LCG
IMPROVE + TRANSFORM

IAPMEI
Parcerias para o Crescimento

| Regulamento Geral de Proteção de Dados em Portugal

| Relatório do Inquérito de Avaliação da Maturidade das PME's face ao RGPD - 2018

| IAPMEI

O IAPMEI tem inscrita na sua missão a promoção da competitividade e do crescimento empresarial. Numa lógica de proximidade, procuramos ajudar as empresas, designadamente as PME, a antecipar e a ajustar o seu desempenho àquelas que são as alterações que impactam diretamente na sua atividade.

A aplicação do RGPD, que entra em vigor em maio de 2018, com um quadro legal que coloca nas organizações públicas e privadas o ónus da responsabilidade da proteção de dados, acrescenta inevitavelmente obrigações que têm um impacto considerável nas suas operações.

O IAPMEI está por isso empenhado em contribuir para que as empresas sejam capazes de construir um plano eficaz de adaptação a esta nova realidade e, assim, evitar perturbações e penalizações na gestão dos seus negócios e nas relações com os diversos *stakeholders*.

| LCG Consultoria

A LCG, através da sua unidade de Digital Lead & Protection (DLP) reúne um conjunto de competências que permite assessorar as organizações na avaliação de conformidade e implementação do novo regulamento.

No âmbito da sua atividade, foi das primeiras entidades a desenvolver ações relacionadas com o Novo Regulamento de Proteção de Dados e tem sido das principais impulsionadoras do estudo dos vários impactos deste novo regulamento, tanto a nível de formações e conferências de sensibilização pragmática e efetiva, bem como no desenvolvimento deste estudo, em parceria com o IAPMEI.

| Índice

| O Regulamento Geral de Proteção de Dados (I/II)

| Contexto

| Em Abril de 2016, o Parlamento Europeu e o Conselho da Europa aprovam o texto do novo Regulamento Geral de Proteção de Dados (RGPD), com aplicação em Maio de 2018, após um período de transição.

O RGPD substitui a Diretiva Geral de Proteção de Dados, de 1995, tem aplicação direta em cada um dos estados membros da União Europeia e substancia as responsabilidades das empresas, reforça os direitos individuais de proteção de dados, facilita a livre circulação de dados pessoais no mercado único digital e reduz a carga administrativa associada.

| Impacto

| O Regulamento, elaborado com o intuito de defender os direitos dos titulares de dados, coloca mais responsabilidade nas empresas, com a exigência de proatividade.

A alteração na legislação tem impacto organizacional ao nível da gestão de recursos humanos, administração de sistemas, gestão de reputação, organização de informação e adequação jurídica de cláusulas contratuais.

| Penalizações severas

| O RGPD traz também novas e mais severas penalizações para casos de incumprimento:

- Violação dos direitos dos titulares: Até 20M € ou 4% do volume de negócios anual;
- Violação das obrigações dos responsáveis: Até 10M € ou 2% do volume de negócios anual;
- Ações Judiciais Coletivas: Com possibilidade de delegação em terceiros e possibilidade de indeminização por danos morais e não apenas materiais;

LCG IMPROVE + TRANSFORM

IAPMEI Parcerias para o Crescimento

| O Regulamento Geral de Proteção de Dados (II/II)

| O Inquérito

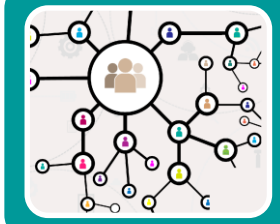
| No âmbito de um protocolo assinado entre a LCG Consultoria e o IAPMEI, foi elaborado um inquérito para promover a sensibilização das empresas sobre o novo Regulamento Geral de Proteção de Dados (RGPD).

Este inquérito, teve como objetivo a recolha de dados que permitissem caraterizar a situação atual das empresas portuguesas e dos seus profissionais, quanto ao seu nível de conhecimento e de preparação para a proteção e privacidade de dados pessoais e, em particular, corresponder às exigências do novo RGPD.

Inteiramente Digital

Realizado entre Março e Abril de 2018

Responderam cerca de 1.375 profissionais



Distribuído pelo IAPMEI

Para cerca de 20.000 empresas

Respostas corresponderam a mais de 1.000 empresas

Maioria de Micro e Pequenas Empresas

17% das respostas de médias empresas

Apenas 2% de empresas com mais de 250 colaboradores

LCG IMPROVE + TRANSFORM

IAPMEI Parcerias para o Crescimento

| Principais Resultados

| Conhecimento e Domínio do Tema

O nível de conhecimento aumentou de forma significativa. Das empresas inquiridas, 27% dizem conhecer detalhadamente o RGPD contra apenas 4.2% em 2017.

| Nível de Preparação

Cerca de 49% das empresas inquiridas afirmam estar parcialmente preparadas e cerca de 35% considera que a sua empresa talvez sofresse uma penalização financeira. 8% das empresas considera ter todas as medidas adequadas para responder às exigências do regulamento.

| Planeamento para a conformidade

Das organizações inquiridas, 17% confirma ter já um plano integrado definido para garantir a conformidade com o RGPD enquanto que cerca de 3% das organizações considera aumentar o número de colaboradores dedicados a programas de proteção de dados.

Cerca de 39% das empresas reconhecem a necessidade de reforçar a informação e promover formação para os colaboradores sobre o RGPD e os seus impactos.

| Conhecimento e Domínio do Tema

A sua empresa tem conhecimento sobre o novo Regulamento Geral de Proteção de Dados aprovado pelo Parlamento Europeu em Maio de 2016?

Resultados

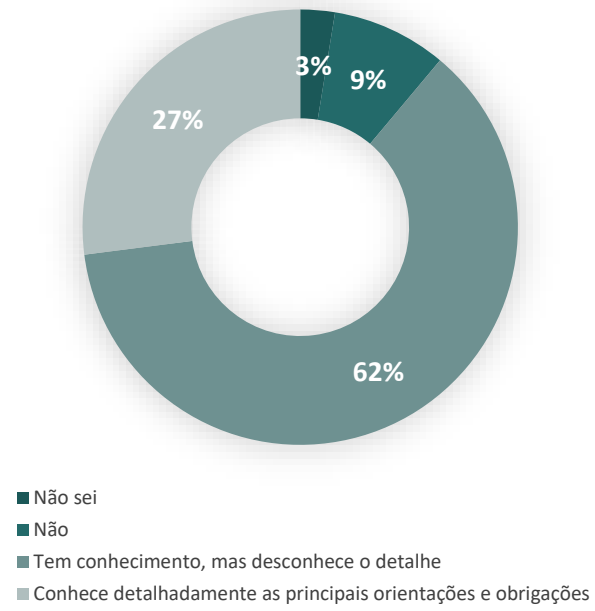
Aproximadamente 62% das empresas que participaram no estudo considera ter conhecimento sobre o novo Regulamento Geral de Proteção de Dados, mas desconhece o detalhe.

As atividades com maior conhecimento sobre o tema de RGPD são as atividades financeiras & seguros, atividades de saúde humana & apoio social e comércio por grosso e retalho.

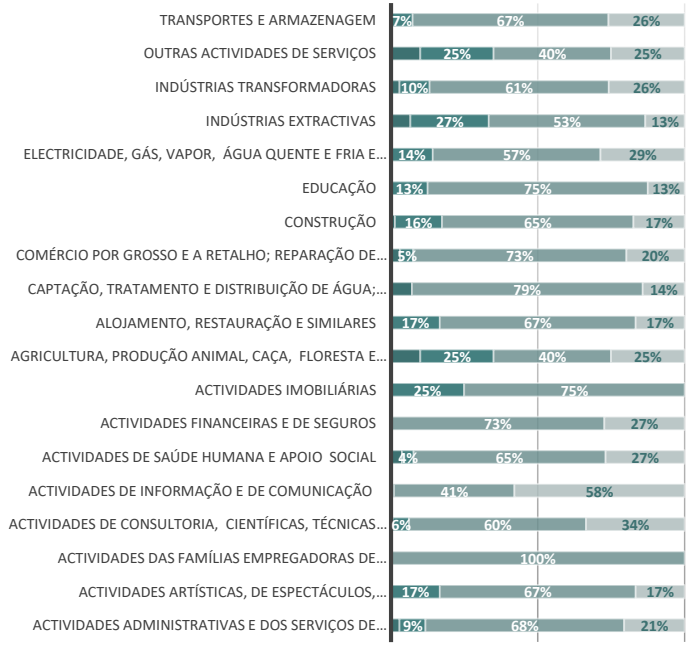
Perspetiva LCG

Ainda se observa alguma confusão nos conceitos basilares do RGPD, fruto da disseminação de mensagens de teor contraditório, emitidas por diversas entidades que procuram lucrar com a aplicação do regulamento.

Grau de Conhecimento



Grau de Conhecimento por Atividade



| Conhecimento e Domínio do Tema

O programa de proteção de dados é uma prioridade na gestão de informação da sua empresa?

Resultados

Cerca de metade das empresas inquiridas considera que o programa de proteção de dados é uma prioridade na gestão de informação.

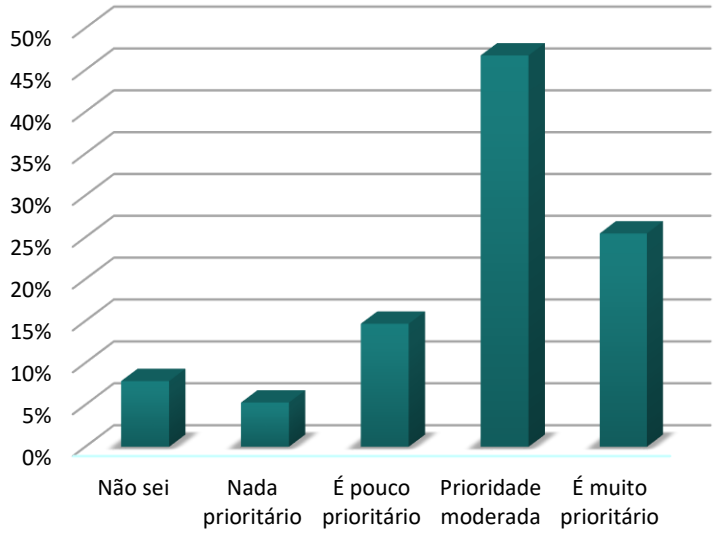
Verifica-se que as médias e grandes empresas tendem a considerar o programa de proteção de dados na gestão de informação como prioritário, sendo que as pequenas empresas tendem a atribuir-lhe uma menor prioridade.

Perspetiva LCG

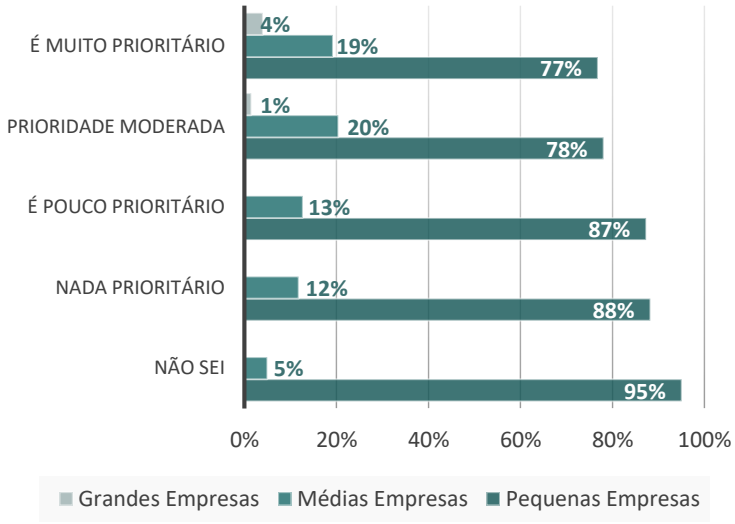
A necessidade de integrar a aplicação do RGPD com a necessária modernização e digitalização dos processos organizacionais, é de mais fácil reconhecimento por parte das organizações de maior complexidade.

Seja pela necessária adequação aos públicos-alvo, pelo relacionamento competitivo de sector, seja pela existência de recursos humanos com diferentes perspetivas e valências, contribuindo para a inovação e consciência internas.

Prioridade na Gestão da Informação



Prioridade de Gestão de Informação por Dimensão da Empresa



| Conhecimento e Domínio do Tema

Qual o estágio de maturidade em termos de compreensão da natureza e do impacto do Regulamento?

Resultados

Cerca de 53% das organizações consideram ter pouca maturidade em termos de compreensão da natureza e do impacto do Regulamento.

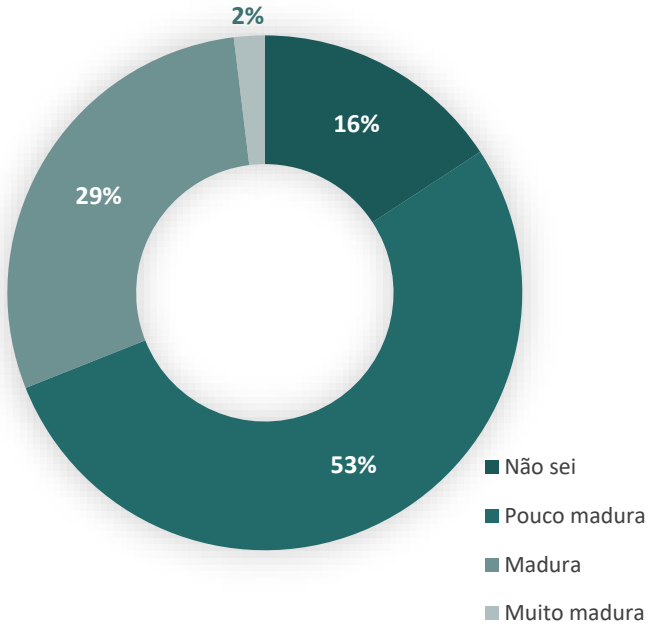
Por outro lado, 2% das organizações inquiridas consideram ter um nível de maturidade elevada em relação a este tema.

A grande maioria dos respondentes reconhece ter pouca maturidade sobre o RGPD, o que implica uma maior necessidade de preparação do tecido empresarial para estas questões.

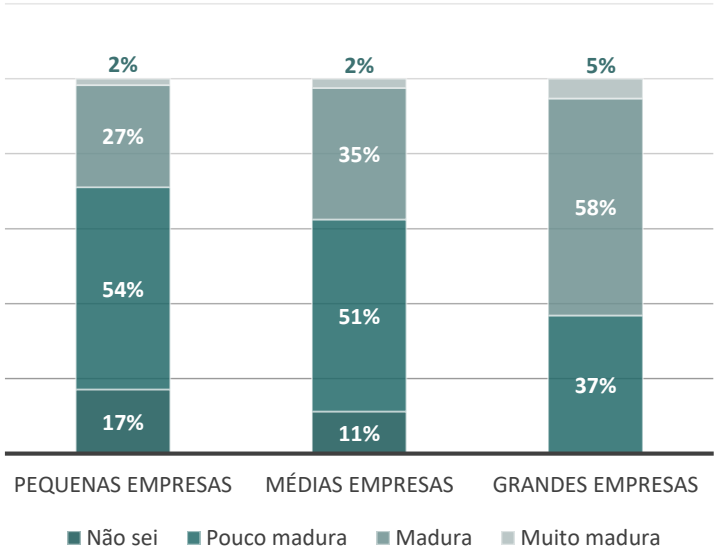
Perspetiva LCG

A ausência de clareza quanto à autoridade de controlo e as suas funções, aliada à existência de múltiplas mensagens de teor contraditório que têm sido apresentadas, contribui para que as organizações não se sintam conhecedoras da natureza e contexto do regulamento.

Estágio de maturidade



Estágio de maturidade por dimensão da empresa



| Conhecimento e Domínio do Tema

Conhece as penalidades no caso de incumprimento do RGPD?

Resultados

Das empresas inquiridas, 33% dizem saber que existem penalidades no caso de incumprimento do RGPD mas desconhecem os detalhes das mesmas.

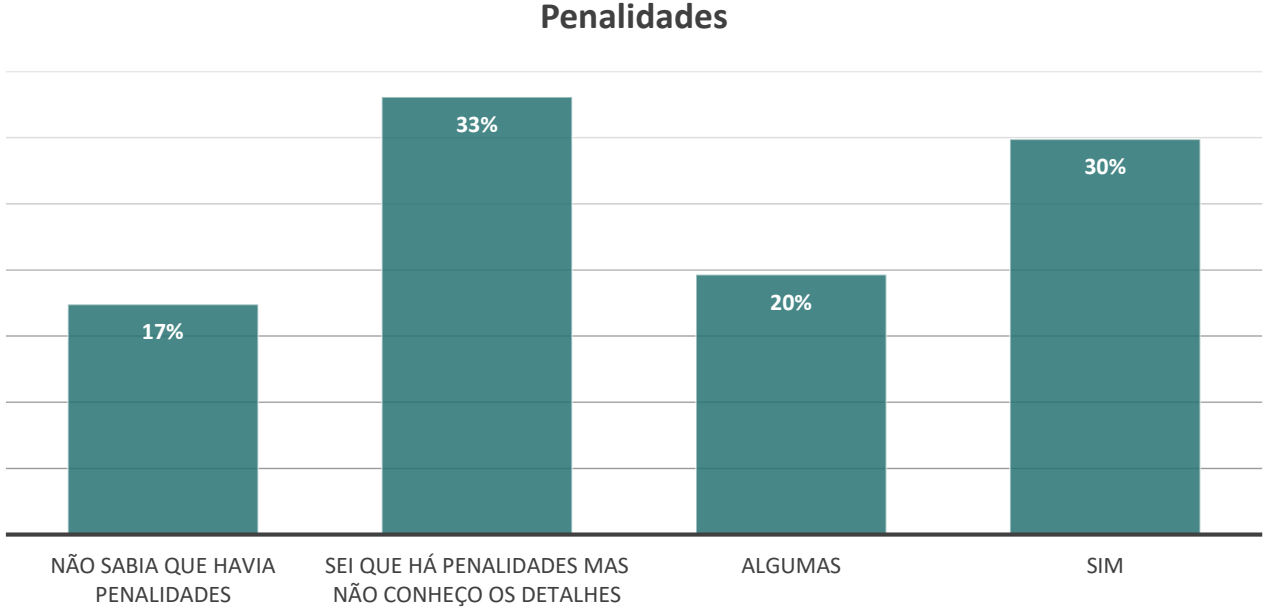
Existe uma expectativa transversal quanto à forma como o legislador nacional irá contextualizar e tipificar as mesmas.

Apesar disso, 17% das empresas desconhecem a existência de penalidades associadas ao incumprimento do RGPD.

Perspetiva LCG

Embora a proposta de lei seja já do conhecimento público, ainda existe uma desconhecimento significativo quanto à mesma no que toca aos valores mínimos aplicáveis, sujeitos à aprovação em Assembleia.

O ênfase dado às coimas máximas, sem referência a eventuais admoestações ou proibições de tratamento de dados, colocaram a aplicação do RGPD longe da realidade.



| Nível de Preparação Atual

Considera que os procedimentos atuais da sua empresa satisfazem os requisitos do RGPD?

Resultados

Na generalidade, a maior parte das empresas inquiridas considera que os procedimentos atuais satisfazem parcialmente os requisitos do RGPD.

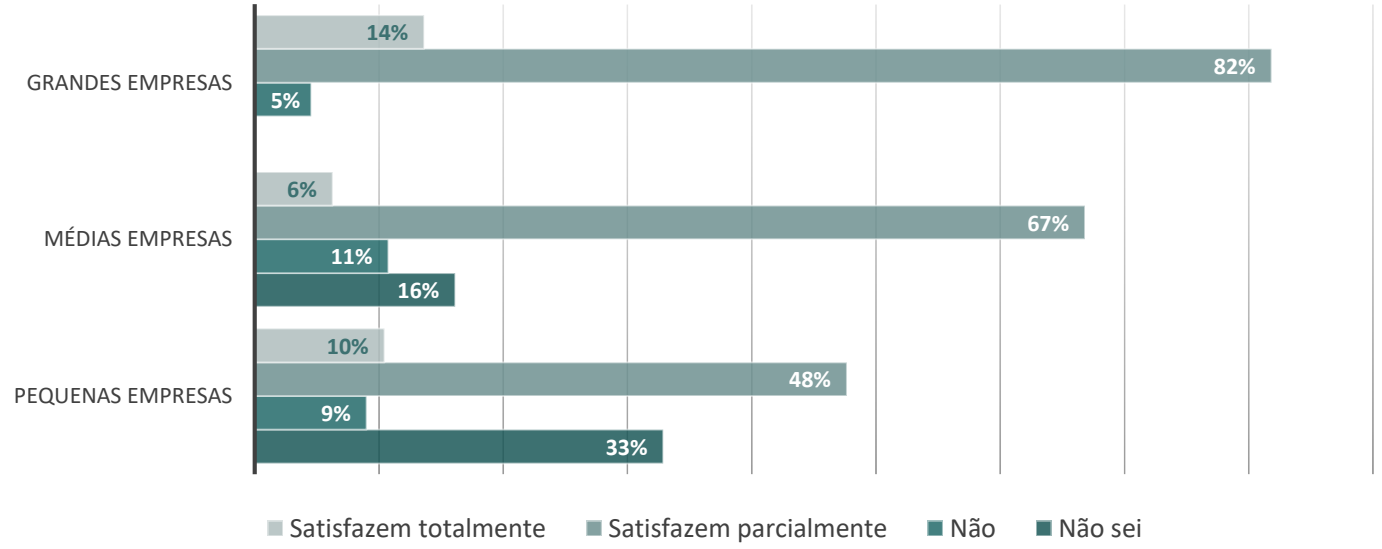
Por sua vez, nas pequenas empresas, 33% dizem não saber se os procedimentos satisfazem os requisitos RGPD, sendo que esse desconhecimento tende a diminuir com o aumento da dimensão das organizações.

Perspetiva LCG

Os procedimentos atuais, quando baseados em normas e certificações, garantem já parte da componente de conformidade exigida pelo RGPD. Compete às organizações efetuar a revisão e adequação das mesmas.

Apenas quando a organização tiver efetuado o diagnóstico de conformidade com o RGPD, poderá categoricamente avaliar a adequação dos procedimentos existentes.

Procedimentos atuais satisfazem os requisitos do RGPD?



| Nível de Preparação Atual

Considera que a sua empresa se encontra tecnologicamente preparada para o RGPD?

Resultados

Na generalidade, a maior parte das empresas inquiridas considera que a tecnologia que existe atualmente nas suas organizações satisfaz parcialmente os requisitos do RGPD.

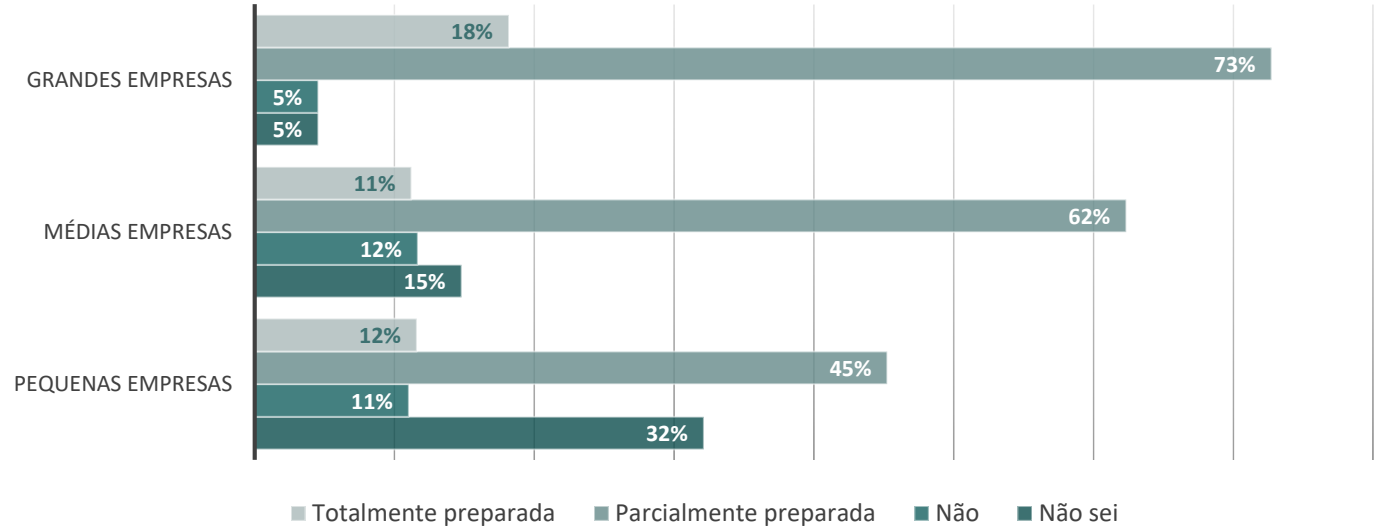
Por sua vez, nas pequenas empresas, 32% dizem não saber se a sua tecnologia satisfaz os requisitos RGPD, sendo que esse desconhecimento tende a diminuir com o aumento da dimensão das organizações.

Perspetiva LCG

O RGPD não elenca as medidas técnicas adequadas à conformidade pelo que é responsabilidade das organizações analisarem e decidirem qual o nível de adequação e as alternativas e soluções necessárias.

Este cuidado deve ser considerado nas ferramentas que sejam proprietárias como de quaisquer soluções disponíveis via prestadores de serviços.

Preparação Tecnológica RGPD



| Nível de Preparação Atual

Considera que a sua organização está bem preparada em termos de segurança de informação?

Resultados

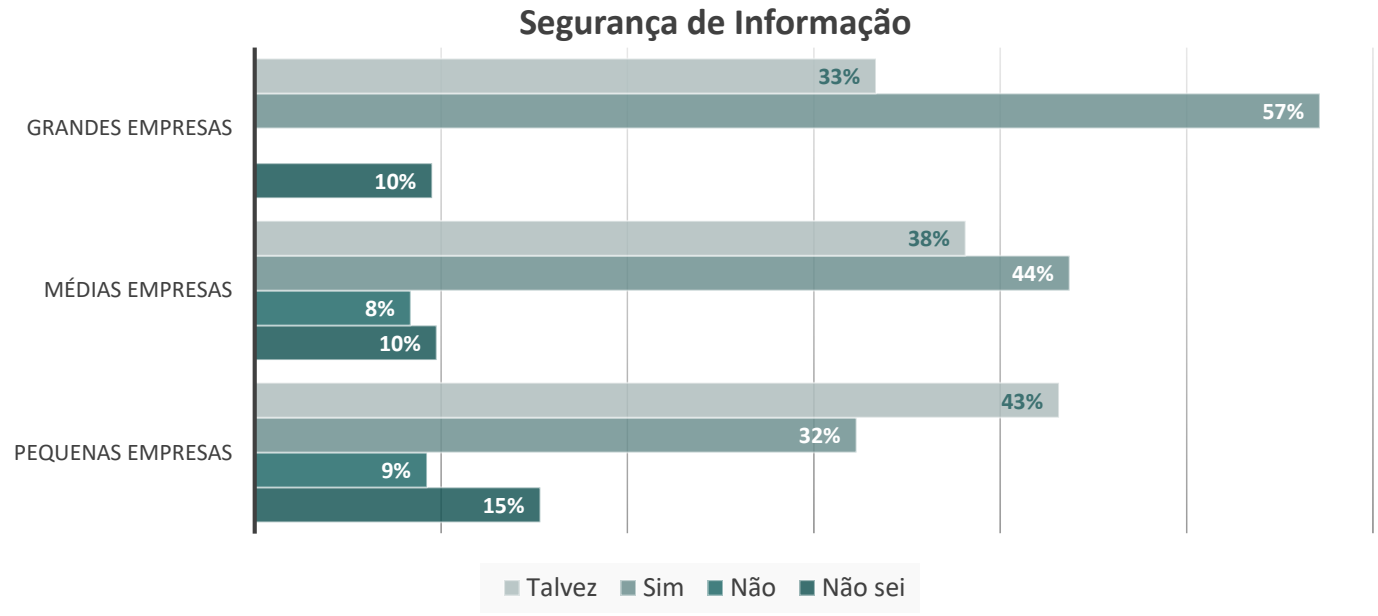
Das empresas de grande dimensão, 57% consideram estar bem preparadas em termos de segurança de informação, embora se observe uma diminuição à medida que a dimensão da empresa se reduz.

De forma transversal, cerca de 10% das organizações não sabem se estão bem preparadas em termos de segurança de informação.

Perspetiva LCG

A segurança de informação é uma área com bastante enfoque, quanto maior for a organização. No entanto, os requisitos de conformidade com o RGPD vêm confirmar a alteração que se observa neste campo, sendo que a Segurança de Informação já não é apenas competência dos recursos técnicos, mas sim de toda a organização.

A preparação e adequação, começa pela formação de todos os colaboradores.



| Nível de Preparação Atual

Considera que a sua organização sofreria uma penalização financeira se o RGPD fosse hoje aplicado?

Resultados

Cerca de 30% dos inquiridos não sabem se a sua organização sofreria uma penalização financeira com a aplicação do RGPD.

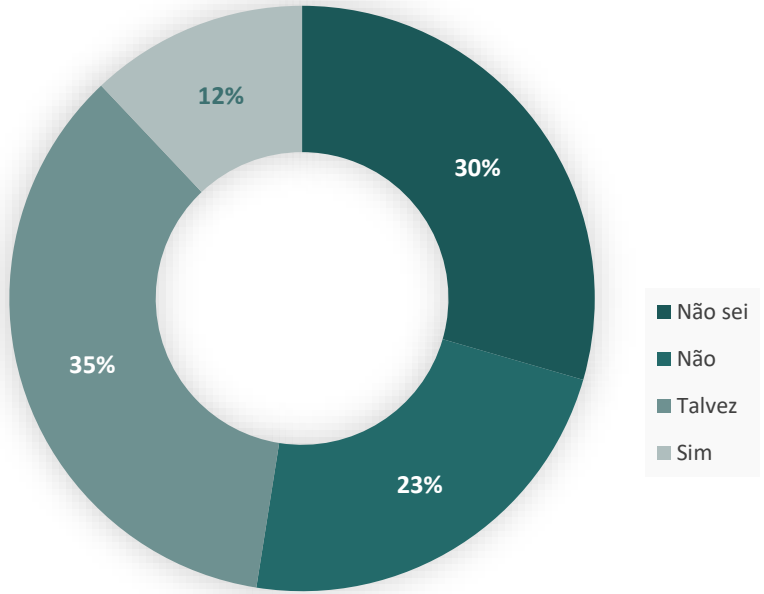
Denota-se claramente pouca confiança na capacidade de aplicação das penalizações, fruto da indefinição ainda existente nalguns aspetos referentes ao regulamento, à sua fiscalização e à autoridade de controlo que a irá tutelar.

Perspetiva LCG

Uma vez mais, a ausência de lei aprovada, em paralelo com a incerteza associada à autoridade de controlo, suas funções e metodologia de trabalho, contribui para a incerteza face à aplicação de penalizações financeiras.

De qualquer modo, não devem ser descuradas as penalizações de igual importância do que as financeiras: as organizacionais, as políticas e - de maior impacto - as reputacionais.

Penalização financeira se o RGPD fosse hoje aplicado?



| Nível de Preparação Atual

A sua organização tem políticas formais de proteção de dados pessoais?

Resultados

Cerca de 44% das organizações consideram ter políticas formais de proteção de dados para algumas áreas e departamentos.

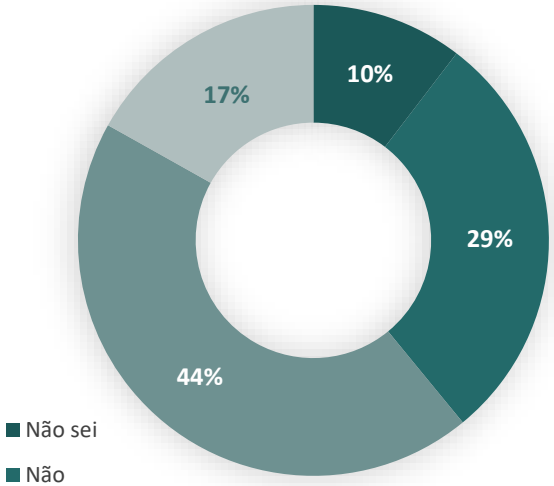
17% considera que as políticas existentes são extensivas e transversais a toda a organização, enquanto que 29% considera que não existem quaisquer políticas de proteção de dados aplicadas.

Perspetiva LCG

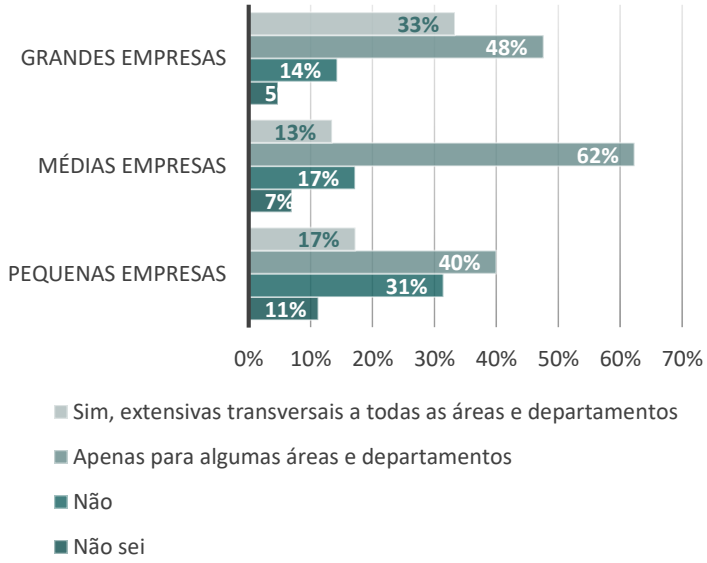
As organizações de maior dimensão, pela necessidade de corresponder a exigências de sector ou por questões de competitividade, têm já políticas que correspondem, total ou parcialmente, às exigências do RGPD.

Observa-se a necessidade de que estas políticas formais de proteção de dados pessoais, na generalidade das organizações, sejam integradas, com aplicação transversal nas diferentes unidades orgânicas.

Políticas de proteção de dados pessoais



Políticas de proteção de dados pessoais por dimensão das empresas



| Nível de Preparação Atual

Qual o nível de adequação das medidas adotadas pela sua organização para garantir a privacidade dos dados?

Resultados

A maioria dos respondentes (56%) considera que as suas medidas são razoavelmente adequadas e 8% afirma serem perfeitamente adequadas.

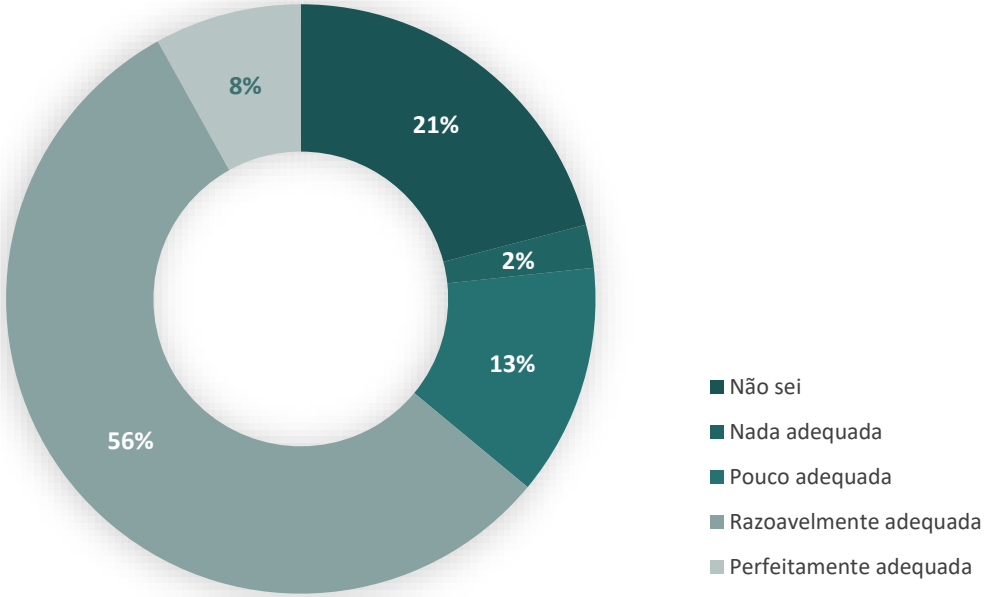
De realçar que 21% dos respondentes desconhece o nível de adequação das medidas adotadas.

Perspetiva LCG

Sendo um novo Regulamento, a maioria das organizações carece ainda de uma primeira aferição do nível de conformidade e adequação das políticas e processos atuais, para uma correta identificação das eventuais alterações.

Este facto pressupõe a necessidade de revisão das mesmas para garantir a sua adequação.

Adequação das medidas adotadas



| Nível de Preparação Atual

Considera que a sua organização está preparada para a gestão e governação do acesso aos dados?

Resultados

35% das empresas de grande dimensão consideram que estão perfeitamente preparadas para a gestão e governação do acesso físico e digital aos dados.

Relativamente às empresas de pequena dimensão, 29% não sabem responder à questão e 28% consideram não estar preparadas.

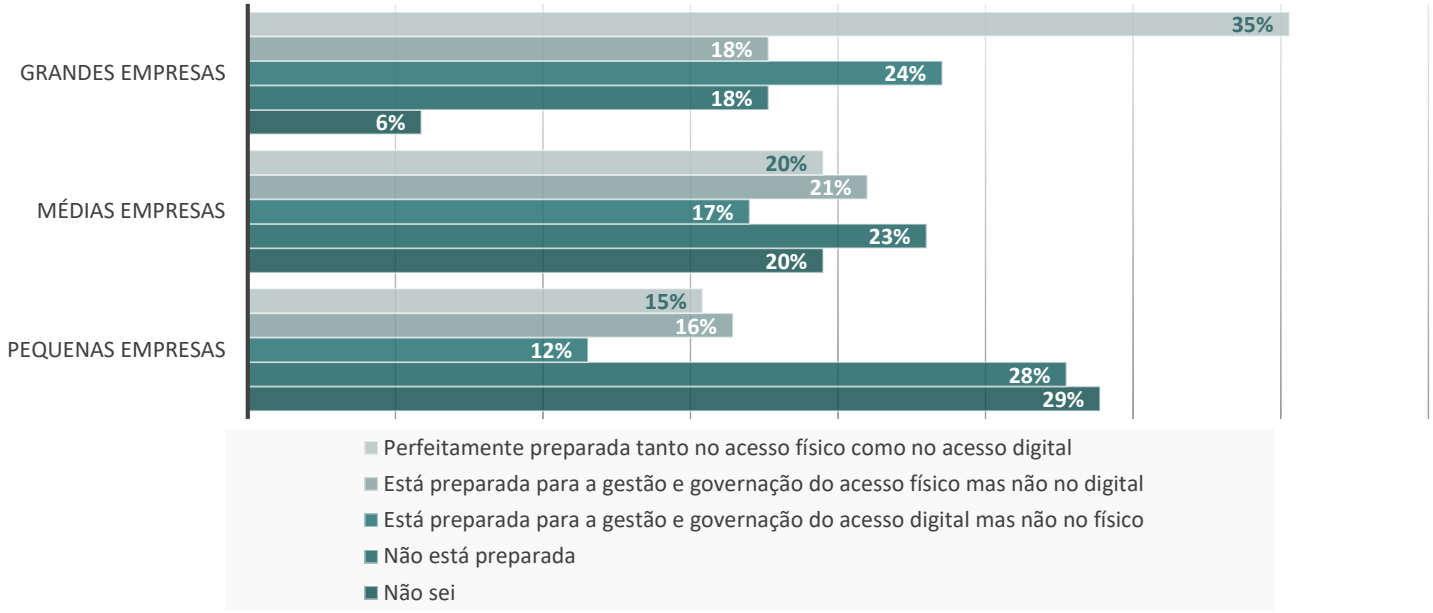
Quanto às empresas de média dimensão, observa-se uma distribuição equilibrada das respostas dadas.

Perspetiva LCG

A gestão e controlo no acesso aos dados, deve ser criteriosamente considerada, de modo a garantir uma matriz de atribuição de privilégios, salvaguardar a segregação de funções e a privacidade dos dados, assegurando os princípios da minimização e limitação de acesso.

A revisão dos acessos físicos e digitais, deve contemplar infraestruturas e recursos, atendendo à necessárias monitorização e registo de logs, permitindo a prevenção e controlo de fugas de informação.

Gestão e governação do acesso aos dados



| Nível de Preparação Atual

Considera serem necessárias correções nos processos existentes de proteção de dados?

Resultados

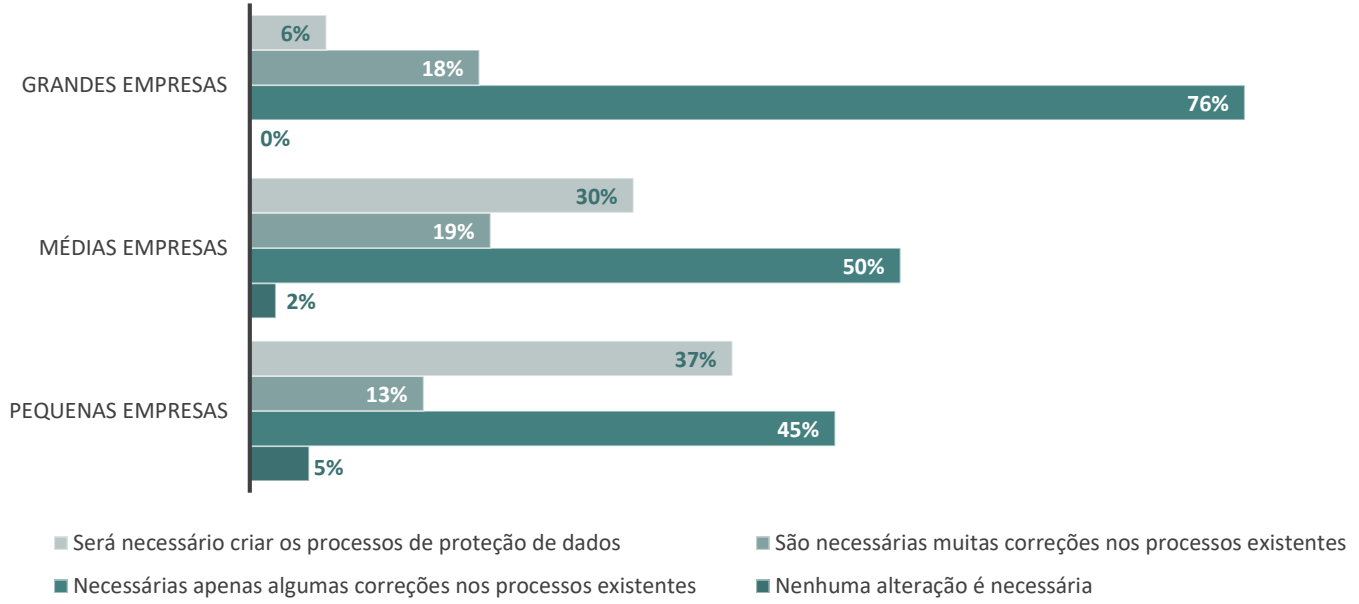
Cerca de metade das empresas de pequena e média dimensão consideram ser necessárias apenas algumas correções nos processos existentes.

De uma forma transversal, as empresas inquiridas acreditam que vão ter de fazer algum tipo de correção aos processos existentes.

Perspetiva LCG

A natureza do RGPD, face aos desafios de modernização e digitalização que as organizações e a sociedade enfrentam, obriga a uma revisão e adequação dos processos existentes. Seja para fazer face aos requisitos de conformidade, seja para aproveitar as alterações implementadas na dinâmica entre organização e utente.

Correções nos processos existentes



| Nível de Preparação Atual

Quais as áreas que considera necessitarem de maior intervenção (escolha múltipla)?

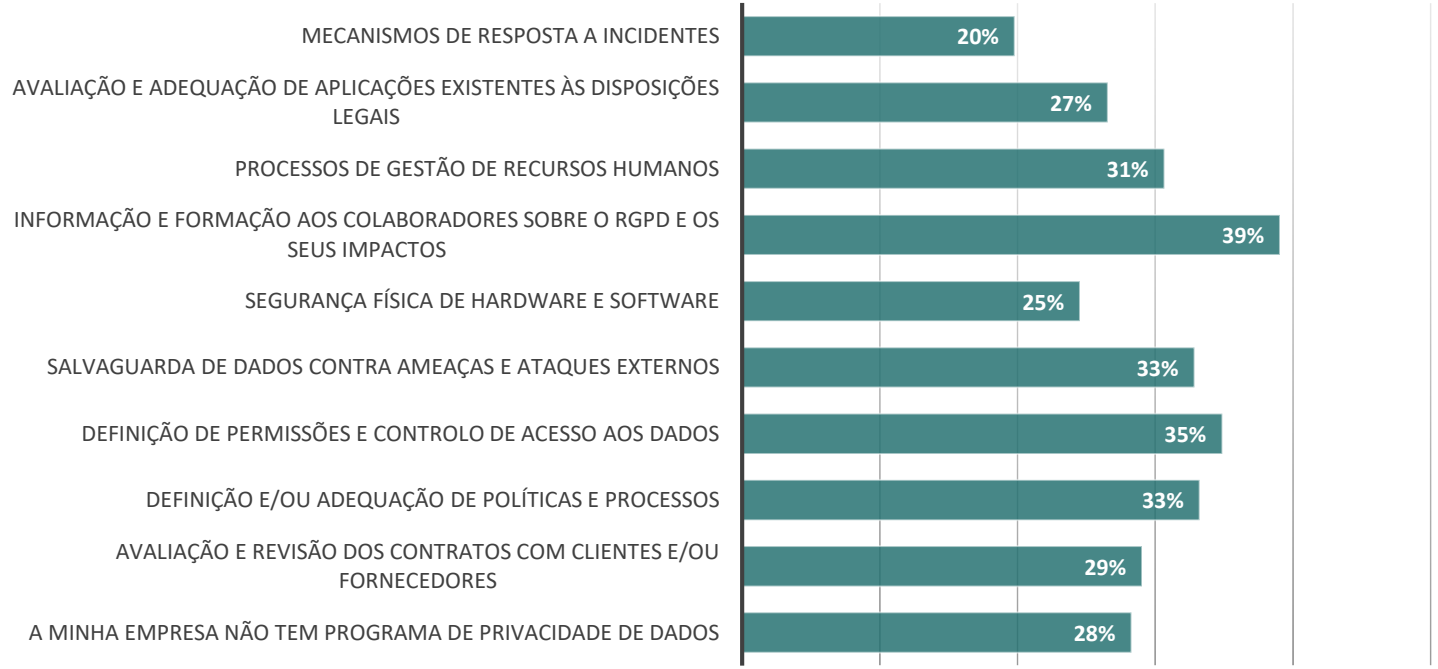
Resultados

Na opinião dos inquiridos, a informação e formação aos colaboradores sobre o RGPD e os seus impactos, é a área que consideram necessitar de maior intervenção, com 39% das respostas.

Outras áreas que se destacam são a definição de permissões e controlo de acesso aos dados, a salvaguarda de dados contra ameaças e ataques externos e a definição e/ ou adequação de políticas e processos.

Perspetiva LCG

Em paralelo a qualquer necessidade de adequação jurídica, processual ou tecnológica, as organizações têm necessariamente que apostar na Gestão da Mudança, promovendo a alteração comportamental dos seus recursos para melhor refletir a sua cultura, identidade e melhores práticas, mitigando ou anulando os riscos inerentes.



| Nível de Preparação Atual

Acredita que a sua organização vai estar totalmente preparada para o RGPD em Maio de 2018?

Resultados

Cerca de 25% das empresas inquiridas acreditam que vão estar preparadas para a entrada em vigor do RGPD.

Por sua vez 38% têm algumas dúvidas sobre se a sua organização vai estar devidamente preparada.

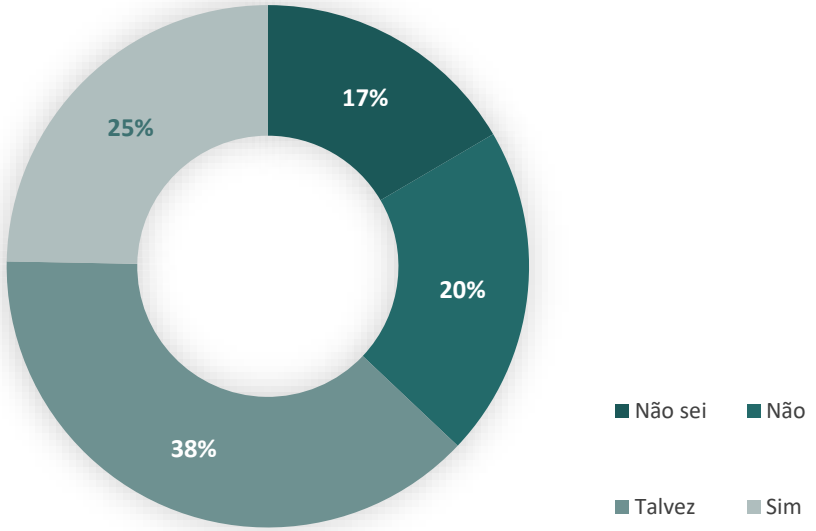
37% dos respondentes dizem não saber ou asseguram que não estarão totalmente preparadas para a aplicação do Regulamento.

Perspetiva LCG

A prioridade deve ser colocada na capacidade, processual e informacional, de responder às questões colocadas pelo RGPD, autoridade de controlo e titulares dos dados.

Cada organização tem o seu conjunto de interlocutores, as suas atividades de processamento e as finalidades respetivas para as quais recolhe e mantém dados pessoais. Como tal, é necessário que cada uma identifique o que significa estar preparada.

A sua organização vai estar totalmente preparada para o RGPD em Maio de 2018?



| Nível de Preparação Atual

Quais os motivos mais relevantes para o programa de privacidade de dados da sua organização (escolha múltipla)?

Resultados

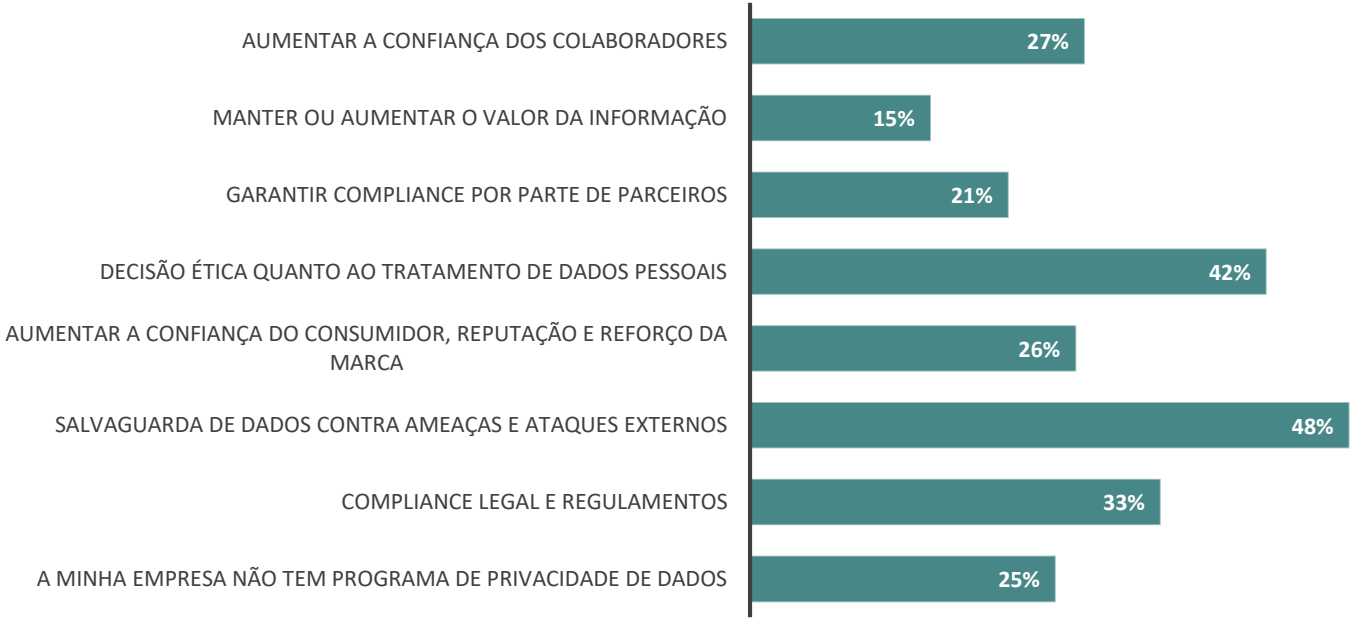
Na opinião dos inquiridos destacam-se três motivos relevantes para o programa de privacidade de dados na organização:

1. Salvaguarda de dados contra ameaças e ataques externos (48%);
2. Decisão ética quanto ao tratamento de dados pessoais (42%);
3. *Compliance* legal e regulamentos (33%).

Perspetiva LCG

Apesar de ser dado maior destaque aos ataques externos, é expectável que as organizações passem a reconhecer, cada vez mais, razões de teor organizacional.

Estas razões serão alicerçadas na necessidade de otimizar processos, promover uma cultura corporativa de segurança, aproveitar oportunidades para reforçar a relação com o utente e aumentar a confiança.



Considera serem necessárias correções nas políticas existentes de proteção de dados?

Resultados

Apenas 5% das pequenas empresas consideram que não é necessário fazer alterações às políticas de proteção de dados existentes.

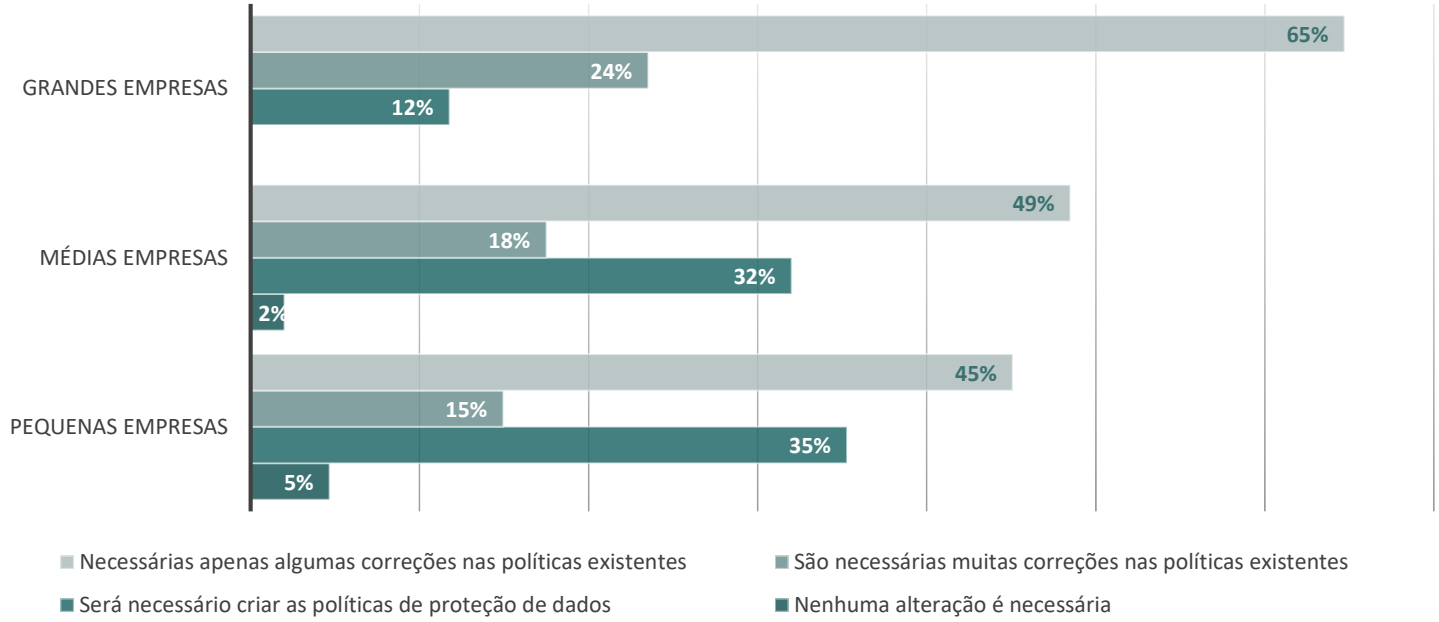
Em relação às médias empresas, 49% acreditam que serão necessárias apenas algumas correções nas políticas existentes, sendo que esta percentagem, nas grandes empresas, sobe para os 65%.

Perspetiva LCG

As organizações de maior dimensão, estando cientes da importância que o conjunto de políticas tem na materialização de processos e procedimentos, são claramente conscientes da necessidade de as rever e corrigir quando aplicável.

Por outro lado, as pequenas e médias empresas, denotam a necessidade de criar essas mesmas políticas.

Correções nas políticas existentes



| Planeamento para Conformidade

A sua organização planeia aumentar o orçamento dedicado ao programa de proteção de dados?

Resultados

De uma forma geral, existe um grande desconhecimento sobre se as organizações planeiam aumentar o orçamento dedicado ao programa de proteção de dados, sendo que 36% dos respondentes asseguram que o orçamento para este tema não vai aumentar.

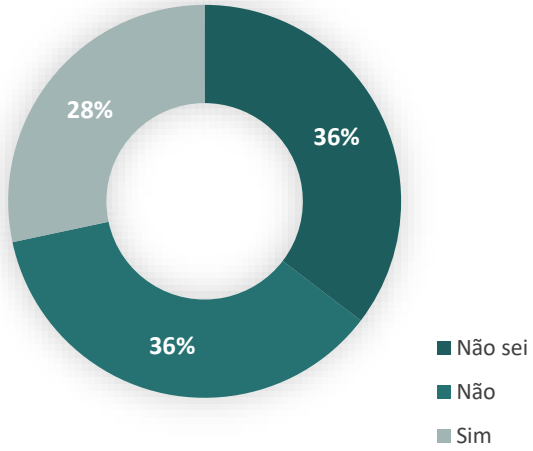
É nas empresas de maior dimensão que se regista um maior número de respostas que confirmam o aumento do orçamento dedicado ao programa de proteção de dados.

Perspetiva LCG

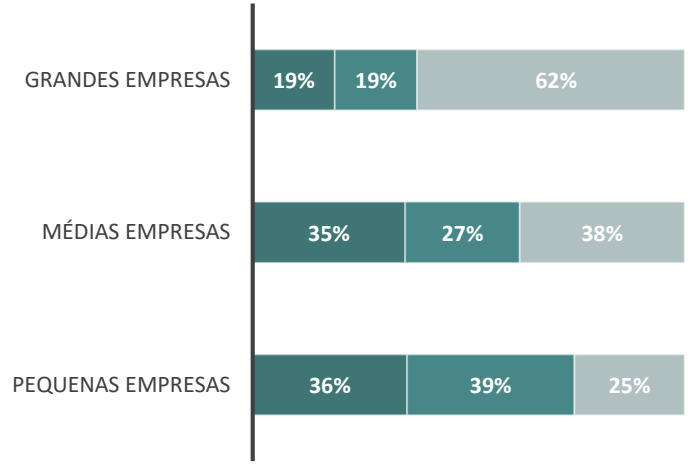
São as organizações de maior dimensão que, dada a sua dimensão e complexidade, mais facilmente reconhecem a necessidade de aumentar o orçamento dedicado.

De uma forma ou de outra, serão poucas as organizações que acabarão por não alocar orçamento adicional, direta ou indiretamente, suscitado pela aplicação do RGPD.

Aumentar o orçamento dedicado ao programa de proteção de dados?



Aumento do orçamento por dimensão da Empresa



| Planeamento para Conformidade

A sua organização tem um plano a decorrer para garantir conformidade com o RGPD em Maio 2018?

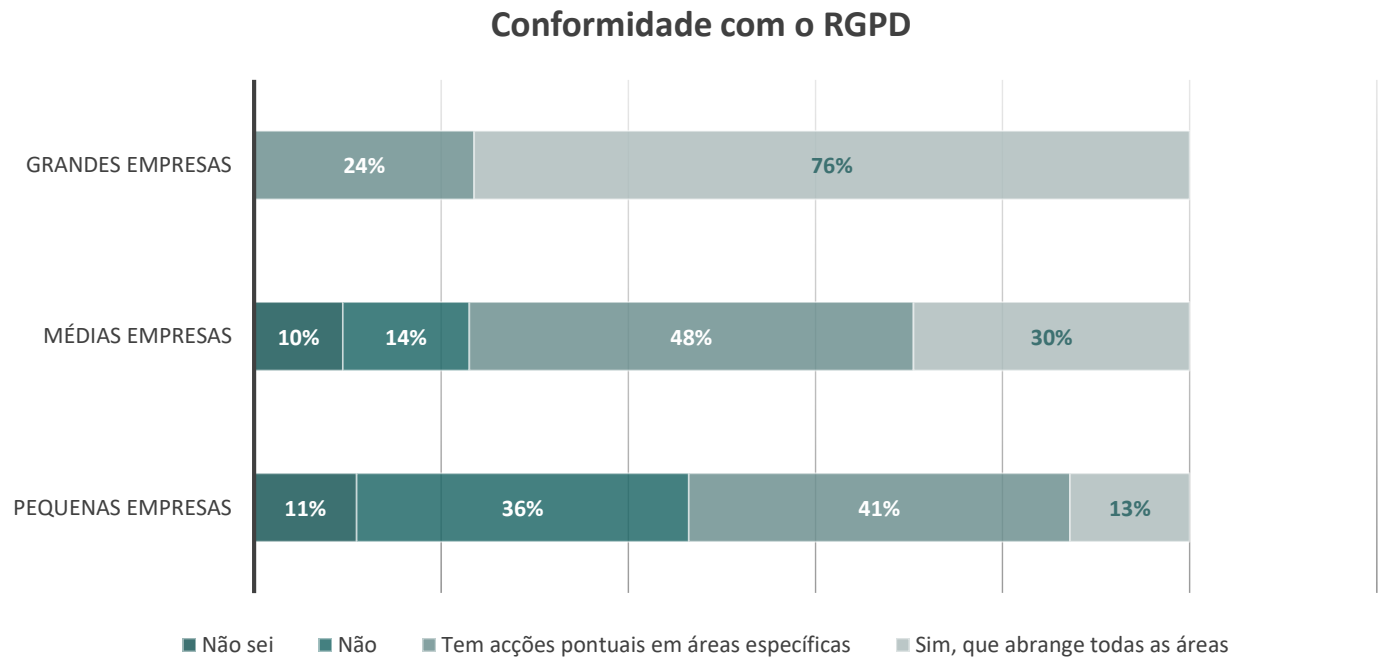
Resultados

Nas pequenas empresas, 41% dos inquiridos confirmam que a sua organização tem ações pontuais em áreas específicas, para garantir conformidade com o RGPD em Maio de 2018.

Nas médias empresas esta percentagem sobe para os 48%, sendo que nas grandes empresas 76% dos inquiridos consideram que o plano da sua organização abrange todas as áreas.

Perspetiva LCG

Apesar da forma mais ou menos integrada com que as organizações terão iniciado a sua aferição de conformidade para com o RGPD, estas irão acabar por criar planos integrados para gestão de conformidade e monitorização da aplicação em paralelo das várias iniciativas, de Âmbito jurídico, processual ou tecnológico.



| Planeamento para Conformidade

Considera que a sua organização irá alterar significativamente os procedimentos e tecnologias que envolvam a segurança de informação até maio de 2018?

Resultados

Existe uma percentagem significativa (21%) de respondentes, que consideram não haver lugar a grandes alterações, enquanto que uma percentagem idêntica de organizações dizem não saber responder a esta questão.

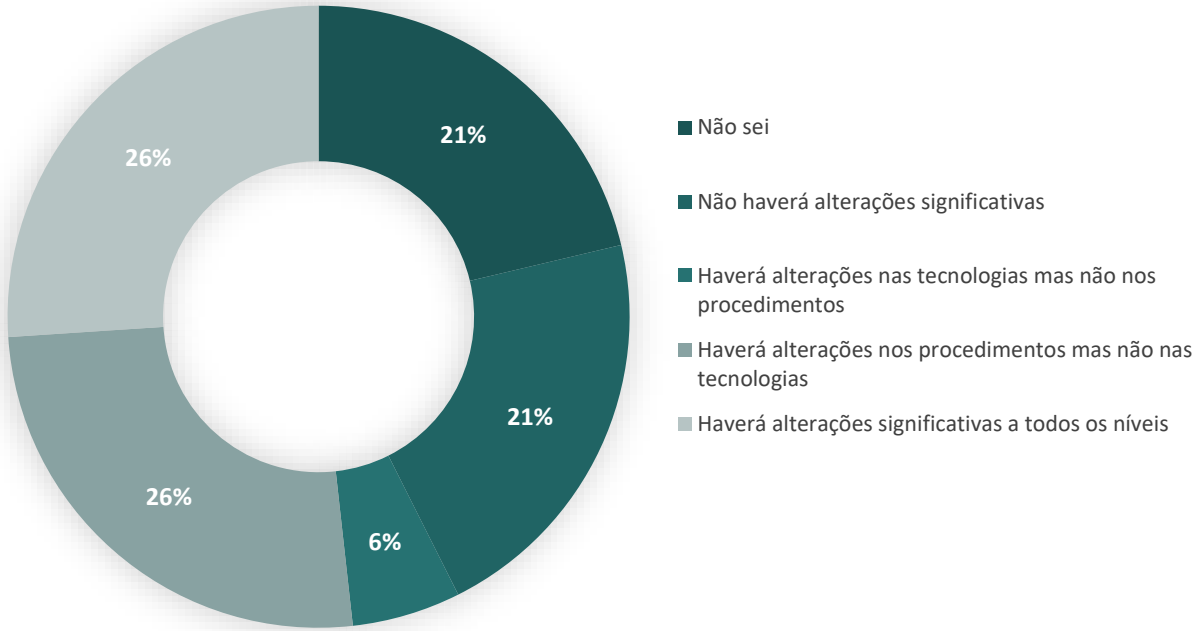
Dos inquiridos, 6% consideram que haverá alterações nas tecnologias que envolvem a segurança de informação mas não nos procedimentos.

Perspetiva LCG

Apenas com uma análise do nível de conformidade e da adequação dos procedimentos e tecnologias, será possível identificar a necessidade para eventuais alterações significativas.

À medida que o RGPD for sendo aplicado, assistir-se-á a uma maior consciência do nível de conformidade e, como tal, a uma diminuição das organizações que não sabem ou consideram não serem necessárias alterações significativas.

Alterar significativamente os procedimentos e tecnologias?



| Planeamento para Conformidade

A sua organização está a planear aumentar o número de empregados dedicados a programas de privacidade de dados?

Resultados

A esmagadora maioria das empresas, de pequena e média dimensão, consideram que a sua organização não está a planear aumentar o número de colaboradores dedicados a programas de privacidade de dados.

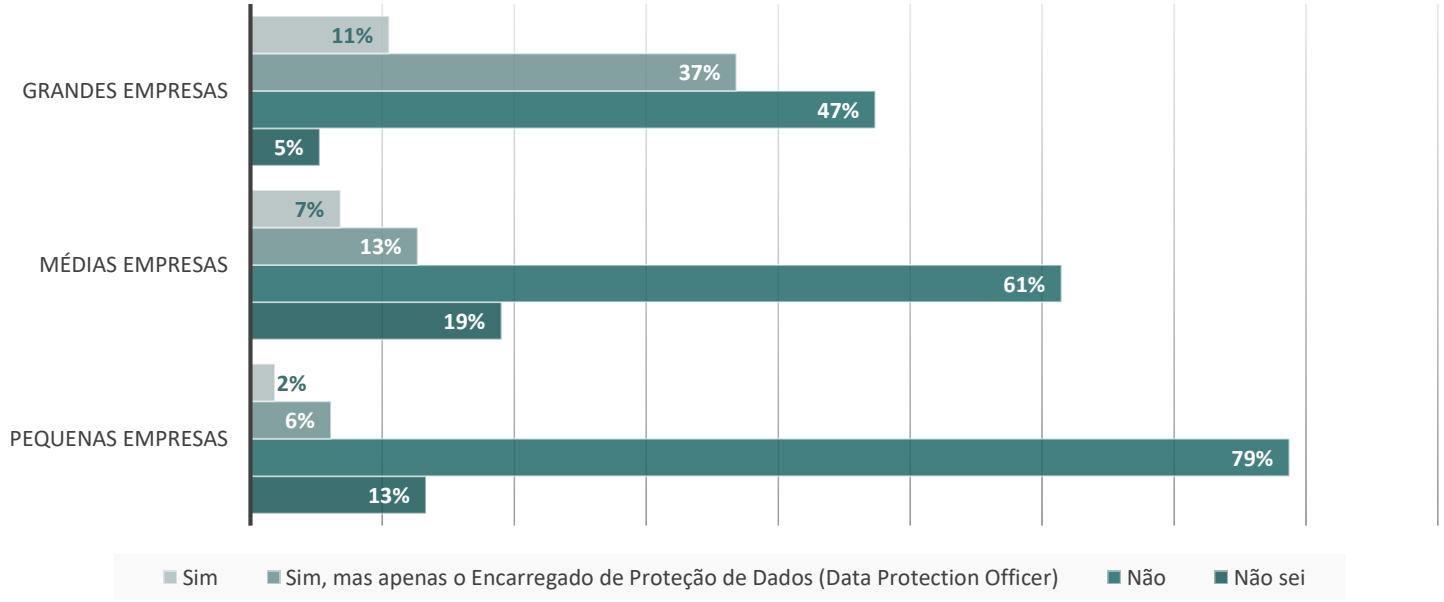
Por outro lado, 37% das empresas de grande dimensão, acreditam que as suas organizações estão a planear ter um encarregado de proteção de dados.

Perspetiva LCG

É nas empresas de maior dimensão que se encontra a necessidade, sensibilidade e capacidade para o aumento de colaboradores dedicados ao programa de proteção de dados.

No entanto, com o evoluir da aplicação do RGPD e o estabelecer das boas práticas, assistir-se-á a um maior investimento das organizações, seja em funções diretamente relacionadas com o RGPD (ex. DPO) ou em funções relacionadas com áreas de atividades complementares (jurídico, processual tecnológico).

Aumentar colaboradores dedicados ao programa?



| Sugestão LCG de Abordagem ao RGPD

| Este documento contou com a direção técnica da LCG e foi produzido por:

Filipe Pereira
Head of Digital Lead & Protection

Sofia Castro
Data Protection Delivery Manager

Para mais informação:
rgpd@lcg.consulting

LCG IMPROVE + TRANSFORM

IAPMEI Parcerias para o Crescimento

| Sugestão LCG de abordagem integrada para garantir a conformidade das organizações com o RGPD

Componente Jurídica

1. Avaliação da licitude do tratamento de dados;
2. Salvaguarda dos direitos dos titulares dos dados;
3. Adequação contratual com clientes e subcontratados;
4. Garantia de cumprimento de acordo com a legislação.

Componente Processual

1. Identificação, recolha, processamento e armazenamento;
2. Manuais de políticas e processos de processamento de dados;
3. Estabelecimento de procedimento de notificação;
4. Identificação inequívoca de responsabilidades.

Componente Tecnológica

1. Segurança e confidencialidade de dados pessoais;
2. Governance de partilha e acesso dos dados;
3. Autenticação e rastreio de utilizadores;
4. *Privacy by Default* e *Privacy by Design*