LGPD

A LEI E SEUS PROCESSOS

Entenda a lei para saber
como se adequar a ela.

- Classificação
- Manipulação
- Armazenamento
- Transporte de Dados

SOBRE A LGPD

LEI GERAL DE PROTEÇÃO DE DADOS (LEI 13.709/18)

O cotidiano das empresas está prestes a sofrer novo marco regulatório que as impactará como poucas leis antes fizeram. É o que promete a Lei Geral de Proteção de Dados ou simplesmente LGPD (lei 13.709/18), sancionada em 13/8/18 pela Presidência da República.

Os recentes escândalos de vazamento de dados da rede social Facebook – o mais famoso com o fornecimento de informações de milhares de usuários para a empresa britânica de big data e marketing político Cambridge Analytica – levaram diversos países a apressarem leis de proteção de informações pessoais.

Depois de a União Europeia publicar o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), o Senado Federal rapidamente aprovou, no dia 10 de julho de 2018, o PLC 53/18 consolidando-se assim como a Lei Geral de Proteção de Dados (LGPD).

A sanção da lei 13.709/18, que altera a lei 12.965, de 2014 (o Marco Civil da Internet), estabelece a proteção e 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.

COMO FUNCIONA

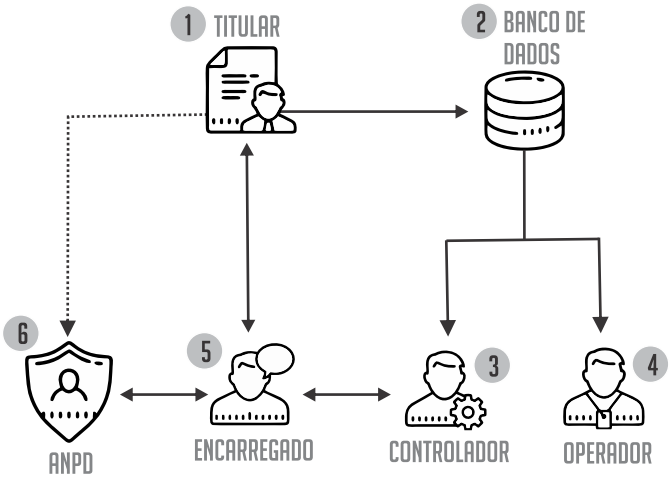
O PROCESSO DE TRATAMENTO DOS DADOS

O processo de tratamento da informação inicia-se com o **dado pessoal do titular** sendo armazenado em um **banco de dados**, estabelecido em um ou em vários locais, com suporte físico ou eletrônico. A partir deste momento, começa o trabalho dos agentes de tratamento: o **operador** que realiza o tratamento** dos dados pessoais em nome do **controlador** e este, a quem compete as decisões referentes a estes dados. Lembrando que, em algumas situações, não existe a figura do operador, neste caso, o próprio controlador realiza o tratamento dos dados.

Os agentes de tratamento, ou mesmo qualquer pessoa que intervenha em uma das fases do tratamento dos dados, obriga-se a **garantir a segurança da informação** em relação aos dados pessoais, **mesmo após o seu término**. Deve-se 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.

A **Autoridade Nacional de Proteção de Dados**, órgão responsável pela fiscalização, poderá receber, por exemplo, reclamações e comunicações diretamente dos titulares, a prestar esclarecimentos e adotar providências sobre seus dados. Por consequência, a autoridade deverá solicitar ao **Controlador,** por intermédio do **Encarregado**, um relatório de impacto à proteção de dados pessoais.

O **relatório de impacto à proteção de dados pessoais** deverá estar de acordo com o exigido na Lei, ou seja, deverá conter a descrição de todos os processos de tratamento de dados que possam gerar riscos às liberdades civis e aos direitos fundamentais.



LEGENDA: **Tratamento de Dados: Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

1. **TITULAR:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento**;
2. **BANCO DE DADOS:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
3. **CONTROLADOR:** Pessoa a quem competem as decisões referentes ao tratamento de dados pessoais;
4. **OPERADOR:** Pessoa que realiza o tratamento de dados pessoais em nome do controlador;
5. **ENCARREGADO:** Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;
6. **AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD):** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.

BLACKBULL network

+55 61 3234 0130
comercial@blackbullbrasil.com
blackbullbrasil.com

LGPD

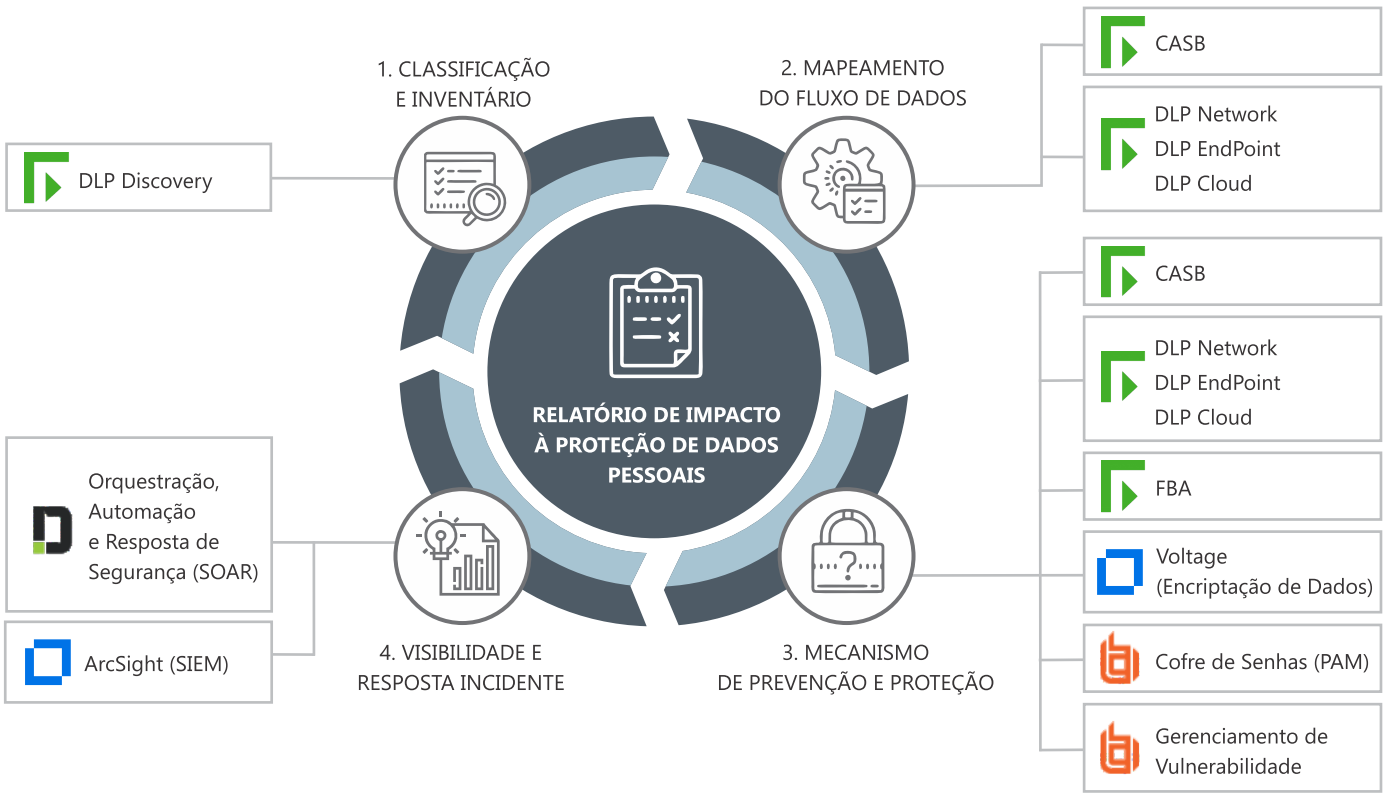
SIGILO E SEGURANÇA

Todos merecem ter sua privacidade respeitada.

Quando se trata de **sigilo e segurança de dados**, oferecemos todas as soluções a garantir que a organização fique adequada ao que exige a lei, no que se refere a **classificação, manipulação, armazenamento e transporte dos dados.**

NOSSO PORTFÓLIO

E AS EXIGÊNCIAS DO RELATÓRIO



FORCEPOINT

- DLP (Data Loss Prevention)
- CASB
- FBA

DLP (Data Loss Prevention)

Desde danos a reputações até multas e penalidades de agências reguladoras, uma violação de dados pode ter consequências devastadoras. **Forcepoint DLP** habilita você a descobrir e proteger dados confidenciais não importa onde estejam – em pontos de extremidade, na nuvem ou no local. Seus componentes podem ser implementadas juntas ou de forma independente para cumprir suas metas de segurança. Isso fornece flexibilidade para satisfazer as necessidades atuais e capacidade para crescer com a empresa.

DISCOVERY
Data at Rest

O Forcepoint DLP Discovery habilita você a localizar e proteger dados confidenciais na rede, e também os dados confidenciais armazenados em serviços na nuvem, como Microsoft Office 365 e Box. Com o acréscimo do Forcepoint DLP Endpoint, a potência do Forcepoint DLP Discovery pode ser ampliada para pontos de extremidade Mac OS X e Microsoft Windows dentro e fora da rede.

NETWORK
Data in Motion

A última chance para impedir o furto de dados é quando estão em movimento nos canais de Email e Web. Forcepoint DLP Network ajuda a identificar e impedir perda de dados maliciosa e acidental contra ataques externos ou da crescente Ameaça Interna. Técnicas contra evasão de ameaças avançadas com OCR potente para reconhecer dados em uma imagem. Use Drip DLP para impedir o furto de dados um registro de cada vez, e para monitoramento de comportamentos e anomalias para identificação de usuários de alto risco.

ENDPOINT
Data in Use

O Forcepoint DLP Endpoint estende OCR, 'Drip DLP' e outros controles contra perda de dados para os pontos de extremidade Mac OS X e Microsoft Windows, dentro e fora da rede. Forcepoint habilita o compartilhamento seguro de dados armazenados em dispositivos removíveis usando políticas para criptografia de arquivos. Monitoramento de uploads da web, incluindo HTTPS, e também uploads para serviços na nuvem, como Microsoft Office 365 e Box. Integração completa com Outlook, Notes e clientes de email, usando a mesma interface de usuário das soluções Forcepoint Data,Web, Email e Endpoint.

CLOUD
Data in Use, in Motion & at Rest

O Forcepoint DLP pode ser usado para monitorar e gerenciar fluxos de dados pessoais entre aplicativos em nuvem sancionados e não sancionados. Implantação em linha: quando implantado em linha (seja integrado com E-mail do Forcepoint ou gateways de segurança da Web, Forcepoint CASB ou qualquer outro provedor de gateway de terceiros), o Forcepoint DLP pode ser usado para proteger os dados pessoais através destes gateways (incluindo tráfego criptografado no caso dos gateways Forcepoint).

GDPR Cobertura total para GDPR em 28 países.

9X Líder no Quadrante Mágico.

CASB (Cloud Access Security Broker)

▶▶▶ VISIBILIDADE COMPLETA DE SHADOW IT

Identifique e classifique os aplicativos de nuvem para avaliar o risco e identificar quais serviços podem ser permitidos, monitorando com Forcepoint Cloud Access Security Broker (CASB).

▶▶▶ PREVINA CONTAS COMPROMETIDAS

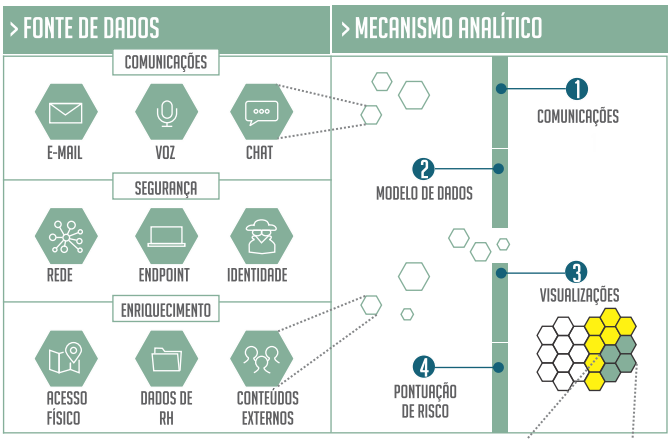
Impeça que invasores acessem dados de aplicativos de nuvem. Use os melhores recursos de aprendizado de máquina e FBA para definir impressões digitais comportamentais para cálculo avançado de riscos.

▶▶▶ PROTEJA O ACESSO MÓVEL A APLICATIVOS DE NUVEM

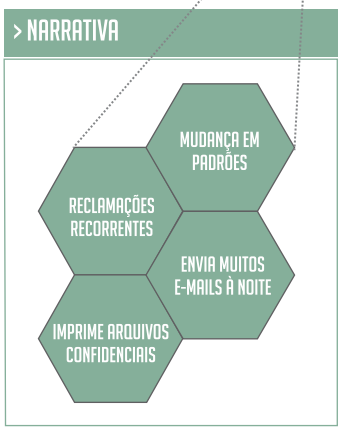
Aplique políticas exclusivas de acesso e segurança com base em dispositivos, diferenciando facilmente entre dispositivos gerenciados e não gerenciados (BYOD).

FBA

Forcepoint Behavior Analytics (FBA) habilita as equipes de segurança a monitorar proativamente comportamentos de alto risco dentro da empresa. Nossa plataforma de análises de segurança fornece contexto inigualável aos mesclar dados estruturados e não estruturados para identificar e impedir usuários maliciosos, comprometidos e negligentes. Nós descobrimos problemas críticos como contas comprometidas, espionagem corporativa, furto de propriedade intelectual e fraude.



1. Análise de Comunicações Especializadas - Conteúdo e meta.
2. Módulo de Dados Extensível para Todas as Fontes Estruturadas e Não Estruturadas.
3. Visualização de Análises Comportamentais.
4. Pontuação de Riscos de Entidades e Progressão ao Longo da Cadeia de Riscos Digitais.



BeyondTrust

- ✓ Cofre de Senhas (PAM)
- ✓ Gerenciamento de Vulnerabilidade

Cofre de Senhas (PAM)

DESCOBERTA AUTOMÁTICA CONTÍNUA — Faça a varredura, identifique e estabeleça o perfil de todos os ativos e aplicativos com integração automática de Contas privilegiadas.

MONITORE E AUDITE AS SESSÕES — Registre e monitore toda atividade e sessões de credenciais com privilégios para conformidade e análise da perícia forense.

GESTÃO E ALTERNÂNCIA — Armazene, gerencie e alterne senhas de contas com privilégios, eliminando credenciais integradas e garantindo a força das senhas.

PERTENCE AO QUADRANTE LÍDER DO GARTNER

BeyondTrust foi indicada como líder em Gestão de Acesso com Privilégios (PAM) no Magic Quadrant.

Gerenciamento de Vulnerabilidade

IDENTIFIQUE — Faça a varredura, identifique e avalie vulnerabilidades em todos os ativos (nas instalações, na nuvem, móvel, virtual, recipiente) dentro da organização.

RETIFIQUE — Retifique e emita relatório sobre vários padrões e comparativos normativos federais e específicos do setor.

PRIORIZE — Priorize vulnerabilidades analisando o impacto nos negócios e utilizando contexto adicional a partir de várias origens de terceiros.

THE FORRESTER WAVE™: VULNERABILITY RISK MANAGEMENT, 2018

A BeyondTrust é nomeada líder no relatório Forrester Wave 2018 para gestão de risco de vulnerabilidades.

MICRO FOCUS®

- ✓ Voltage (Encriptação de Dados)
- ✓ ArcSight (SIEM)

Voltage (Encriptação de Dados)

	SST	FPE		
	CREDIT CARD 1234 5678 8765 4321	SSN/ID 934-72-2356	E-MAIL BOB@VOLTAGE.COM	DATE OF BIRTH 31-07-1966
FULL	8736 5533 4678 9453	347-98-8309	HRV@GHOHAWD.JIW	20-05-1972
PARTIAL	1234 5681 5310 4321	634-34-2356	HRV@GHOHAWD.JIW	20-05-1972

CAMPO DE NÍVEL, PRESERVAÇÃO DO FORMATO DE ENCRIPTAÇÃO, DADO DE IDENTIFICAÇÃO REVERSÍVEL

A **Micro Focus** é líder e especialista em criptografia de dados e soluções de **pseudonimização**, **tokenização** e **mascaramento** para privacidade de dados corporativos e conformidade normativa. Em vários setores – desde determinações ligadas à conformidade, como PCI e GDPR, a novas iniciativas de TI, como analítica de dados e migração para a nuvem – as empresas contam com o Voltage SecureData para proteger as informações em seu núcleo, tanto em repouso quanto em movimento e em uso, para uma proteção abrangente, sem lacunas.

ArcSight (SIEM)

CORRELAÇÃO DE DADOS EFICIENTE EM TEMPO REAL

Colete dados e correlacione eventos em tempo real — até 75.000 eventos por segundo — para encaminhar ao nível hierárquico superior as ameaças que violam as regras internas da plataforma.

AUTOMAÇÃO DE FLUXOS DE TRABALHO, ORQUESTRAÇÃO DA SEGURANÇA

Capacite as suas equipes de monitoramento de SOC a fazer, com eficiência e eficácia, a triagem dos alertas detectados usando o ArcSight Command Center (ACC).

COMMUNITY-DRIVEN SECURITY CONTENT

Beneficie-se de conjuntos de regras de segurança, painéis e relatórios desenvolvidos por especialistas de SOC da MicroFocus e Comunidade. O ArcSight Activate inclui centenas de soluções de casos de uso e pacotes ESM para resolver seus requisitos de segurança de gerenciamento de eventos de informações.

MATRIZ DE PERMISSÕES UNIFICADA E COM MULTILOCAÇÃO

Utilize os recursos de gerenciamento centralizado, incluindo limites baseados em regras e uma matriz unificada de funções, permissões, direitos e responsabilidades.

COMPATÍVEL COM ARCSIGHT DATA PLATFORM E ARCSIGHT INVESTIGATE

Detecte melhor as ameaças desconhecidas à segurança com um pacote abrangente de coleta de dados, correlação de eventos eficiente e em tempo real e investigação intuitiva com arquitetura aberta.

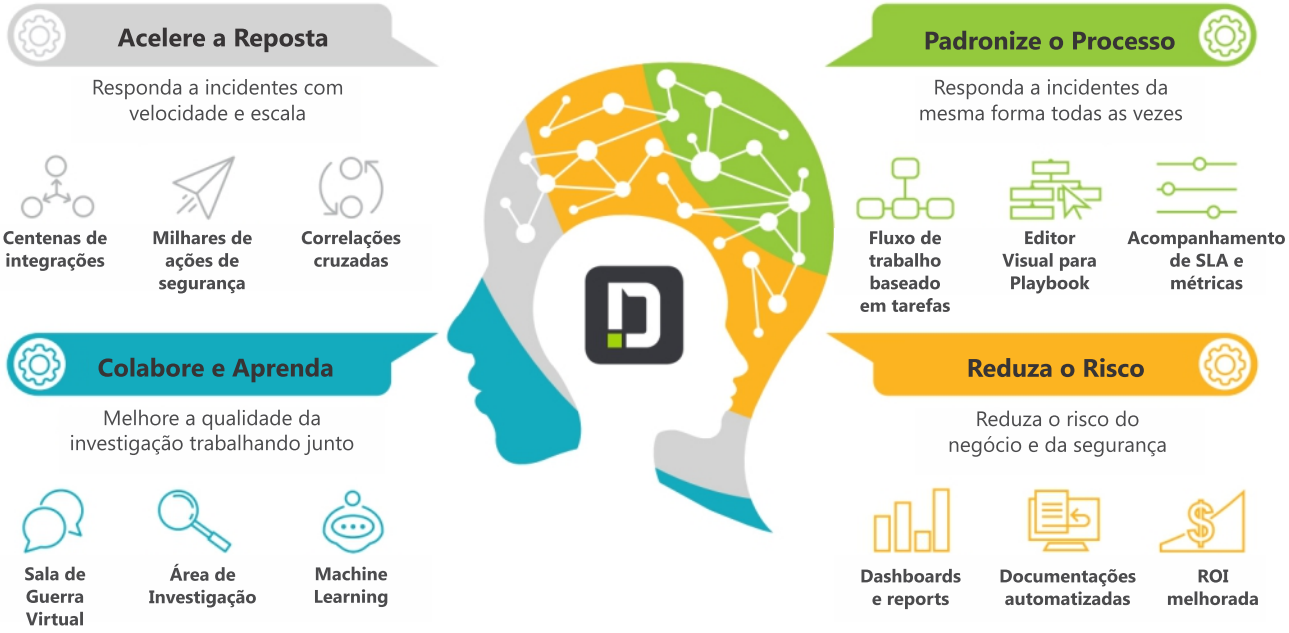
DADOS DE EVENTOS DE SEGURANÇA ENRIQUECIDOS

Melhore e enriqueça suas variáveis e informações de eventos para mais de 400 pontos de dados individuais e específicos.

DEMISTO

✓ Orquestração, Automação e Resposta de Segurança (SOAR)

Orquestração, Automação e Resposta de Segurança (SOAR)



O Demisto Enterprise é uma abrangente plataforma de **Orquestração de Segurança, Automação e Resposta (SOAR)** que combina gerenciamento completo de casos, automação inteligente e colaboração em tempo real para atender às equipes de segurança em todo o ciclo de vida do incidente.

O Demisto ingere alertas agregados de fontes de detecção (como SIEMs, ferramentas de segurança de rede e caixas de correio) antes de executar playbooks automatizados e orientados a processos para enriquecer e responder a esses alertas. Esses manuais se coordenam entre tecnologias, equipes de segurança e usuários externos para visibilidade e ação de dados centralizados.

BLACKBULL network

+55 61 3234 0130
comercial@blackbullbrasil.com
blackbullbrasil.com