

Como a Varonis ajuda na conformidade com a LGPD



Conteúdo

Introdução	3
Dados pessoais em LGPD	3
Direitos de acesso do titular dos dados.....	4
Base legal para processamento de dados pessoais	5
Relatório de violações de dados	5
Multas	5
Como a Varonis ajuda na conformidade LGPD	6
Onde estão os dados pessoais.....	6
Automatizar Solicitações de Acesso de Assunto ..	7
Quem pode acessar dados pessoais.....	8
O que está acontecendo com os dados pessoais agora	9
Avaliação de Risco LGPD	10

Introdução

O Brasil aprovou a Lei Geral de Proteção de Dados Pessoais (LGPD) em agosto de 2018 e a maior parte da legislação entrará plenamente em vigor em agosto de 2021. Os especialistas em conformidade descrevem a LGPD como o "GDPR brasileiro" com diversas semelhanças entre as duas leis.

Neste artigo, discutiremos os principais conceitos da LGPD, o que os profissionais de cybersegurança precisam fazer para estarem em conformidade com ela e como a Varonis ajuda a cumprir seus requisitos.

Nota do editor: o autor não lê nem fala português. Todas as pesquisas e referências que se seguem são provenientes de outras pesquisas e de uma [tradução da lei](#).

Dados pessoais na LGPD

A LGPD define dados pessoais como "informações sobre uma pessoa natural identificada ou identificável". Dados pessoais podem incluir dados pessoais confidenciais ou dados pessoais anonimizados.

Assim, a LGPD considera todos os dados sobre um indivíduo brasileiro como dados pessoais, sendo necessário tratar igualmente todos os dados pessoais. A LGPD tem escopo extraterritorial, ou seja, se a sua empresa processa dados de cidadãos brasileiros, ela deve cumprir essa lei.

1. Direitos de acesso do titular dos dados
2. Base legal para o tratamento de dados pessoais
3. Como a Varonis ajuda na conformidade com a LGPD
4. Quem pode acessar os dados pessoais?
5. O que está acontecendo com os dados pessoais neste momento?
6. Relatório de risco gratuito

Direitos de acesso do titular dos dados

Solicitações do "direito a ser esquecido"

Na LGPD, os indivíduos têm o direito de saber quais dados você possui a respeito deles. Eles podem solicitar que você faça atualizações ou exclua dados. Eles podem saber quais outras organizações têm acesso aos dados deles por meio da sua organização e se os dados foram compartilhados com outras entidades. Podem também revogar o consentimento de tratamento dos dados pela organização, o que é popularmente conhecido como "direito de ser esquecido".

Na prática, o gerenciamento de solicitações do "direito de ser esquecido" é um desafio para os departamentos de TI. Não basta encontrar todos os dados de uma dada pessoa, é preciso também ser capaz de eliminá-los ou alterá-los em um prazo razoável.

A LGPD elenca vários direitos específicos dos "titulares dos dados", que são os indivíduos por trás da definição de dados pessoais da seção anterior. **Esses direitos estão presentes no art. 18.**

- I. Confirmação da existência de tratamento;
- II. Acesso aos dados;
- III. Correção de dados incompletos, inexatos ou desatualizados;
- IV. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com as disposições desta Lei;
- V. Portabilidade dos dados a outro fornecedor de serviços ou produtos, mediante requisição expressa e sujeita a sigilo comercial e industrial, conforme a regulamentação do órgão de controle;
- VI. Eliminação dos dados pessoais tratados com o consentimento do titular dos dados, exceto nas hipóteses previstas no art. 16 desta Lei;
- VII. Informações sobre entidades públicas e privadas com as quais o controlador compartilhou os dados;
- VIII. Informações sobre a possibilidade de negar o consentimento e as consequências de tal negativa;
- IX. Revogação do consentimento, conforme previsto no §5º do art. 8º desta Lei.

Base legal para o tratamento de dados pessoais

No art. 7º, a LGPD estabelece as maneiras como as organizações podem usar os dados pessoais e para quais finalidades.

As organizações precisam do consentimento do titular dos dados (o indivíduo que os dados representam) ou precisam anonimizar os dados para uso em estudos e pesquisas. Há também disposições que tratam do uso dos dados pessoais por parte do poder público para fins de saúde pública ou em processos judiciais, quando há necessidade documentada.

As organizações que obtêm consentimento para usar dados pessoais devem criar proteções e monitoramento para garantir que sejam usados somente para os fins corretos.

Para evitar vazamento de dados, acesso não autorizado e multas, você precisa saber o que está acontecendo com os dados pessoais. Caso haja um vazamento, você pode obter os logs e provar quais dados do indivíduo foram acessados e abordar o vazamento com essas informações. Caso contrário, você pode ter que assumir o pior cenário, em que houve vazamento de um servidor inteiro e lidar com um problema muito maior.

Você precisa saber o que está acontecendo com os dados pessoais.

Comunicação de vazamentos de dados

A LGPD não fornece um prazo específico para comunicar um vazamento de dados. O art. 48 diz que os controladores (organizações que tratam dados pessoais) devem comunicar vazamentos de dados à autoridade nacional (a Agência Nacional de Proteção de Dados, ou ANPD). Os controladores devem apresentar detalhes sobre os dados e os possíveis riscos que o incidente possa representar para os titulares. Devem também explicar como o vazamento ocorreu e que medidas foram tomadas para reverter ou mitigar os dados.

Multas

A eficácia das leis de proteção de dados está diretamente ligada às suas capacidades de execução. A multa máxima definida no art. 52 é de até 2% da receita brasileira, não podendo exceder 50 milhões de reais (que hoje equivale a cerca de 9 milhões de dólares).

Como a Varonis ajuda na conformidade com a LGPD

A Varonis ajuda a proteger e monitorar dados não estruturados para que você possa cumprir a LGPD e impedir vazamentos de dados que resultem em multa. A Varonis responde às perguntas: "onde nós armazenamos dados pessoais", "quem tem acesso a esses dados" e "o que está acontecendo com esses dados neste momento?" Essas três perguntas são vitais para provar e conseguir a conformidade com a LGPD.

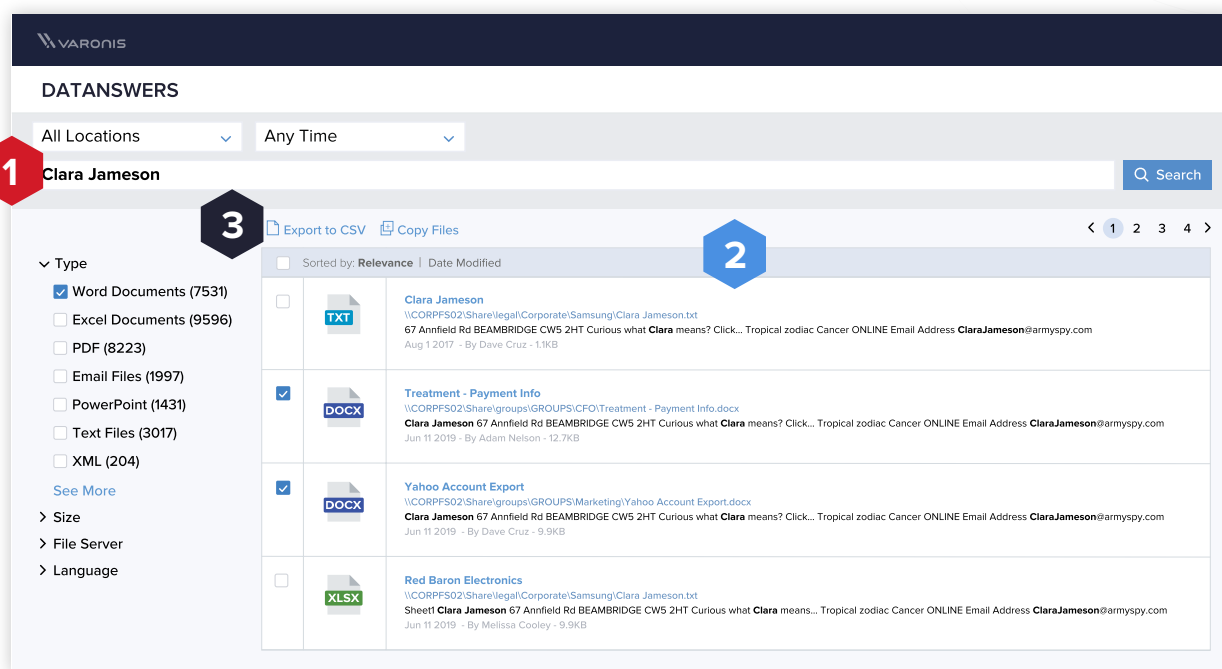
Onde estão os dados pessoais?

O **Data Classification Engine** é pré-configurado com centenas de padrões que podem descobrir, de maneira precisa e automática, informações pessoais específicas de cidadãos brasileiros em escala de petabytes. A Varonis vai além das expressões regulares com bancos de dados pré-construídos de valores válidos conhecidos, correspondência por proximidade, palavras-chave negativas e confirmação algorítmica para gerar resultados de alta precisão com poucos falsos positivos. Os padrões e as regras do Data Classification Engine são atualizados automaticamente para que você não fique para trás com alguma mudança na LGPD.

VARONIS				
File Server	Access Path	File Name	Classification Results	Match Count
CORPFS02	C:\Share\finance\bl\Braz...	Brazil Customer Data.docx	BR Personal	3
CORPFS02	C:\Share\finance\bl\Braz...	Brazil Customer Data.docx	BR Personal	3
CORPFS02	C:\Share\Market\Custom...	ClientFile.docx	BR Personal	3
CORPFS02	C:\Share\Market\Custom...	ClientFile.docx	BR Personal	3
CORPFS02	C:\Share\HR\Brazil...	Brazil ApplicantDetails.docx	BR Personal	3
CORPFS02	C:\Share\HR\Brazil...	BrazilApplicantDetails.docx	BR Personal	3
CORPFS02	C:\Share\legal\User Da...	User Data.docx	BR Personal	3

Automatização para solicitações de acesso a informações

O **DatAnswers** é um mecanismo de pesquisa rápido e poderoso, que pode ajudar você a encontrar PII em arquivos na nuvem e no local, em tempo recorde. Nunca foi tão fácil atender às solicitações de acesso de titulares dos dados (DSARs) ou cumprir os requisitos de descobertas eletrônicas na LGPD. Por trás da interface intuitiva do DatAnswer há uma lógica sofisticada e integrada, que garante resultados de alta fidelidade em todas as pesquisas. Os resultados da pesquisa em todos os tipos de repositórios de dados podem ser facilmente filtrados, exportados ou copiados para compartilhamento legal ou em conformidade.



1

Nosso formulário de DSAR emprega lógica sofisticada no back-end para garantir resultados de alta fidelidade

2

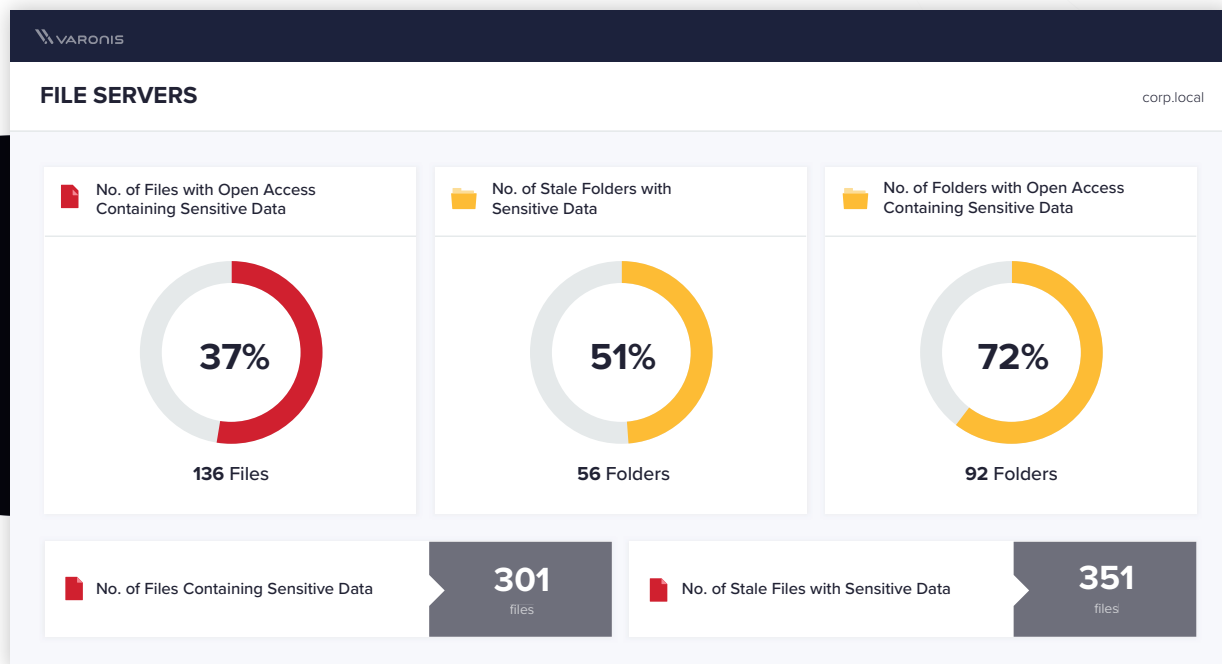
A lógica integrada marca os arquivos que trazem identificadores pessoais e os filtros facilitam o refinamento dos resultados

3

As informações pessoais podem ser facilmente copiadas, exportadas ou excluídas para atender às DSARs

Quem pode acessar os dados pessoais?

A **Varonis** mostra cada usuário, pasta e ACL em todos os seus repositórios de dados. Em seguida, obtém os resultados da classificação para mostrar onde estão os riscos de acesso não autorizado dos dados pessoais que possam levar a um vazamento de dados. O excesso de permissões de acesso é, de longe, o fator mais significativo em vazamentos de dados e ataques de ransomware. Quanto mais informações confidenciais um invasor puder acessar, mais danos poderá provocar e maior será a multa.



A limpeza dos grupos de acesso global e responsáveis pelo acesso excessivo é uma tarefa quase impossível de se fazer manualmente. Dada a complexidade para descobrir quem tem e quem realmente precisa ter acesso, aliada à velocidade com que novos dados são criados, as equipes podem levar anos para corrigir a superexposição dos dados. O Automation Engine pode remover automaticamente os grupos de acesso global em grande escala para reduzir o risco exponencialmente. São necessários apenas alguns dias para realizar uma tarefa que exigiria anos para ser feita manualmente. E como o DataPrivilege sabe quem acessa os dados, o Automation Engine pode dar acesso aos usuários ativos no processo. Assim, somente algumas pessoas têm acesso aos dados pessoais em uma pasta compartilhada, em vez de todo o grupo de usuários com acesso global.

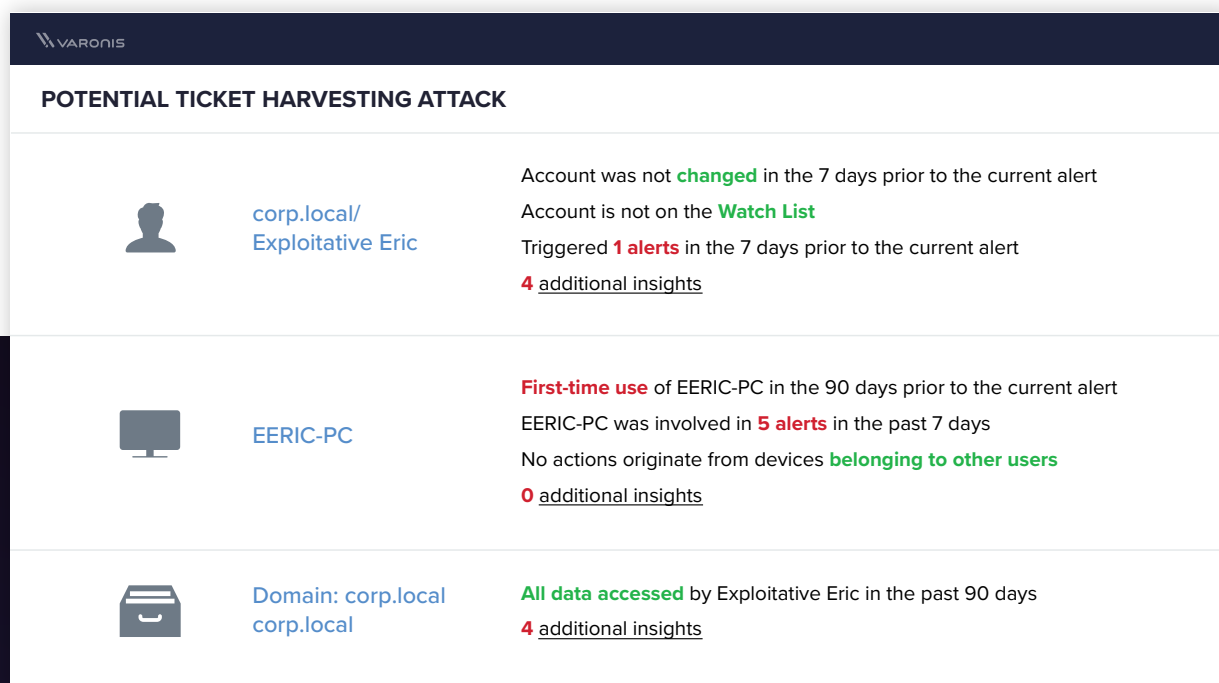


Seguindo em frente, a Varonis ajuda você a definir os proprietários dos dados que são responsáveis pelo acesso a seus dados. O **DataPrivilege** cria um processo para os usuários solicitarem acesso do proprietário dos dados, que pode aprovar, negar ou aprovar por um tempo limitado. O DataPrivilege automatiza auditorias de acesso a dados, para que a organização possa provar que implementou e mantém ativamente o acesso com privilégios mínimos.

O que está acontecendo com os dados pessoais neste momento?

Além dos modelos de ameaças integrados, a Varonis utiliza **análises avançadas de comportamento do usuário para detectar ameaças**. Coletamos bilhões de eventos de várias fontes de dados, sem recorrer a agentes de endpoint, e empregamos aprendizado de máquina para criar perfis comportamentais de cada usuário e dispositivo. Quando o comportamento foge do normal, disparamos um alerta.

Ao combinarmos eventos de fluxos de dados díspares, podemos adicionar contexto exclusivo aos alertas, tais como sensibilidade do arquivo e tipo de conta, tornando-os mais úteis do que os alertas SIEM tradicionais. Sinopses ricas em contexto do incidente e uma trilha de auditoria completa de todos os dados acessados ajudam a impulsionar as investigações para interromper os ataques antes que se tornem vazamentos de dados, bem como fornecer uma descrição clara e concisa do incidente para evitar grandes violações da LGPD.



POTENTIAL TICKET HARVESTING ATTACK

	corp.local/ Exploitative Eric	Account was not changed in the 7 days prior to the current alert Account is not on the Watch List Triggered 1 alerts in the 7 days prior to the current alert 4 additional insights
	EERIC-PC	First-time use of EERIC-PC in the 90 days prior to the current alert EERIC-PC was involved in 5 alerts in the past 7 days No actions originate from devices belonging to other users 0 additional insights
	Domain: corp.local corp.local	All data accessed by Exploitative Eric in the past 90 days 4 additional insights

A **Varonis** captura uma trilha de auditoria unificada de atividade dos arquivos, acesso ao Active Directory e telemetria do perímetro para que você saiba o que está acontecendo com os dados pessoais. Em caso de vazamento, é fácil ver exatamente quais arquivos foram afetados, para que você possa relatar tudo com precisão e se recuperar do incidente.

Nossa equipe de resposta a incidentes de cortesia pode ajudar você a investigar qualquer incidente gratuitamente.

Comece com um relatório de risco gratuito para a LGPD

Para ver onde estão as informações protegidas pela LGPD no seu ambiente, inscreva-se para um relatório de risco de dados gratuito para a LGPD. Nossos engenheiros fazem todo o trabalho pesado (definição, configuração e análise) e geram um relatório personalizado que mostra onde há informações pessoais expostas. Os resultados são seus, sem compromisso.



Rápido E Sem Complicações

Um engenheiro dedicado fará todo o trabalho pesado para você: implementação, configuração e análise. Você vai investir muito pouco tempo.

Totalmente Personalizado

A avaliação de segurança é totalmente adaptada às suas necessidades, regras e configurações para disponibilizar informações úteis para você.

Invisível E Não Intrusivo

A Varonis monitora milhões de eventos por dia para as maiores empresas do planeta. Não vamos desacelerar você nem o seu sistema.

Experimente a Varonis gratuitamente

Instale a Varonis no seu próprio ambiente.
É rápido e simples.

<https://info.varonis.com/pt/risk-assessment>

SOBRE A VARONIS

A Varonis é pioneira em segurança de dados e análises, lutando uma batalha diferente das empresas de segurança digital convencional. A Varonis tem foco em proteger dados corporativos locais ou armazenados em nuvem: arquivos e e-mails confidenciais; dados confidenciais de cliente, paciente e funcionário; históricos financeiros; planos estratégicos e de produto; e demais propriedades intelectuais.

A Plataforma de segurança de Dados Varonis detecta ameaças internas e ataques cibernéticos, analisando dados, as atividades de conta e o comportamento do usuário; impede e limita desastres bloqueando dados obsoletos e confidenciais; e mantém com eficiência um estado seguro com automação. Voltada para a segurança de dados, a Varonis atende a uma variedade de aplicações, entre elas governança, conformidade, classificação e análises sobre ameaças. A Varonis iniciou suas operações em 2005 e conta com milhares de clientes em todo o mundo, entre eles líderes de diversos setores como tecnologia, consumo, varejo, serviços financeiros, assistência médica, fabricação, energia, mídia e educação.