LGPD
Lei Geral de Proteção de Dados

H2H HUMAN TO HUMAN

21 DE SETEMBRO

+55 11 9.5214-4909 tel. (corporativo - WhatsApp) – www.bemav.com.br – contato@bemav.com.br

LGPD

Encontrar, proteger, controlar, autorizar e auditar

LGPD é uma realidade, já está em vigor e as áreas de TI/SI tem o desafio de entrar, proteger, controlar e auditar os dados sensíveis.

A visão de soluções da be.MAV para LGPD é:

- **Encontrar** – definido pela organização quais são os campos sensíveis, é hora de localizá-los dentro do ambiente tecnológico, se estão em banco de dados, arquivos, pastas, planilhas, e-mail etc. (IONATE e IRI)

- **Proteger** – ao detectar onde esses dados estão, é o momento de criptografá-los, protegendo da visão de pessoas não autorizadas. (IRI)

- **Controlar** – através de integração da criptografia com os sistemas de gestão de acesso, permitir somente a quem está autorizado ver a informação. (IRI)

- **Auditar** – após a implantação da estrutura para suportar a LGPD, é hora de ter um sistema que irá monitorar todos os acessos aos dados e montar relatórios eliminando possíveis punições por quebra da lei. (IONATE e IRI)

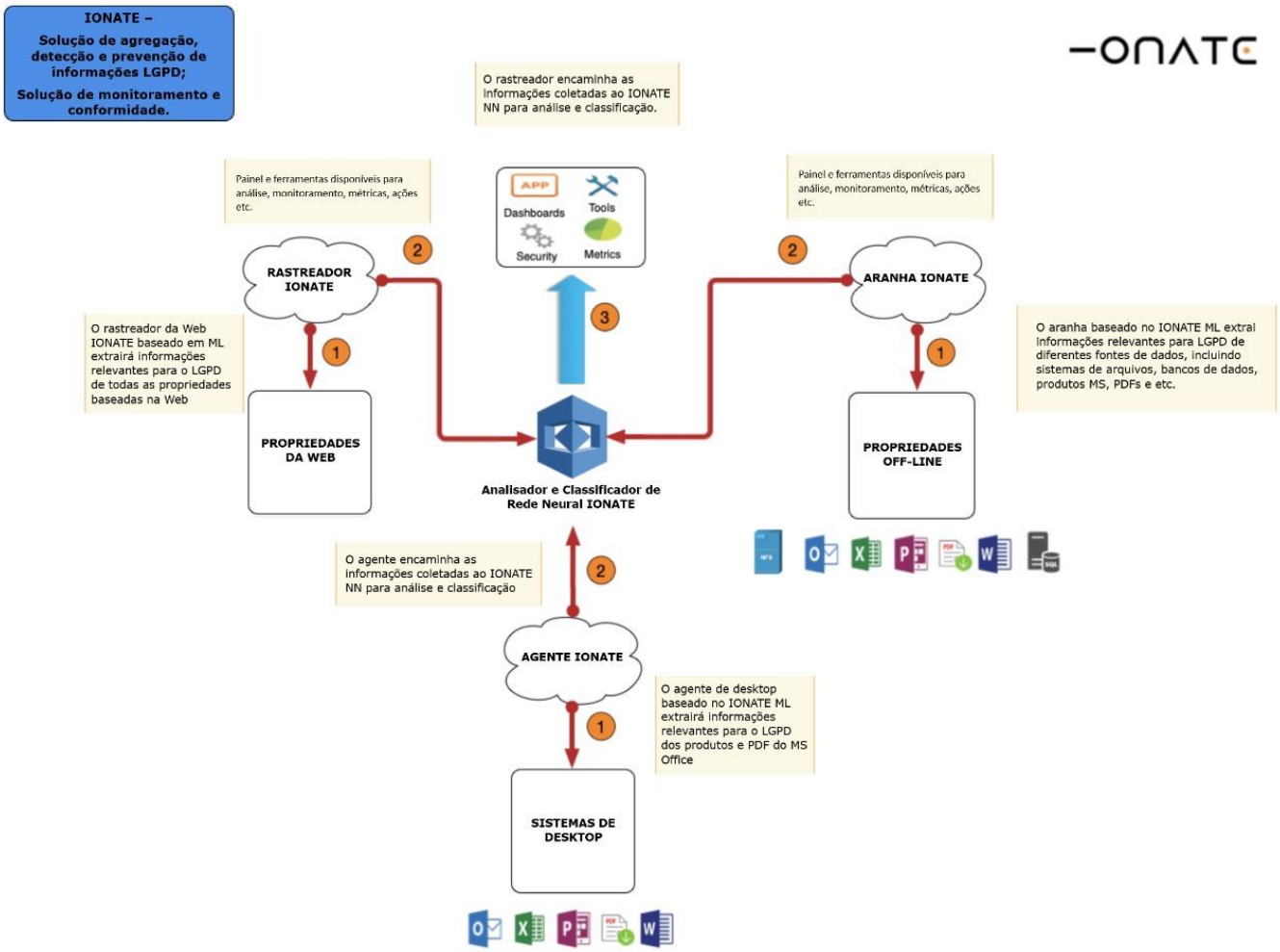
- **Consultoria de controle de acesso** – um dos principais problemas hoje é a não existência de uma estrutura de controle de acesso ou mesmo algo desatualizado permitindo que pessoas não autorizadas acessem os dados sensíveis, para isso temos a nossa equipe que poderá atuar na montagem do perfil das funções entrevistando gestores, integrando com RH e TI/SI.

+55 11 9.5214-4909 tel. (corporativo - WhatsApp) – www.bemav.com.br – contato@bemav.com.br

Visão da Ionate – localizar e auditar os dados sensíveis

Quando falamos da nossa parceira com a Ionate, o nosso foco está em localizar e auditar os dados sensíveis que foram elencados, a solução tem como base “olhar” o ambiente e prover relatórios, dashboards e alertas.

Através de agentes a solução da Ionate encontra e audita as atividades feitas com os dados sensíveis, é ideal para quando estamos fazendo o reconhecimento da nossa base de TI e no pós, para o acompanhamento de como os dados estão sendo usados.



A Ionate foi fundada em 2016, San Francisco, California, através do Programade Startup da MIT– Membro desde 2016, seu fundador, Ajanta Adhikari - Founder, CEO e Presidente, é Veterano da indústria de Cloud, Big Data e Infraestrutura de identidade, com uma década de experiência como arquiteto da Akamai e vencedor do prêmio Denny Lewin, ajudou a Aspera, uma empresa do grupo IBM, e outras com desafios de crescimento e escalabilidade. Em 2018 a Ionate foi listada entre as 50 melhores startups dentre um total de 2800 no vale do silício.

Visão IRI - Localizar, proteger, autorizar e auditar dados sensíveis

"A IRI já vem atuando nos EUA, Europa e Ásia protegendo dados conforme a legislação local."

Na última edição do CyberSecurity Sourcebook, a IRI definiu o termo 'Startpoint Security' para abranger nove conceitos de segurança centrados em dados:

1. **Permissão e divulgação** - autorizando você a armazenar informações sensíveis enviadas por acordo do usuário
2. **Descoberta e classificação** - localizando e catalogando as informações sensíveis para encontrar e mascará-lo de forma consistente
3. **Mascaramento de dados** – proteção dos dados sensíveis por meio de criptografia, redação, pseudonimização etc.
4. **IAM e RBAC** - gerenciamento de autorização de acesso, (des) mascaramento de trabalhos, programas e logs
5. **Dados e metadados Linhagem** - salvando e analisando alterações nos dados e trabalhos de mascaramento
6. **Latência** - arquitetando, configurando e executando trabalhos de mascaramento de dados estáticos ou dinâmicos
7. **Pontuação de Risco** - medindo a probabilidade estatística de re-identificação (por exemplo, para HIPAA & FERPA)
8. **Auditoria Registros** - vendo ou consultando quem fez o que e quem viu o que, quando e onde
9. **Avaliação e seguro** - conduzindo análises processuais, estatísticas e legais de especialistas

Essas atividades podem complementar e ser realizadas, usados em conjunto com abordagens de segurança de endpoint para proteger alvos de dados vulneráveis contra hackers, ameaças internas ou violações e cumprir as leis de privacidade de dados dos EUA e internacionais, LGPD.

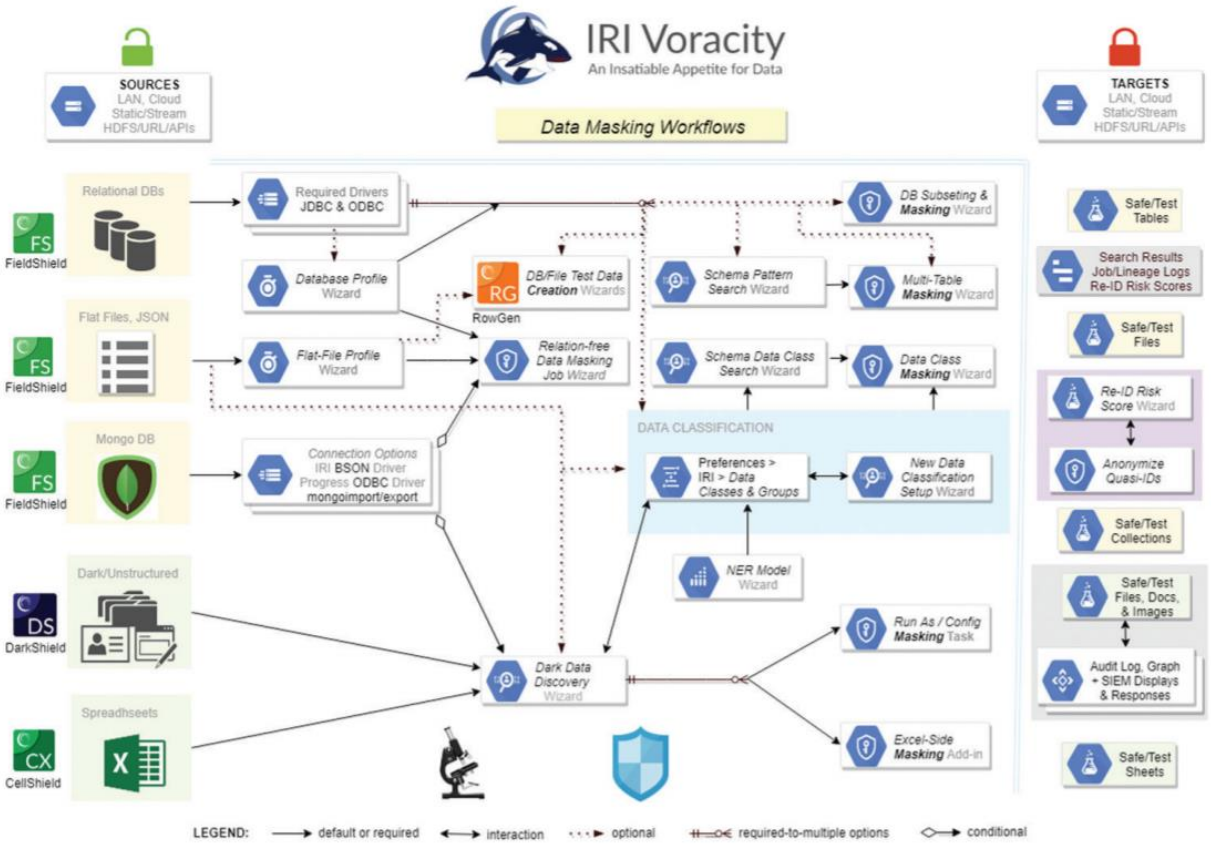
Atualmente, o IRI oferece três produtos de busca e mascaramento dos dados e que atendem a grande parte desses requisitos com base nas fontes de dados envolvidas:

- **FieldShield** - Mascaramento de dados estruturados, o FieldShield classifica, localiza de-identifica, pontuações de risco e audita PII em bancos de dados, arquivos simples, JSON etc.

- **CellShield EE** - Mascaramento de dados do Excel®, o CellShield localiza, relata, máscara e audita alterações nas informações sensíveis nas colunas do Excel e valoriza toda a LAN

- **DarkShield** - Mascaramento de dados não estruturados, o DarkShield classifica, localiza e exclui dados sensíveis em texto, pdf, documentos MS, logs e arquivos de imagem, além de faces.

IRI DMaaS - Mascaramento de dados como serviço, os engenheiros da IRI DMaaS nos EUA e no exterior fazem o trabalho de classificar, encontrar e desidentificar as informações sensíveis para você.



O esquema acima ilustra o fluxo típico de atividade desses produtos e serve como um modelo de instruções para o design e a implementação da solução.

Esses produtos também pertencem ao pacote IRI Data Protector e estão incluídos componentes da plataforma de gerenciamento de dados IRI Voracity.

Fundada em 1978, a IRI é um fornecedor independente de software (ISV), especializado em gerenciamento rápido de dados e proteção centrada em dados. A tecnologia principal da empresa e as interfaces comuns de usuário permitem executar, combinar e acelerar grandes volumes de dados: extração, transformação, carregamento, limpeza, migração, replicação, federação, mascaramento, relatórios, preparação de dados analíticos e geração de dados de teste.

Visão be.MAV na LGPD

Ao escolher a IRI e Ionate, a be.MAV estruturou uma linha de soluções que considera ideal para as áreas de TI/SI.

As ferramentas poderão ser usadas em separado ou combinadas de forma a atender as efetivas necessidades dos nossos clientes.

Outras áreas de atuação:

- Serviços, desenvolvimento e consultoria especializada
- Inovação tecnológica, redução dos custos de infraestrutura, melhoria de performance e segurança
- IoT - Internet das coisas
- Segurança da Informação
- LGPD encontrar, proteger, controlar, autorizar e auditar
- Prevenção a desvios, perdas e fraudes
- Gestão de Telecom
- Transformação digital na comunicação e atendimento
- Blockchain como serviços (BaaS)
- Captura de transações (rede de adquirência)

Quem é a be.MAV

A empresa nasceu no ano de 2014 com o objetivo inicial de atuar na representação e consultoria para prevenção a desvios, perdas e fraudes e na área da segurança da informação. A oferta de soluções teve crescimento à medida que outros fornecedores, que acreditam na nossa forma de trabalho, nos procuraram.

Nossa filosofia é ter somente parceiros especialistas em suas áreas e comprometidos com os nossos clientes, parceiros com quem podemos atuar diretamente influenciando na qualidade da entrega.

Marco A. Vidal – CEO – Linkedin: marcovidal - www.bemav.com.br

Quem representamos