

TREND MICRO™ E A LEI GERAL DE PROTEÇÃO DE DADOS

O QUE É A LGPD?

Aprovada em 14 de Agosto de 2018, a Lei Geral de Proteção de Dados (LGPD) foi baseada na lei europeia de proteção de dados (*General Data Protection Rule*, GDPR), e “[...] dispõe sobre o tratamento de dados pessoais [...], com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”, entrando em vigor em 2020.

.....

AS SOLUÇÕES

TREND MICRO™

Com a intenção de ajudar as organizações a superar esse desafio, a Trend Micro™ elaborou um compilado de ações direcionadas por nossa estratégia de segurança em camadas a nível de usuário (*User Protection*), rede (*Network Defense*) e nuvem híbrida (*Hybrid Cloud Security*), que já podem ser tomadas.



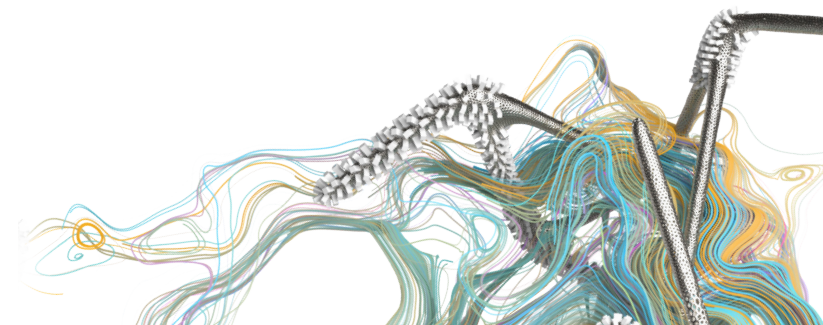
DESAFIOS

Empresas e organizações têm à frente o desafio de se adequar aos requerimentos dessa nova lei em um período relativamente curto. Em 28 de Dezembro de 2018, a Autoridade Nacional de Proteção de Dados foi criada, no entanto até o momento, a mesma não lançou nenhuma definição formal e específica de requisitos ou *guidelines* técnicos que devem ser atendidos para fortalecer a postura defensiva de operadores de dados.

A possibilidade de multas no montante de 2% do faturamento do seu último exercício (limitadas a R\$ 50.000.000,00), em adição à outras perdas financeiras e de reputação vindas de um vazamento de dados, apenas aumenta a ansiedade tanto da liderança quanto das equipes técnicas de instituições de todos os setores.

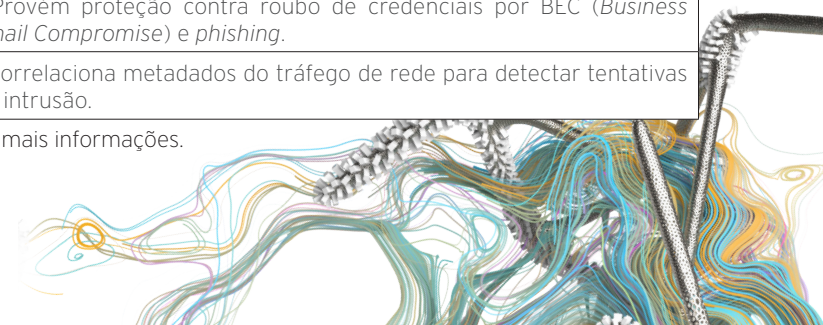


REQUISITO LGPD	ESTRATÉGIAS	PRODUTOS / SERVIÇOS	FUNCIONALIDADES
Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.	  	Gap Analysis	Maiores detalhes na descrição dos serviços abaixo.
		Health Check	
		Risk Assessment	
Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: [...] § 2º As informações e os dados poderão ser fornecidos, a critério do titular: I - por meio eletrônico, seguro e idôneo para esse fim; [...]	 	Cloud App Security	• Controle interno de conteúdo enviado nos e-mails; • Proteção contra vazamentos de dados (iDLP); • Proteção de armazenamento em nuvem.
		InterScan Messaging Security	• Módulo adicional de controle criptográfico (Encryption for Email); • Proteção contra vazamentos de dados (iDLP).
		ScanMail	• Controle interno de conteúdo enviado nos e-mails; • Proteção contra <i>inside threat actors</i>; • Proteção contra vazamentos de dados (iDLP).
		Trend Micro Email Security	• Módulo adicional de controle criptográfico (Encryption for Email); • Proteção contra vazamentos de dados (iDLP).
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.		Deep Security (System Security)	• O módulo de Integrity Monitoring pode monitorar registros de importância, detectando alterações nos mesmos.

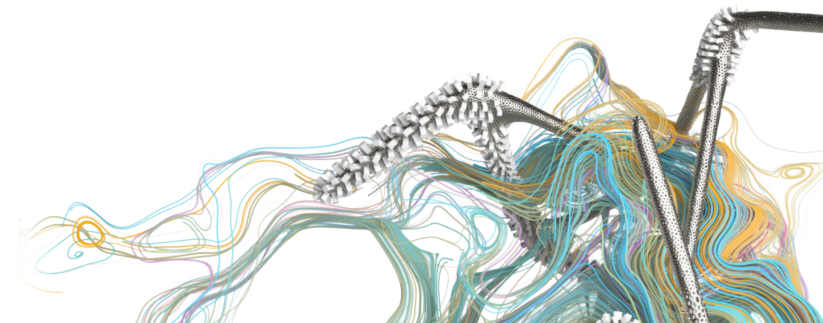


REQUISITO LGPD	ESTRATÉGIAS	PRODUTOS / SERVIÇOS	FUNCIONALIDADES
Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.	  	Apex One ¹	- Endpoint Detection and Response (EDR) para detecção e investigação de incidentes de segurança; - Geração de relatórios relacionados às configurações de segurança do ambiente.
		Detecção e Resposta a Incidentes (MDR)	Maiores detalhes na descrição dos serviços abaixo.
		Gap Analysis	
		Health Check	
		Risk Assessment	
		Cloud App Security	- Geração de relatórios relacionados às configurações de segurança do ambiente; - Mantém registros de inconformidades e anomalias na manipulação de arquivos.
		Trend Micro Email Security	
		ScanMail	
		InterScan Messaging Security	- Geração de relatórios baseados em tentativas de intrusão bloqueadas; - Geração de relatórios detalhando filtros e vacinas digitais ativadas.
		TippingPoint	
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. [...] § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.	  	Apex One ¹	- Bloqueio de programas não previamente autorizados (Application Control); - Detecção comportamental de indicadores de ataque (IOA); - Previne intrusões por exploração de vulnerabilidades (Vulnerability Protection); - Proteção contra vazamentos de dados (iDLP).
		Cloud App Security	- Detecção de <i>spam</i> e <i>phishing</i> por aprendizado de máquina; - Proteção contra vazamentos de dados (iDLP); - Varredura de <i>malware</i> em arquivos.
		ScanMail	
		Deep Discovery Inspector	- Detecta comunicações suspeitas ou de fontes maliciosas conhecidas; - Detecta tentativas de intrusão na rede; - Protege contra ataques direcionados.
		Deep Discovery Email Inspector	Provém proteção contra roubo de credenciais por BEC (<i>Business Email Compromise</i>) e <i>phishing</i>.
		Deep Discovery Director Network Analytics	Correlaciona metadados do tráfego de rede para detectar tentativas de intrusão.

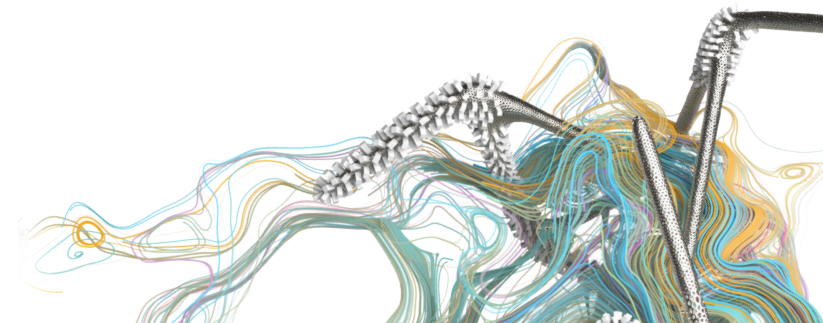
1 Algumas funcionalidades também se aplicam às soluções Worry-Free Services e OfficeScan. Consulte seu parceiro para mais informações.



REQUISITO LGPD	ESTRATÉGIAS	PRODUTOS / SERVIÇOS	FUNCIONALIDADES
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. [...] § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.	  	Deep Security	• Bloqueia programas não autorizados previamente (Application Control); • Impede comunicação com sites maliciosos (Web Reputation); • Impede conexões de rede não autorizadas (Firewall); • Inspecciona automaticamente logs para detectar atividades suspeitas (Log Inspection); • Monitora arquivos e diretórios de importância detectando alterações nos mesmos (Integrity Monitoring); • Previne intrusões por exploração de vulnerabilidades (Intrusion Prevention); • Protege contra software malicioso (Anti-Malware).
		Deep Security Smart Check	• Detecção de vulnerabilidades e <i>malware</i> em imagens de <i>containers</i>; • Integração transparente no ambiente CI/CD (<i>Continuous Integration/Continuous Delivery</i>); • Possibilita a identificação de imagens vulneráveis antes que cheguem em ambientes de produção de forma automatizada, contínua e frequente.
		InterScan Messaging Security	• Possui mecanismos para controle de criptografia dos dados em trânsito;
		InterScan Web Security	• Proteção contra vazamentos de dados (iDLP);
		Trend Micro Email Security	• Provém proteção contra roubo de credenciais por BEC (<i>Business Email Compromise</i>) e <i>phishing</i>.
		TippingPoint	• Detecta e previne continuamente intrusões a nível de rede, de ameaças conhecidas, desconhecidas e não divulgadas.
		Trend Micro Endpoint Encryption	• Criptografia completa de disco, diretório ou dispositivos removíveis, tornando os dados ininteligíveis a pessoas não autorizado; • Possui mecanismos para controle de criptografia dos dados em trânsito e dados em repouso.



REQUISITO LGPD	ESTRATÉGIAS	PRODUTOS / SERVIÇOS	FUNCIONALIDADES
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. § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: [...] III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. [...] § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: [...] II - medidas para reverter ou mitigar os efeitos do incidente. § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.	  	Deep Discovery Inspector	• Detecta comunicações suspeitas ou de fontes maliciosas conhecidas; • Distribuição de indicadores de ataque para prover proteção através de <i>Connected Threat Defense</i>; • Geração de relatórios relacionados às configurações de segurança do ambiente; • Monitora continuamente a rede por atividades suspeitas.
		Deep Discovery Director Network Analytics	• Correlaciona metadados do tráfego de rede para detectar tentativas de intrusão.
		Deep Security Smart Check	• Detecção de vulnerabilidades e <i>malware</i> em imagens de <i>containers</i>; • Gestão de riscos a partir da detecção de vulnerabilidades de imagens em <i>registries</i>.
		Detecção e Resposta a Incidentes (MDR)	Maiores detalhes na descrição dos serviços abaixo.
		Gap Analysis	
		Health Check	
		Risk Assessment	
		Trend Micro Endpoint Encryption	
			• Criptografia completa de disco, diretório ou dispositivos removíveis, tornando os dados ininteligíveis a pessoal não autorizado.



REQUISITO LGPD	ESTRATÉGIAS	PRODUTOS / SERVIÇOS	FUNCIONALIDADES
Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. [...] § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: I - implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; [...] d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; [...] f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;	  	Apex Central ¹	- Centraliza informações referentes às definições de segurança do ambiente; - Permite visão holística de <i>compliance</i> referente às regras estabelecidas pela companhia.
		Deep Discovery Inspector	- Detecta comunicações suspeitas ou de fontes maliciosas conhecidas; - Detecta tentativas de intrusão na rede; - Geração de relatórios relacionados às configurações de segurança do ambiente; - Monitora continuamente a rede por atividades suspeitas; - Protege contra ataques direcionados.
		Deep Security Smart Check	- Detecção de vulnerabilidades e <i>malware</i> em imagens de <i>containers</i>; - Possibilita a identificação de imagens vulneráveis antes que cheguem em ambientes de produção de forma automatizada, contínua e frequente.
		Detecção e Resposta a Incidentes (MDR)	Maiores detalhes na descrição dos serviços abaixo.
		Gap Analysis	
		Health Check	
		Phish Insight	
		Risk Assessment	
		TippingPoint	Detecta e previne continuamente intrusões a nível de rede de ameaças conhecidas, desconhecidas e não divulgadas.

¹ Algumas funcionalidades também se aplicam ao Trend Micro Control Manager. Consulte seu parceiro para mais informações.

REQUISITO LGPD	ESTRATÉGIAS	PRODUTOS / SERVIÇOS	FUNCIONALIDADES
Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. [...] § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: I - implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; [...] d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; [...] f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;	  	Trend Micro Endpoint Encryption	• Criptografia completa de disco, diretório ou dispositivos removíveis, tornando os dados ininteligíveis a pessoal não autorizado; • Geração de relatórios com informações referentes a adequação às normativas; • Possui mecanismos para controle de criptografia dos dados em trânsito e dados em repouso.

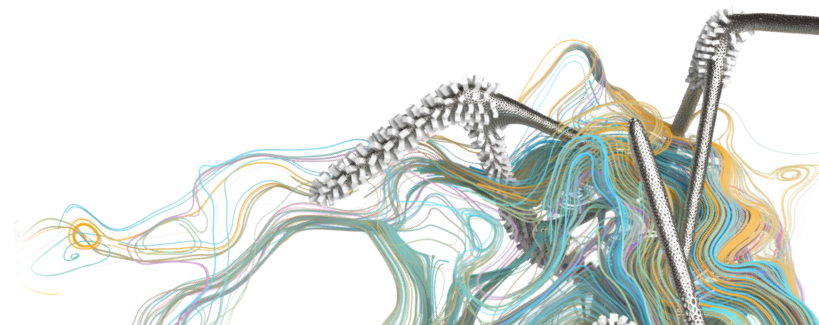


NETWORK DEFENSE

Atualmente as empresas estão na mira de um conjunto cada vez mais complexo de *ransomware*, ameaças avançadas, ataques direcionados, vulnerabilidades e *exploits*. Somente a visibilidade completa de todo o tráfego e atividade da rede manterá a organização à frente de ataques direcionados, que driblam controles tradicionais, exploram vulnerabilidades de rede e sequestram ou roubam dados sensíveis, comunicações e propriedade intelectual. Trend Micro™ *Network Defense* detecta e previne violações em qualquer lugar da rede, para proteger dados críticos e a reputação da organização.

As soluções Trend Micro™ de *Network Defense* preservam a integridade da rede enquanto garantem que dados, comunicações, propriedade intelectual e outros ativos intangíveis não sejam comprometidos por intrusos. Uma combinação de prevenção contra invasões e detecção de brechas *next-generation* permite que a empresa evite ataques direcionados, ameaças avançadas e *ransomware* infectem ou se disseminem na rede.

- **Art. 6º** [...] demonstração, pelo agente, da adoção de medidas eficazes [...] de proteção de dados pessoais
- **Art. 19** § 2º As informações e os dados poderão ser fornecidos, a critério do titular:
I - por meio eletrônico, seguro e idôneo para esse fim; [...]
- **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** [...] 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.
- **Art. 46** [...] 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.
- **Art. 50** [...] que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

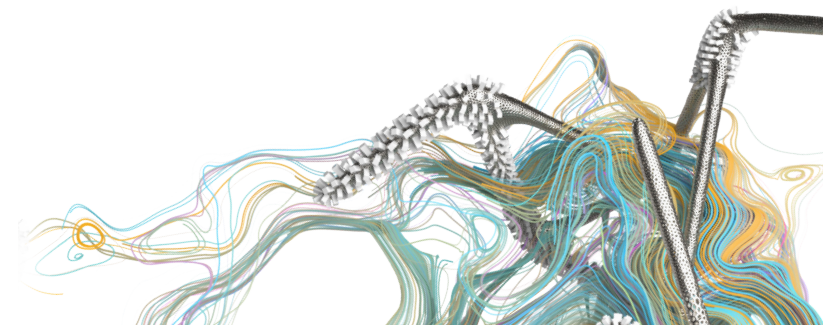


HYBRID CLOUD SECURITY

A solução Trend Micro™ *Hybrid Cloud Security* protege os *workloads* corporativos no *data center* e em nuvem contra ameaças críticas, que podem causar interrupções significativas nos negócios, ao mesmo tempo em que ajudam a acelerar a conformidade regulamentar.

Se você está focado em proteger ambientes físicos, virtuais, em nuvem ou híbridos, a Trend Micro™ oferece a segurança avançada do servidor que você precisa com a plataforma Trend Micro™ Deep Security. Disponível como *software*, no Amazon Web Services e no *marketplace* da Azure, ou como um serviço, o Deep Security oferece segurança otimizada para VMware, Amazon Web Services e Microsoft Azure.

- **Art. 6º** [...] demonstração, pelo agente, da adoção de medidas eficazes [...] de proteção de dados pessoais
- **Art. 19** § 2º As informações e os dados poderão ser fornecidos, a critério do titular:
I - por meio eletrônico, seguro e idôneo para esse fim; [...]
- **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** [...] 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.
- **Art. 46** Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais [...].
- **Art. 48** [...] III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; [...].
- **Art. 50** [...] a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; [...]



USER PROTECTION

É uma suíte interconectada de produtos de segurança a técnicas avançadas de defesa, protegendo usuários de *ransomwares* e outras ameaças que afetam *endpoints*, *gateways* e aplicações. Permite à organização proteger as atividades de todos os usuários em qualquer aplicação, dispositivo ou local.

Ferramentas como o novo Apex One, representam a crista da onda na nossa frente de *User Protection*, unindo tecnologias intergeracionais de proteção contra ameaças, proteção contra perda de dados sensíveis (*Data Loss Prevention*, DLP) e mecanismos para detecção e resposta à incidente (v. DETECÇÃO E RESPOSTA A INCIDENTES) em um único agente e gerenciado a partir de um único console.

- **Art. 19 § 2º** As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; [...]

- **Art. 46** Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais [...]

DEEP SECURITY SMART CHECK

A segurança tradicional para times de desenvolvimento tem sido feita de maneira segmentada, com diversas ferramentas para diferentes departamentos operados por várias pessoas. No entanto, essa abordagem está mudando rapidamente com as empresas visando a migração das operações de desenvolvimento para plataformas de *container* e em nuvem. Isso acaba fazendo com que as organizações comecem a revisar as melhores maneiras de proteger esses ambientes mantendo integridade e confidencialidade. Soluções de segurança precisam ser modeladas para conseguir proteger variados tipos de ambiente, como físico, virtual, e em nuvem, provendo sinergia entre as equipes de segurança e *DevOps*, utilizando uma ferramenta que consiga consolidar e colabora com os requisitos de segurança e conformidade sem interferir nos ciclos de desenvolvimento de CI/CD. O Deep Security Smart Check entrega de maneira automatizada um *scan* de imagem com verificações tanto de vulnerabilidades quanto de ameaças e controle de acesso.

A solução foi feita para garantir a segurança das imagens antes de entrar em linha de produção do CI/CD (*Continuous Implementation/Continuous Delivery*) sem nenhum risco de impactos negativos, fazendo com que os times de desenvolvimento continuem a entregar as aplicações com menor chance de impactar o negócio nem o cliente final.

- **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. [...]

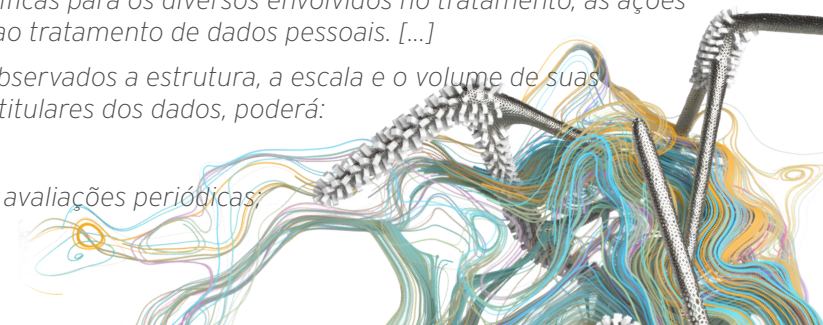
§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

- **Art. 50** Os controladores e operadores [...] poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos [...] as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. [...]

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo: [...]

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;



PHISH INSIGHT

Trend Micro™ Phish Insight é uma ferramenta de simulação de *phishing* totalmente gratuita que permite testar e instruir seus funcionários sobre como identificar e evitar ataques de *phishing*. Com o Phish Insight você pode executar uma simulação de *phishing* realista e seguro em menos de 5 minutos. Através dele, é possível envolver todos os membros de sua organização em um processo educativo, construindo de maneira interativa uma cultura de segurança que fortalecerá os elos mais fracos da sua postura defensiva.

- **Art. 50** [...] poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
-

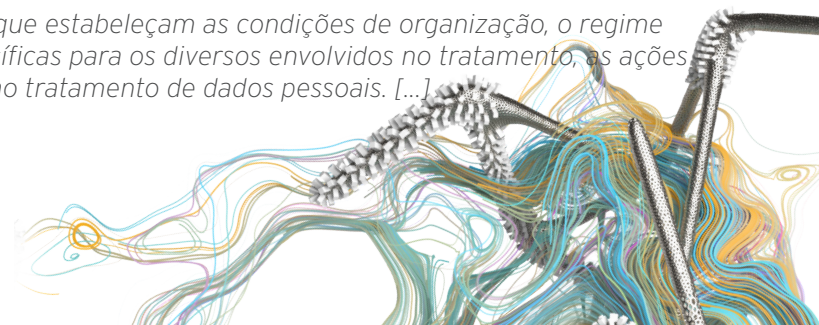
GAP ANALYSIS

Utilizando as ferramentas Trend Micro™ da frente de *Network Defense*, o *Gap Analysis* é um serviço que coleta dados de tráfego de rede e à partir dos mesmos formula relatórios, transformando dados em inteligência e provendo uma visão sucinta e holística de ameaças ao ambiente. Essas mesmas informações podem ser correlacionadas com os resultados de detecção e resposta à incidente para obter discernimentos aprofundados sobre ameaças previamente desconhecidas.

- **Art. 6º** [...] 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.
- **Art. 38** A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais [...] o relatório deverá conter [...] a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.
- **Art. 48** O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança [...] e deverá mencionar, no mínimo:
 - III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados [...]
 - IV - os riscos relacionados ao incidente;
 - VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. [...]

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá [...] determinar ao controlador a adoção de providências, tais como: [...]

 - II - medidas para reverter ou mitigar os efeitos do incidente.
- **Art. 50** Os controladores e operadores [...] poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, [...] as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. [...]
 - f) [...] estabeleça e aplique mecanismos de supervisão internos e externos; [...]
 - h) seja atualizado constantemente com base em informações obtidas a partir de [...] avaliações periódicas;



DETECÇÃO E RESPOSTA A INCIDENTES (MDR)

Com a sofisticação cada vez maior das invasões, as empresas precisam ter recursos de detecção e resposta a incidentes mais avançados. Correlacionar ameaças de rede, do servidor e dos endpoints para se ter uma imagem completa de um ataque direcionado é uma estratégia de detecção muito eficaz. Infelizmente, em virtude da falta de conhecimento em cibersegurança e de profissionais capacitados, as empresas têm muitas dificuldades para correlacionar os diversos alertas e dados por conta própria.

Nosso serviço de MDR usa IA avançada para correlacionar e priorizar alertas e dados do cliente, analisando-os com a inteligência de ameaças da Trend Micro™ para determinar se ameaças ou eventos fazem parte de um ataque maior. Com as ameaças correlacionadas e priorizadas, nossa equipe começa a investigá-las mais a fundo. Além disso, realizamos varreduras regulares no ambiente dos clientes para detectar possíveis indicadores de ataque (IoAs) e os procuramos continuamente.

A equipe de resposta a incidentes investiga as ameaças em questão, coletando mais informações (com a aprovação do cliente), determinando vulnerabilidades e entendendo o que mais pode ter sido baixado ou se a ameaça original sofreu uma mutação e se espalhou. Fazemos uma análise completa para determinar a causa raiz e o possível impacto, além de gerar IoCs sobre o incidente para evitar futuros ataques. Você recebe um relatório sobre o incidente, recomendações sobre como reagir e remediar o ataque e, em alguns casos, ferramentas para ajudar na remediação.

- **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. [...]

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: [...]

II - medidas para reverter ou mitigar os efeitos do incidente.

- **Art. 50** Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo [...] mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

[...] § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador [...] poderá:

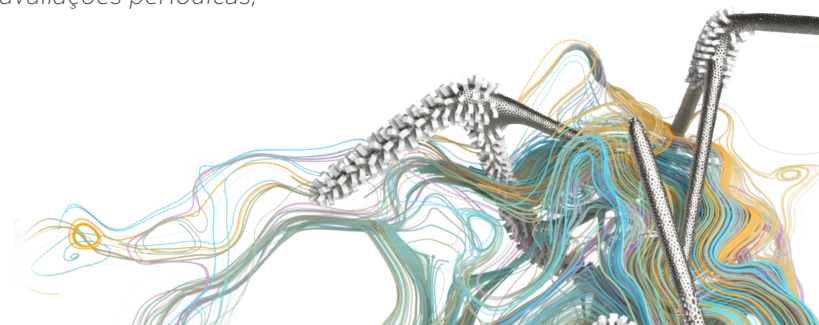
I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; [...]

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; [...]

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;



RISK ASSESSMENT

É uma análise de risco no ambiente de servidores do cliente que coleta informações sobre a postura defensiva atual relativa ao módulo de *Intrusion Prevention* do Deep Security. Devido às capacidades de *virtual patching*, que blinda aplicações e serviços obsoletos, o *Risk Assessment* pode ser de interesse particular para sistemas legados.

Ao final da análise, o cliente recebe um relatório completo contendo todas as informações relativas às vulnerabilidades encontradas no ambiente e recomendações para mitigar e/ou corrigir as mesmas.

HEALTH CHECK

Quando o ambiente está configurado adequadamente é possível um melhor acompanhamento do seu estado e aproveitamento das suas funcionalidades.

Uma vez que as soluções da Trend Micro atendem aspectos de conformidade de padrões internacionais (PCI-DSS, HIPAA, etc.), conhecer essas funções e validá-las através de um Health Check não só agrega confiabilidade a solução, mas também facilita a vida dos administradores, fornecendo dados para as auditorias e processos internos executados.

Além disso, mesmo as melhores ferramentas da indústria ainda têm sua eficácia limitada apenas pelo seu uso. Para tal, a Trend Micro™ disponibiliza diversos guias de melhores práticas para seus produtos.

Eles estão disponíveis para consulta em: docs.trendmicro.com

- **Art. 6º** [...] demonstração, pelo agente, da adoção de medidas eficazes [...] de proteção de dados pessoais
- **Art. 37** [...] controlador que elabore relatório de impacto à proteção de dados pessoais [...] para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.
- **Art. 38** [...] controlador que elabore relatório de impacto [...] deverá conter, [...] a metodologia [...] para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.
- **Art. 48** [...] O controlador deverá comunicar à autoridade nacional e ao titular [...] a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; [...] as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
- **Art. 50** [...] implementar programa de governança em privacidade que [...] seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

CONCLUSÃO

Conforme notícias de vazamentos de dados pessoais e sensíveis de centenas de milhões de cidadãos brasileiros se tornam mais comuns, somos lembrados da eminência da LGPD, das sanções legais que poderiam ser aplicadas às instituições afetadas, dos impactos que esses vazamentos têm em cidadãos e, por consequência, da necessidade da lei para a proteção dos mesmos.

A LGPD não deve ser vista como um empecilho, mas como uma oportunidade de fortalecer a segurança de todos os elementos, humanos, computacionais e processuais de todas as organizações dentro e fora de território nacional que operam dados brasileiros, dessa maneira tornando o Brasil mais seguro para a troca de informações digitais.

Descubra mais em www.trendmicro.com.br



Securing Your Connected World

©2019 by Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, endpoints,

