A LGPD PARA EMPRESAS

LGPD ADVANCE

Riosoft®

-A LGPD

Princípios da LGPD

Dados pessoais e dados sensíveis

Direitos do cidadão

Porque se preocupar com a LGPD?

Novas oportunidades de trabalho

-Segurança da Informação

Vulnerabilidades e Engenharia Social

Segurança da Informação X Segurança na TI

-A adequação à LGPD

Passos para a adequação

A LGPD Advance

SUMÁRIO

SUMÁRIO • SUMÁRIO • SUMÁRIO • SUMÁRIO • SUMÁRIO

-INTRODUÇÃO

No início de agosto de 2021 inicia-se a monetização da LGPD (aplicação de multas e sanções previstas na lei) e, diante disso, fica claro que as empresas precisam se adequar o quanto antes. No entanto, a aplicação dessas medidas não põe fim à preocupação das empresas, já que a Gestão de Dados pessoais não se encerra nessa data: esse é um processo contínuo de melhoria, que levará anos para se estabilizar até que a adequação segura seja atingida.

Assim, a adequação à LGPD é um grande desafio, uma vez que esse é um processo complexo que demanda comprometimento de todos os departamentos da empresa e um bom planejamento, além de uma metodologia eficaz.

Pensando nessas dificuldades e também nos ganhos inestimáveis que essa lei pode trazer para as organizações e para profissionais do setor jurídico e de outros setores que queiram trabalhar com LGPD, preparamos esse e-book com detalhes da lei, dicas para adequação, oportunidades de trabalho e processos que podem facilitar a adequação à LGPD.

-A LGPD

Com os avanços tecnológicos e o crescente acesso à Internet, surgiu a necessidade de que fossem criadas políticas para o tratamento de um conjunto de temas relacionados à Segurança da Informação.

Em maio de 2018, na União Europeia, entrou em vigor a GDPR (General Data Protection Regulation, em inglês), lei que visa proteger os dados de todos os indivíduos desse bloco econômico. A GDPR institui que somente países adequados a uma lei de proteção de dados podem se relacionar com os países europeus e, por isso, caso uma legislação não fosse adotada no Brasil, nosso país perderia espaço comercial.

Assim, em agosto daquele mesmo ano, o então presidente da República do Brasil, Michel Temer, sancionou a Lei 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), que determina regras sobre coleta, armazenamento, tratamento e compartilhamento de dados com o objetivo de regulamentar e garantir a privacidade e a transparência no uso de dados pessoais por parte de pessoa física ou pessoa jurídica, de direito público ou privado, em qualquer meio, inclusive nos meios digitais.

Após anos de discussões sobre a proteção de dados e direitos de informação ao cidadão, a LGPD consolida e unifica diversas legislações e dispositivos que tratam do assunto.

ME
NU

Princípios da LGPD

A LGPD traz mudanças significativas na forma de utilização dos dados dos consumidores por empresas e terceiros. De acordo com essa nova lei, as práticas das organizações devem respeitar 10 princípios de privacidade a fim de comprovar, por exemplo, a necessidade dos dados coletados para o seu negócio, assim como a qualidade e a segurança no tratamento e compartilhamento desses dados.

1- FINALIDADE

Tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

2- ADEQUAÇÃO

Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

3- NECESSIDADE

Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

4- LIVRE ACESSO

Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

5- QUALIDADE DOS DADOS

Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados.

6- TRANSPARÊNCIA

Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis
sobre a realização do tratamento e os respectivos agentes de tratamento;

Princípios da LGPD

A LGPD traz mudanças significativas na forma de utilização dos dados dos consumidores por empresas e terceiros. De acordo com essa nova lei, as práticas das organizações devem respeitar 10 princípios de privacidade a fim de comprovar, por exemplo, a necessidade dos dados coletados para o seu negócio, assim como a qualidade e a segurança no tratamento e compartilhamento desses dados.

7- SEGURANÇA

Utilização de medidas 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 difusão;

8- PREVENÇÃO

Adoção medidas prévias para evitar a ocorrência de danos em virtude do tratamento de dados pessoais;

9- NÃO DISCRIMINAÇÃO

Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

10- RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS

Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Dados pessoais e dados sensíveis

A LGPD define **dado pessoal** como "qualquer informação relativa a uma pessoa natural identificada ou identificável", o assim chamado **titular de dados**. Os dados pessoais são classificados como **identificados**, pelos quais é possível identificar diretamente o indivíduo (por exemplo: nome completo, RG, CPF), ou como **identificáveis**, que não identificam diretamente o indivíduo, mas que, junto a outros dados, podem ajudar a identifica-lo (por exemplo: número do cartão de crédito, empresa em que trabalha, endereço, IP do computador).

A LGPD também determina regras específicas para a utilização dos **dados sensíveis**, que se referem aos dados raciais e de etnia, de opinião religiosa ou política, dados genéticos ou sobre a vida sexual da pessoa. Veja a diferença:

Dados Pessoais	***Dados Pessoais Sensíveis***
CPF ou RG	Origem racial ou étnica
Endereço	Convicção religiosa
E-mail	Opinião política
Número de telefone	Filiação a sindicato ou a organização de caráter religioso, filosófico ou político
	Informação referente à saúde ou à vida sexual
	Dados genéticos ou biométricos

Direitos do cidadão

A LGPD proporcionará uma maior segurança ao titular dos dados, que deve manifestar, de forma clara e por escrito, consentimento na utilização de seus dados. Hoje, apesar de esses dados serem confidenciais, é comum que sejam compartilhados ou comercializados sem conhecimento e autorização dos consumidores, o que resulta, entre outros problemas, em telefonemas e contatos indesejados. Com a nova lei, isso não será mais permitido.

Pela LGPD, está garantido ao titular, por exemplo, o direito de **anonimização**, **bloqueio ou eliminação** de seus dados dentro de uma organização, assim como o direito de **confirmação e acesso**, no qual o titular pode solicitar a confirmação da existência de um tratamento e acesso aos seus dados pessoais, a razão pelas quais eles são armazenados, a origem da informação e quais os critérios de uso da empresa.

Porque se preocupar com a LGPD?

Empresas de todos os setores e de diferentes portes tratam dados pessoais. Assim, a utilização desses dados é, na maioria das vezes, crucial para o negócio. No entanto, com a instituição da LGPD, o tratamento de dados pessoais somente poderá ser realizado se estiver em conformidade com uma das bases legais previstas na lei. Por isso, as empresas devem adotar medidas de segurança, governança e boas práticas, de modo que garantam os direitos dos titulares de dados e o cumprimento da lei, sem que isso afete o seu negócio.

Além disso, a LGPD prevê, sob a fiscalização da ANPD, a aplicação de sanções e multas às companhias em caso de descumprimento das normas estabelecidas pela nova lei, que variam desde a suspensão do exercício da atividade de tratamento dos dados pessoais até a aplicação de multas no valor de 2% a 5% do faturamento da empresa.

Novas oportunidades de trabalho

Para o correto cumprimento da lei, surgem, além de oportunidades para os prestadores de serviços, novos postos de trabalho dentro das empresas, cada um com responsabilidades e deveres específicos quanto ao uso dos dados pessoais do titular:

- ENCARREGADO (DPO)

Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador e o titular (ou com A ANPD caso já efetuada alguma denúncia). Independentemente do porte ou segmento da empresa, torna-se obrigatório nomear um DPO, que será indispensável no processo de adequação à lei. Essa nova função é uma excelente oportunidade profissional para advogados e profissionais do setor jurídico e pode ser exercida por um funcionário ou, devido ao alto grau de especialização que a profissão exige, por uma empresa terceirizada.

- CONTROLADOR

Responsável pelo tratamento (uso) dos dados pessoais.

Exemplo: Loja que coleta os dados do titular para a realização de um cadastro.

- OPERADOR

Pessoa ou empresa terceira que realiza o tratamento dos Dados.

Exemplo: O escritório contábil que administra a carteira da empresa.

-Segurança da Informação

É preciso estar preparado para manter a proteção de dados e da empresa diante das ameaças internas e externas existentes. É preciso vencer os desafios para se proteger dos crimes cibernéticos. E a Segurança da Informação (SI) está diretamente relacionada com a proteção de um conjunto de informações no sentido de preservar o valor que possuem para um indivíduo ou uma organização.
Os princípios da Segurança da Informação (SI) são: confidencialidade, integridade, disponibilidade e autenticidade. Vejamos cada um deles a seguir.

SEGURANÇA DA INFORMAÇÃO • SEGURANÇA DA INFORMAÇÃO • SEGURANÇA DA INFORMAÇÃO • SEGURANÇA DA INFORMAÇÃO • SEGURANÇA DA INFORMAÇÃO • SI

CONFIDENCIALIDADE

• Somente pessoas explicitamente autorizadas podem ter acesso à informação;
• A principal forma de mantê-la é por meio da autenticação, controlando e restringindo os acessos;
• É necessário garantir que a informação esteja acessível apenas para pessoas autorizadas, impondo limites aos milhares de dados sigilosos que as empresas possuem.

Sem a confidencialidade as empresas ficam vulneráveis a ataques cibernéticos, a roubos de informações confidenciais e até à utilização de dados pessoais de clientes, o que pode causar diversos prejuízos, inclusive prejuízos financeiros.

INTEGRIDADE

• Refere-se à manutenção das condições iniciais das informações de acordo com a forma que foram produzidas e armazenadas;
• A informação acessada é completa, sem alterações ou distorções (confiável). Só deve ser mantida a origem da informação, ou seja, ela não pode ser alterada;
• Somente pessoas autorizadas poderão acessar e modificar os dados no sistema.

Quando o processo é executado com habilidade e inteligência, é possível utilizar ferramentas para realizar a recuperação das informações danificadas ou perdidas.

DISPONIBILIDADE

Esse princípio se refere à eficácia do sistema de funcionamento da rede para que seja possível utilizar a informação quando necessário.

• Os dados corporativos precisam estar seguros e disponíveis para serem acessados a qualquer momento pelos usuários autorizados. A hospedagem das informações deve ser realizada em um sistema a prova de falhas lógicas e redundantes, ou seja, excessivas e exageradas.
• Os dados precisam ser facilmente encontrados e processados quando houver necessidade de gerar relatório.

AUTENTICIDADE

Esse princípio diz respeito quando um usuário manipula algum dado e ocorre uma documentação sobre esta ação. Esse processo realiza a tarefa de identificar e registrar o usuário que está enviando ou modificando a informação.

Mas é preciso tomar cuidado: os dados são fatos em sua forma primária e, por isso, precisam ser arranjados e organizados de uma maneira mais significativa. A informação é o conjunto de dados organizados de tal maneira que adquirem valor adicional, além do valor do dado em si. Somente o princípio da autenticidade garante a veracidade da informação, a origem autêntica, mas a informação gerada, não. Neste sentido, é preciso pensar nas ameaças, ataques e vulnerabilidades do sistema.

-Vulnerabilidade e Engenharia Social

Quando falamos em Segurança dos Dados temos que ter em mente que todos os dados do titular estão sujeitos a vulnerabilidades que podem comprometer a sua integridade e ocasionar, entre outros problemas, o vazamento dos dados. Essas vulnerabilidades podem ser, por exemplo, físicas (instalação predial, controle de acesso, data center), naturais (desastres como incêndios, quedas de energia) ou humanas (falta de treinamento e alinhamento com as políticas de segurança da empresa, vandalismo e sabotagem).

A má instalação do hardware ou a utilização de um software desatualizado são exemplos de situações que também podem trazer vulnerabilidades no tratamento dos dados, já que expõem a empresa a ameaças virtuais. Dentre essas ameaças, as mais comuns são:

VÍRUS

Programa de computador que, propositalmente, se instala e infecta redes de computador em questão de minutos, podendo implicar na interrupção das atividades operacionais. É uma ameaça poderosa para a proteção de dados pessoais ou informações confidenciais.

MALWARE

Malware vem da junção de duas palavras inglesas “malicious” e “software” e se refere a softwares indesejados, tais como vírus, worms, cavalo de troias (trojans) e spyware. Para evita-lo, utilze antivírus e firewalls.

PHISHING

É uma forma de fraude na internet. Geralmente a vítima recebe um e-mail pedindo para alterar um cadastro, autenticar uma senha ou participar de alguma promoção, que não existe. O cadastro serve apenas para roubar as informações.

SPAM

E-mails ou mensagens publicitárias indesejadas que podem vir acompanhadas de mecanismos para induzir a outros problemas técnicos, como algum vírus.

RANSOMWARE

Tipo de software que restringe o acesso ao sistema infectado com uma espécie de bloqueio e cobra um resgate para devolver o controle de acesso às informações.

Então, surge o elemento que deve despertar preocupação, a Engenharia Social, termo utilizado para descrever o método de ataque no qual alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário para obter informações que podem ser utilizadas para a obtenção de acesso não autorizado a computadores ou informações.

A Engenharia Social é baseada na manipulação de pessoas, ou seja, tenta fazer com que as pessoas façam o que ela – a engenharia social – quer que elas façam. A Engenharia Social também é baseada na inteiração humana: é comandada por pessoas que usam o erro, a falha, o equívoco, para violar os procedimentos de segurança que, normalmente, deveriam ser seguros.

Exemplos:

• Uso de dois computadores com facilidade, entre eles, de acesso a informações confidenciais. Muitas empresas têm o costume de pegar aqueles relatórios que não estão usando mais e usar o verso das folhas como rascunho. Isto representa um risco;

• Uso de impressoras compartilhadas por mais de um departamento, onde alguém imprime folhas de teste. Essas folhas ficam ao lado da impressora e servem de base para informações – que muitas vezes podem ser informações confidenciais;

• Uso de pen drive. O uso descuidado de um pen drive representa um risco, porque nele pode ter um software malicioso que vai capturar informações e pode infectar a máquina;

• Uso de caderninhos, agendas ou bloquinhos de notas, que normalmente ficam ao lado da máquina com senhas e anotações, também facilitam a divulgação de dados e até mesmo a invasão a máquinas.

• Uso de e-mails fishing que consiste em mensagens falsas, enviadas por criminosos, que se passam por empresas ou pessoas confiáveis com o intuito de obter dados privados das vítimas;

• Uso de smishing, um tipo de fishing, realizado por mensagens de texto enviadas por celular;

• Uso de visching, um tipo de fishing, realizado por meio de chamadas telefônicas;

• Bentin (ou isca) que assim como um Cavalo de Troia, usa a mídia física e explora a curiosidade do alvo.

• Uso de redes sociais (como LinkdIn e o Facebook) por parte dos criminosos, para criar confiança do usuário e obter os dados.

Diante dessas vulnerabilidades, cabe à empresa mitigar e diminuir a probabilidade de que ataques ou ciberameaças sejam bem-sucedidos. Isso deve ser feito, por exemplo, com a implantação de uma **política de backup**, que mantém a integridade e a disponibilidade das informações e das instalações computacionais e, se realizado da maneira correta, pode dar continuidade às operações empresariais caso ocorra algum ataque hacker ou problemas técnicos.

Atrelado à política de backup, as empresas devem aplicar **protocolos de armazenamento e tratamento de dados** que respeitem as imposições da lei e o ciclo de vida dos dados, além de **políticas de recuperação de desastres.** A adoção de uma **política de senhas** também se faz necessária. A maioria das violações de hackers é feita a partir de senhas corporativas legítimas consideradas fracas. O sequestro de dados feito por ransomwares foi um dos ataques mais frequentes nos últimos dois anos. Sua causa, quase sempre, foi por comportamento inadequado no ambiente de trabalho, o que reforça a importância de garantir que os usuários da rede corporativa realizem acessos seguros aos dados da empresa. A política de senhas surge nesse cenário para resolver a situação.

Segurança da Informação X Segurança na TI

É importante observar que a LGPD não diz respeito somente aos dados digitais.

Um dado físico também pode passar por um vazamento, passível de punições previstas na lei. Uma nota escrita à mão, a pasta do funcionário no RH ou um contrato impresso contendo os dados de um cliente precisam ser protegidos tanto quanto os dados no computador, no servidor ou na nuvem. Portanto é importante enxergar a forma que a empresa manuseia os dados como um todo.

Assim, a LGPD não abrange apenas o setor de TI, mas também o financeiro, os recursos humanos, o departamento comercial, o marketing e todos os setores que trafegam dados pessoais. Por isso, não confunda a Segurança da Informação com a Segurança na TI.

-A adequação à LGPD

A Lei Geral de Proteção de Dados determina que uma pessoa natural ou jurídica, de direito público ou privado, deve deixar claro para qual finalidade utilizará dados pessoais, solicitar o consentimento de seus titulares e realizar o devido tratamento dos dados.

Entender e classificar corretamente os dados se torna, então, um processo importante para estar em conformidade com a LGPD, através da implementação de políticas, processos e programas apropriados para gerenciar a forma de coletar, processar, analisar, armazenar, compartilhar, reutilizar e eliminar esses dados.

Diante desse contexto, a Gestão do Ciclo de Vida dos Dados deve ser incorporada ao negócio, considerando a finalidade do fornecimento de seus bens e serviços.

MENU

-Passos para a adequação

A Riosoft desenvolveu uma metodologia de implantação da LGPD, a LGPD Advance. Seu conteúdo, descrito abaixo, é decisivo para iniciar os trabalhos de implantação da LGPD e reduz em mais de 60% o tempo para conformidade e em 80% os custos para o cumprimento da lei. Esse caminho é desenhado em etapas e cada um atende a ações específicas do processo de validação da LGPD.

O primeiro passo do projeto interno para a implantação da segurança de dados na empresa é o planejamento do projeto a partir da definição do cronograma e da mobilização e conscientização das equipes.

Em seguida, é necessário realizar o mapeamento de dados, incluindo o ciclo de vida e os riscos de privacidade associados. Ao mapear os dados pessoais tratados na empresa, é possível diagnosticar a situação em relação à legislação e, a partir disso, planejar as estratégias para a adequação. Nesse levantamento inicial é importante saber, por exemplo:

- ✔ Qual informação pessoal é coletada?
- ✔ Descrição da informação
- ✔ Qual a necessidade dessa informação?
- ✔ A informação é obrigatória?
- ✔ Como a informação chega?
- ✔ Qual a origem da informação?
- ✔ Como a informação é enviada?
- ✔ Qual o formato da informação?
- ✔ Onde fica armazenada?
- ✔ Quem tem acesso?
- ✔ Quanto tempo a informação permaneceu no setor?
- ✔ A informação é destruída?
- ✔ Existe normativo exigindo a informação? Se sim, qual ou quais?

Desse modo, o comitê interno deve mapear todos os pontos da empresa que estão passíveis de um vazamento de dados, identificar a probabilidade de vazamento e quais seriam os impactos causados por esse vazamento. É nessa etapa que os testes de invasão (Pentest) devem ser realizados e, após a revisão de processos, incluindo a revisão dos procedimentos de segurança física, as políticas de segurança e de privacidade precisam ser definidas.

Por fim, a empresa deve construir o **plano de ação** para a jornada de conformidade à LGPD, tomando decisões e aplicando ações que reduzam os riscos dos pontos mais críticos identificados no mapeamento.

CONSCIENTIZAÇÃO	*MAPEAMENTO*		*PLANO DE AÇÃO*
Capacitação dos colaboradores	**Inventário de dados** Políticas Gestão de terceiros Impacto à privacidade	**Governança e DPO** **Teste de invasão aplicações**	**Adequação dos pontos críticos**

MENU

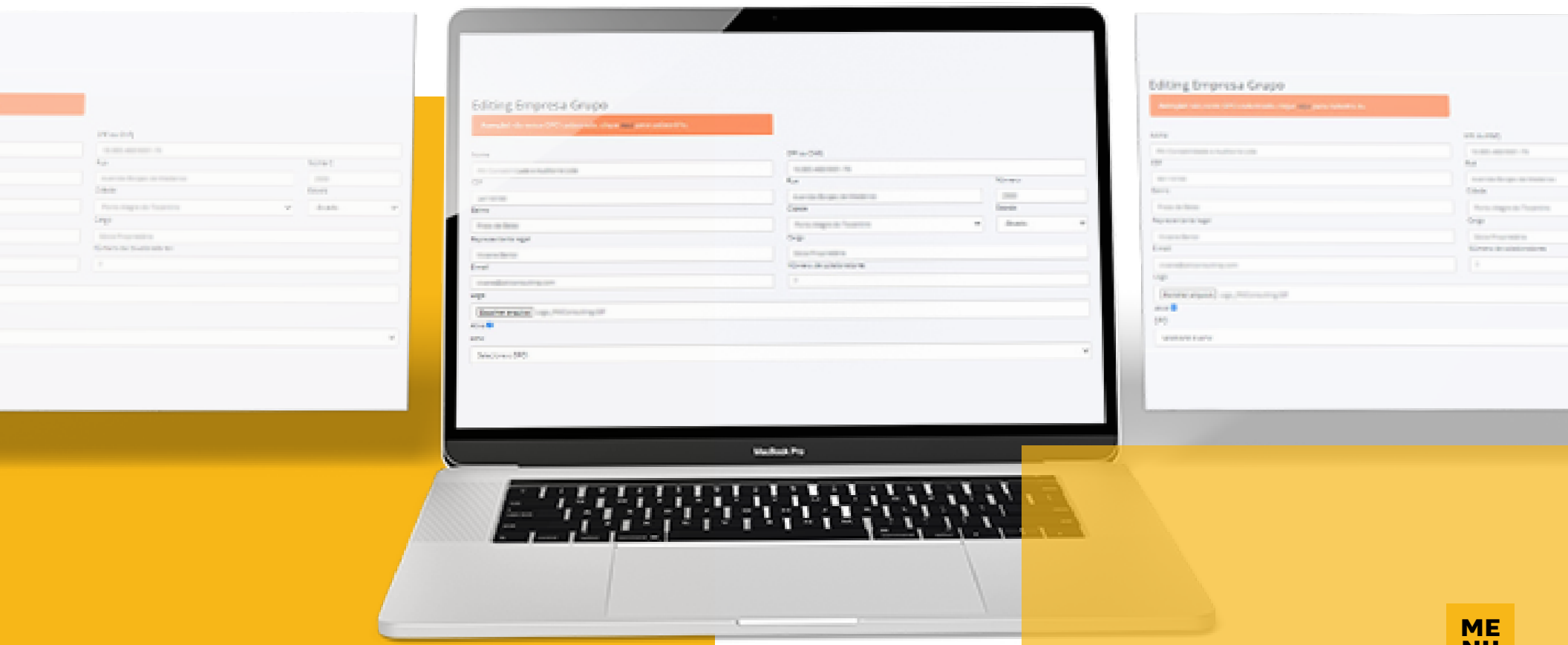
-A LGPD ADVANCE

Além da implantação da lei em 3 passos, a LGPD Advance e oferece um completo sistema para gerenciamento e implantação das exigências da LGPD, o Alvo Scan. Esse sistema conta com uma base de dados com mais de 40 modelos de documentos, tutoriais, políticas, cronogramas e inventários com processos pré-definidos, com possibilidade de customização de acordo com a necessidade da sua empresa. Por meio de nosso sistema é possível, ainda, gerenciar riscos através de DPIA (Matriz de Risco), controlar ocorrências e incidentes e emitir relatórios com filtros e dashboards.


Arquivos
Legenda:
Aguardando validação
Aprovado
Revisar
+ Novo Arquivo
Filtrar
Todos
Modelo de Cláusula Pa
Data de validade: 22/04/2021
Contrato
Data de validade: 18/11/2021
Nomeação DPO
Data de validade: 25/03/2021
Nomeação do Comitê
Data de validade: 09/04/2021
Relatório Inventário de Dados
Parâmetros
Todos
Gerar Relatório
Veja algumas das
funcionalidades do sistema
ALVO SCAN
Minhas solicitações
3
Solicitações não atendidas
12
Solicitações Respondidas
9
solicitações em tramitação
1
Pesquisar
Protocolo
Tipo
Data da abertura
Solicitante
2020.1
Acesso aos dados
09/10/2020
Roberto
2020.2
Informação das entidades que o controlador realizou uso compartilhado de dados
09/10/2020
Rodrigo
2020.18
Informação das entidades que o controlador realizou uso compartilhado de dados
08/12/2020
Everton
2020.3
Portabilidade dos dados
09/10/2020
Maria Alice
2020.4
Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa
09/10/2020
Pedro Roberto

DIAGNÓSTICO

Questionário individual e setorizado para levantamento de informações relacionadas a processos, engenharia social, políticas, contratos e documentos.



MENU

INVENTÁRIO DE DADOS (MAPEAMENTO)

Criação do mapa do fluxo de dados dentro da organização de modo que se possa ter uma visão unificada do inventário de dados e de como esses dados foram planejados para estarem em conformidade com a LGPD.

MATRIZ DE RISCO

Ferramenta integrada com o inventário de dados que define a probabilidade e impacto de todos os processos da empresa que trafegam dados de pessoas físicas (gerenciamento dos riscos).

DIREITOS DOS TITULARES

Gerenciamento de solicitações dos titulares dos dados que, de acordo com a LGPD, têm o direito de solicitar a revisão de decisões tomadas em relação ao tratamento de seus dados pessoais e que afetem os seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

OCORRÊNCIAS

Gestão das ocorrências com a possibilidade de instalação de sistema na máquina dos colaboradores para que os mesmos possam relatar ocorrências anonimamente.

MENU

DOCUMENTOS COMPLEMENTARES

As políticas e manuais, com modelos pré-formatados, trazem observações jurídicas e orientações que auxiliam na adequação de seus processos à LGPD. É possível inserir políticas de segurança da informação, código de ética e outros documentos de acordo com a necessidade de sua empresa.

RELATÓRIOS

Emissão de relatórios de impacto de dados, de mapeamento de fluxo de dados e de compartilhamento com terceiros, com opções de filtros de dashboards.

MENU


ESTÁ PRONTO?
Pronto para a adequação?
Conte com nossa equipe!

Ficou com alguma dúvida?

Acesse **www.lgpdadvance.com.br** para saber mais ou entre em contato com nossos consultores.

E-mail: contato@lgpdadvance.com.br

Telefone/Whatsapp: (17) 3215-9199

NÓS PODEMOS TE AJUDAR • NÓS PODEMOS TE AJUDAR • NÓS PODEMOS TE AJUDAR • NÓS PODEMOS TE AJUDAR