliza criptografia para proteger os dados pessoais quando estes estão em repouso, ou seja, a chamada criptografia de armazenamento	Sim	24,00%	25,84%
utiliza criptografia para proteger os dados pessoais quando estes estão em trânsito na rede interna da organização ou na Internet	Sim	37,33%	48,58%
possui norma(s) interna(s) que orientam os colaboradores quanto à obrigatoriedade do uso de mascaramento/ocultação/tarjamento	Sim	17,33%	20,93%
disponibiliza aos colaboradores ferramenta/solução tecnológica para realização do mascaramento/ocultação/tarjamento	Sim	36,00%	32,30%
adota medidas para assegurar que seus processos e sistemas sejam projetados, desde a concepção, em conformidade com a LGPD (*Privacy by design* e *Privacy by default*)	Sim	26,67%	30,49%
ainda não atende nenhum dos itens anteriores	Não	29,33%	19,90%
Subindicador iProt	**100,00%**	**29,67%**	**33,95%**

O gráfico da Figura 13 possibilita comparar visualmente os valores do subindicador relativo à dimensão "Medidas de Proteção" (iProt) que foram calculados para o(a) **PETROBRAS** com os valores médios calculados para as organizações pertencentes à área temática **Outra** e com os valores médios do conjunto das 387 organizações avaliadas.

Figura 13 - Dimensão "Medidas de Proteção" (iProt) - Valor do(a) **PETROBRAS** e valores médios



3 Perspectiva para o futuro

Ao longo dos próximos anos, a organização pode esperar que esta Corte de Contas continue realizando fiscalizações acerca da Lei Geral de Proteção de Dados Pessoais (LGPD), seja sobre o conjunto das organizações públicas federais ou mesmo sobre grupos específicos de órgãos/entidades, a exemplo das organizações pertencentes à área temática **Outra**.

A organização também deve aguardar, como consequência desta auditoria, a edição e a publicação, por parte dos chamados Órgãos Governantes Superiores (OGSs), de normativos e guias com vistas a induzirem a continuidade dos processos de adequação das suas organizações jurisdicionadas à LGPD, sobretudo quanto ao endereçamento das principais carências apontadas.

Por fim, frise-se que a grande maioria dos itens de verificação avaliados por meio do questionário aplicado nesta auditoria, entre diversos outros que visam a materializar o espírito da LGPD, não são opcionais, mas, sim, de cumprimento obrigatório: "As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios" (Lei 13.709/2018, art. 1º, parágrafo único).

Ou seja, a própria organização, por meio da atuação da respectiva unidade de controle/auditoria interno/a e mesmo como consequência do trabalho dos gestores e dos colaboradores envolvidos com as áreas afetas ao tema, deve ser a primeira interessada em continuar a sua jornada de adequação e de implementação dos dispositivos da LGPD.

Com esse propósito em mente, adiciona-se a seguir, inclusive, ferramentas que permitem avaliar qualitativamente Políticas de Proteção de Dados Pessoais (Anexo I) e Políticas de Privacidade

(Anexo II).

Anexo I – *Checklist* para verificação de Política de Proteção de Dados Pessoais

As normas ABNT NBR ISO/IEC 27001:2013, 27002:2013 e 27701:2019 fornecem diretrizes para gestão de segurança da informação e sua relação com a proteção de dados pessoais, levando em consideração os ambientes de risco das organizações. Essas normas foram projetadas para serem usadas como referência na seleção e na implementação de controles de segurança da informação e proteção de dados pessoais comumente aceitos.

De acordo com o item 5.1 da ABNT NBR ISO/IEC 27701:2019 c/c o item 5.2 da ABNT NBR ISO/IEC 27001:2013 e o item 5.1 da ABNT NBR ISO/IEC 27002:2013, a alta direção deve estabelecer um conjunto de políticas de segurança da informação, entre as quais sugere-se uma política de proteção de dados pessoais. Este *checklist* para verificação de POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS foi definido conforme as diretrizes para implementação relacionadas nos referidos itens.

#	Verificar se	S/N	Observações/ evidências
1	Existe uma política de proteção de dados pessoais (ou instrumento normativo equivalente) formalmente estabelecida		
2	A política de PD foi publicada para as partes interessadas (públicos interno e externo)		
3	A política de PD é assinada pela alta direção, refletindo o comprometimento em satisfazer os requisitos legais aplicáveis relacionados com a proteção de dados pessoais		
4	A política de PD prevê a relação com outros normativos associados (*e.g.* Política de Segurança da Informação)		
5	A política de PD regulamenta os agentes de tratamento no âmbito da organização		
6	A política de PD define gestores e estruturas, atribuindo-lhes papeis e responsabilidades pela proteção de dados pessoais		
7	A política de PD abrange e é aplicável aos fornecedores da organização (que tratem dados pessoais)		
8	A política de PD regulamenta os principais aspectos para a proteção de dados pessoais na organização (tratando, no mínimo, das hipóteses de tratamento de dados pessoais utilizadas, do exercício dos direitos dos titulares, das transferências e compartilhamentos de dados e da interação com a ANPD)		
9	A política de PD prevê a necessidade de comunicação/conscientização aos interessados		
10	A política de PD prevê a sua revisão periódica ou quando ocorrerem mudanças significativas		

Anexo II – *Checklist* para verificação de Política de Privacidade

A Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) estabeleceu diretrizes para a proteção de dados pessoais, levando em consideração os ambientes de risco das organizações. Essa norma definiu novas formas de interação com os titulares de dados, bem como obrigações adicionais de transparência sobre o tratamento de dados pessoais.

Este *checklist* para verificação de POLÍTICA DE PRIVACIDADE foi definido conforme as exigências previstas na LGPD.

#	Verificar se	S/N	Observações/ evidências
1	Existe uma política de privacidade (ou instrumento equivalente) estabelecida		
2	A política de privacidade foi publicada para as partes interessadas (públicos interno e externo)		
3	A política de privacidade informa o titular de dados sobre os princípios aplicáveis ao tratamento de dados pessoais		
4	A política de privacidade fornece informações sobre o controlador, o operador e o encarregado		
5	A política de privacidade informa como se dá a custódia de dados pessoais		
6	A política de privacidade informa sobre como o titular de dados pode obter as informações previstas no art. 18 da LGPD, quando aplicáveis		
7	A política de privacidade informa sobre como o titular de dados pode exercer seus direitos		
8	A política de privacidade informa quais são as hipóteses em que, no exercício de suas competências, a organização realiza o tratamento de dados pessoais		
9	A política de privacidade fornece informações claras sobre a previsão legal, a finalidade, as informações de contato do controlador, os procedimentos e as práticas utilizadas no tratamento de dados		
10	A política de privacidade fornece informações acerca do uso compartilhado de dados pelo controlador e sua finalidade		
11	A política de privacidade informa a data de sua última atualização		