THALES

# White Paper: Acelerando a Conformidade com a Lei Geral de Proteção de Dados do Brasil (LGPD)

- Anonimização e / ou pseudonimização de dados pessoais
- Controle de acesso a dados sensíveis
- Monitoramento e registros de acessos aos dados
- Proteção de dados em ambientes de infraestrutura híbridos
- Autenticação segura e centralizada

# LGPD: Um divisor de águas para os direitos de privacidade brasileiros

## A Lei Geral de Proteção de Dados (LGPD) do Brasil foi sancionada em 14 de agosto de 2018, e entra em vigor em agosto de 2020.

A LGPD cria uma nova estrutura legal para o uso de dados pessoais no Brasil, tanto online quanto off-line, nos setores público e privado. A LGPD está substituindo ou complementando várias leis e regulamentações já existentes, algumas das quais estavam em conflito ou não tinham segurança jurídica. A LGPD torna o país mais competitivo no contexto de uma sociedade cada vez mais impulsionada pela transformação digital.

**De acordo com o Artigo 1 da Lei:**

Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Ao promulgar a Lei Geral de Proteção de Dados, o Brasil pode ser considerado como um país com nível adequado de proteção à privacidade e ao uso de dados pessoais.

**Ampla aplicabilidade e pesadas penalidades**

De maneira semelhante ao General Data Protection Regulation (GDPR) da União Europeia, a LGPD terá aplicação extraterritorial, ou seja, o dever de cumprimento excederá os limites geográficos do país. Qualquer empresa estrangeira que tenha pelo menos uma filial no Brasil, ou ofereça serviços para o mercado brasileiro e colete e processe dados pessoais de titulares de dados localizados no país, independentemente da nacionalidade, estará sujeita à nova lei.

E como o GDPR, a penalidades pesadas podem ser aplicadas às organizações que não cumprem a lei. Entre as sanções, há autuações e multas, que podem variar de 2% do faturamento da empresa no Brasil (limitado no total a 50 milhões de reais) por infração. Há também a possibilidade de multa diária e a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

# Artigos relevantes a proteção de dados

Os trechos a seguir foram extraídos da Lei Brasileira nº 13.709 (LGPD), de 14 de agosto de 2018.[1]

## Aplicação

**Art. 3.** Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural

ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados ….

## Dados anonimizados

**Art. 5.** Para fins desta Lei, aplicam-se as seguintes definições:

ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados ….

III - dado anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

## Tratamento de dados

**Art. 6.** As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

VII - 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;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

X - 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 anonimizados não considerados dados pessoais

**Art. 12.** Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

**Art. 13.** §4º. "Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro"

## Responsabilidade e registro de acesso

**Art. 37.** O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

**Art. 38.** A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, uma descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e análise do controlador com relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados.

[1]http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

# Artigos relevantes a proteção de dados

### Responsabilidade do controlador e dos processadores

**Art. 42.** O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

### Da segurança e do sigilo de dados

**Art. 46.** Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

### Notificação de vazamento de dados

**Art. 48.** O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

### Melhores práticas de segurança de dados

**Art. 49.** Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

### Sanções administrativas

**Art. 52.** Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I – advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a 50 milhões de reaispor infração;

III – multa diária, observado o limite total a que se refere o inciso II;

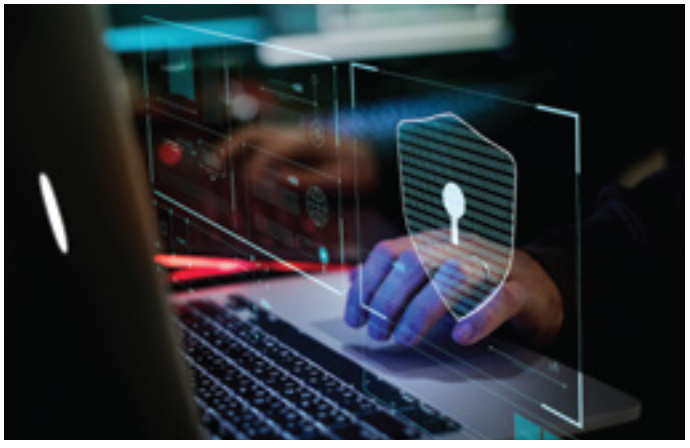
IV – publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V – bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI – eliminação dos dados pessoais a que se refere a infração;

# Transformação digital, nuvem, big data e o desafio da conformidade

A Lei Geral de Proteção de Dados (LGPD) do Brasil exige as melhores práticas em segurança para dados pessoais e observa que os dados pessoais que tiverem sido anonimizados não serão considerados no escopo da Lei, se não puderem ser revertidos facilmente para o seu estado original por aqueles que possam obtê-los.



O desafio para a empresa moderna, é como equilibrar a necessidade de usar estes dados para processos, análises de negócios e ultimamente o sucesso no mercado, com a proteção aos dados confidenciais contra hackers, pessoas de dentro da organização ou vazamentos acidentais.

Por exemplo, os dados têm que fluir entre várias plataformas na nuvem e nas dependências da empresa, além de serem acessados por funcionários remotos e analisados em plataformas de big data. Durante todo o processo, os dados devem estar seguros para permanecer em conformidade com a LGPD e leis semelhantes.

Diante da transformação digital, as atuais estratégias de segurança usadas por empresas se tornam insuficientes. À medida que as empresas implementam novas tecnologias como nuvem e big data, muitas vezes escolhem soluções pontuais para proteger dados em uma plataforma ou outra. Isso leva a uma abordagem de segurança fragmentada e a falhas na proteção de dados.

# Melhores práticas e as soluções da Thales Cloud Protection & Licensing

## Entre as melhores práticas de conformidade e segurança para uma empresa com infraestrutura de TI híbrida incluímos quatro aspectos que se tornam essenciais no processo de conformidade com a LGPD:

- Anonimização e / ou pseudonimização de dados pessoais
- Proteção de dados em ambientes de infraestrutura híbridos
- Autenticação segura e centralizada
- Controle de acesso a dados sensíveis
- Monitoramento e registros de acessos aos dados

A Thales Cloud Protection & Licensing tem ampla experiência em conformidade com legislações como GDPR ou regulamentos como PCI. Além disso, a Thales é extremamente experiente em implementações abrangentes para corporações globais, em múltiplas plataformas de TI híbridas.

## Nossas soluções oferecem aos clientes recursos para:

1. Anonimização e pseudonimização de dados
2. Proteção de dados em nuvens múltiplas
3. Gerenciamento das chaves usadas para criptografia de dados
4. Controle de acesso do usuário a dados
5. Registros de eventos de acesso a dados
6. Proteção de dados em implementações abrangentes em TI híbrida.

# 1. Anonimização e pseudonimização de dados

### Criptografia transparente de dados em repouso

A solução Vormetric Transparent Encryption da Thales protege os dados com criptografia para dados em repouso de arquivo e nível de volume, controles de acesso e registro de auditoria de acesso a dados sem aplicativos de reengenharia, banco de dados ou infraestrutura. A instalação do software de criptografia transparente de arquivos é simples, escalável e rápida, com agentes instalados acima do sistema de arquivo em servidores ou máquinas virtuais para assegurar políticas de segurança e conformidade de dados. O gerenciamento de política e criptografia de chaves é fornecido pela Vormetric Data Security Manager.

### Tokenização com mascaramento dinâmico de dados

A solução Vormetric Vaultless Tokenization com Mascaramento Dinâmico de dados reduz drasticamente os custos e os esforços necessários para cumprir com as políticas de segurança e normas regulatórias, como a LGPD. A solução oferece capacidades para tokenização de banco de dados e segurança de tela dinâmica. As empresas podem eficientemente realizar seus objetivos de proteger e pseudoanonimizar ativos sensíveis — estejam eles em ambiente de data center, big data, em container ou na nuvem.

### Módulos de Segurança de Hardware (HSMs)

Os Módulos de Segurança de Hardware (HSMs) SafeNet Luna são certificados FIPS 140-2 nível 3, e INMETRO (ITI ICP-BRASIL), com uma ampla gama de usos para acelerar operações criptográficas, proteger o ciclo de vida de chave criptográfica e fornecer uma base de confiança para toda a sua infraestrutura de criptografia. A premiada solução SafeNet Data Protection On Demand é uma plataforma baseada em nuvem que fornece uma ampla gama de serviços de gerenciamento de chaves e HSM na nuvem por meio de um simples mercado on-line. Isso inclui o HSM como serviço e o Key Management como serviço.

# 2. Proteção de dados em nuvens múltiplas

### Soluções de segurança BYOE e BYOK para nuvem

A Thales oferece várias maneiras de proteger dados em plataformas na nuvem. Organizações podem trazer sua própria criptografia para a nuvem (BYOE - Bring Your Own Encryption) usando nossa solução Vormetric Transparent Encryption. Clientes também podem adicionar camada de segurança às suas implementações BYOK (Bring Your Own Key), usando o CipherTrust Cloud Key Manager (CCKM) para obter visibilidade e gerenciamento centralizados de ciclo de vida de várias nuvens, com armazenamento seguro de chaves FIPS-140-2.

# 3. Gerenciamento das chaves usadas para criptografia de dados

### Gerenciamento de chaves centralizado

A solução Vormetric Integrated Key Management unifica e centraliza o gerenciamento de criptografia de chaves no local e fornece gerenciamento seguro de chaves para soluções de armazenamento de dados. Os produtos para gerenciamento de chave na nuvem incluem o CipherTrust Cloud Key Manager.

# 4.Controle de acesso do usuário e autenticação

### Gerenciamento de acesso baseado em nuvem como serviço

O SafeNet Trusted Access simplifica o login dos usuários, pois é um serviço de gerenciamento de acesso que protege e gerencia centralmente o acesso a aplicativos baseados na web ou na nuvem. Empresas podem escalar os controles de acesso à nuvem enquanto atendem às necessidades dos negócios, de gerenciamento de riscos e de conformidade ao aplicar políticas flexíveis baseadas em risco, SSO na nuvem e métodos de autenticação universal.

### Gerenciamento de identidades e acesso

Com as soluções Safenet Identity and Access Management, empresas podem proteger facilmente os aplicativos na nuvem ou no centro de dados, e atender às necessidades de gerenciamento de risco com base em suas estruturas de segurança atuais e utilizando os métodos de autenticação existentes para acesso à informação.

### Gerenciamento de acesso a dados baseado em criptografia

A solução Vormetric Data Security Manager da Thalespermite que a organização limite os privilégios de acesso de usuários a sistemas de informações que contenham informações sensíveis.

## 5. Registro de acesso ao banco de dados

### Security Intelligence Logs

A solução Security Intelligence Logs da Plataforma Vormetric permite que sua organização identifique tentativas de acesso não autorizado e desenvolva parâmetros de modelos de acesso do usuário autorizado. A Vormetric Security Intelligence integra-se aos principais sistemas de gerenciamento de eventos e informações de segurança (SIEM) que tornam essas informações acionáveis.

## 6. Proteção de dados em ambientes de infraestrutura híbridos

### Plataforma de proteção de dados para infraestrutura hibrida

A Vormetric Data Security Platform é uma plataforma extremamente flexível e escalonável, oferecendo proteção e controle de acesso a bancos de dados, arquivos e contêineres - e pode proteger dados que residem em ambientes de nuvem, virtuais, big data e físicos. As plataformas e tecnologias suportadas inclui:

- **IaaS, PaaS e SaaS: Amazon Web Services, Google Cloud Platform, Microsoft Azure, Salesforce, Microsoft Office365**
- **OSs: Linux, Windows and Unix**
- **Big data: Hadoop, NoSQL, SAP HANA e Teradata**
- **Container: Docker, Red Hat OpenShift**
- **Database: IBM DB2, Microsoft SQL Server, MongoDB, MySQL, NoSQL, Oracle, Sybase entre outros**

**Aonde quer que você opere e qualquer que seja o regulamento, você pode confiar na Thales para ajudá-lo a gerenciar o seu risco. A Thales pode ajudar a sua organização a cumprir com muitos dos requisitos da LGPD.**

## Recursos relacionados

Vormetric Data Security Platform Overview[2]

Vormetric Transparent Encryption[3]

Vormetric Tokenization com Mascaramento Dinâmico de dados[4]

Gerenciamento Centralizado de Chaves[5]

CipherTrust Cloud Key Manager[6]

Information and Access Management Solutions[7]

SafeNet Trusted Access: Cloud-based Access Management[8]

SafeNet Data Protection on Demand[9]

SafeNet Luna Network HSMs[10]

Vormetric Security Intelligence com Integração SIEM[11]

[2]https://www.thalesesecurity.com/products/data-encryption/vormetric-data-security-platform
[3]https://www.thalesesecurity.com/products/data-encryption/vormetric-transparent-encryption
[4]https://www.thalesesecurity.com/products/data-tokenization-masking-and-transformation/tokenization-data-masking
[5]https://www.thalesesecurity.com/products/key-management
[6] https://go.thalesesecurity.com/rs/480-LWA-970/images/CipherTrust-Cloud-Key-Manager-from-Thales-pb.pdf
[7]https://www.gemalto.com/enterprise-security/identity-access-management
[8]https://safenet.gemalto.com/resources/data-protection/safenet-trusted-access-product-brief/
[9]https://safenet.gemalto.com/data-protection-on-demand/
[10]https://safenet.gemalto.com/data-encryption/hardware-security-modules-hsms/safenet-network-hsm/
[11]https://www.thalesesecurity.com/products/data-encryption/security-intelligence-logs

## Sobre a Thales Cloud Protection & Licensing

A Thales Cloud Protection & Licensing é líder mundial em proteção de dados e habilita as organizações a proteger e gerenciar suas informações mais confidenciais – dados, identidades e propriedade intelectual – onde quer que sejam criadas, compartilhadas ou armazenadas. A Thales ajuda as empresas a enfrentar momentos decisivos, como mudar sua segurança para a nuvem, alcançar a conformidade com confiança e criar mais valor através de software em dispositivos e serviços usados por milhões de consumidores todos os dias. Seja protegendo a nuvem, pagamentos digitais, blockchain ou a Internet das Coisas, as marcas mais respeitadas e as maiores organizações de todo o mundo confiam na Thales para acelerar sua transformação digital. A Thales Cloud Protection & Licensing faz parte do Grupo Thales.

THALES


### Americas - Thales Cloud Protection and Licensing

Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100 | Austin, TX 78759 USA

Tel: + 1 888 343 5773 or + 1 512 257 3900
Fax: +1 954 888 6211 | Email: sales@thalesesec.com

### Asia Pacific - Thales Transport & Security (HK) Ltd

Unit 4101-3, 41 /F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 814 | E-mail: asia.sales@thales-esecurity.com

### Europe, Middle East, Africa

Meadow View House, Long Crendon,
Aylesbury, Buckinghamshire HP18 9EQ
Tel: +44 (0) 1844 201800 | Fax: +44 (0) 1844 20550
E-mail: emea.sales@thales-esecurity.com


**> thalescpl.com <**