

EY Webinar

A importância do uso de tecnologia na jornada adequação LGPD


EY
Building a better
working world

 **Microsoft**

Agenda



Marcos Semola
Partner - Líder Data
Privacy LAS



Viviane Oliveira
Partner



Rodrigo Monteiro
GBB Data & AI



Viviane Oliveira

Partner Cybersecurity



Aliança Microsoft & EY

Visando **impulsar** essa expansão sobre as demandas de privacidade, a EY tem buscado parcerias e alianças que possam impactar e otimizar seus serviços, oferecendo soluções que podem ser utilizadas para obter maior **valor agregado ao negócio** e maximizar tanto a **governança de dados** quanto sua **infraestrutura de privacidade e proteção de dados pessoais**.

E dentro desta busca, identificamos que a **Microsoft** possui soluções que podem ser utilizadas dentro deste contexto de privacidade, de modo a aprimorar a estratégia utilizada pela EY de forma tecnológica impactando diretamente sobre nossos serviços e clientes.



EY and Microsoft expand strategic relationship

Carmine Di Sibio, EY Global Chairman & CEO, and Satya Nadella, Microsoft CEO, announce expansion driving US\$15bil growth opportunity. Increased collaboration focuses on new solutions and platforms for digital transformation.

O que a LGPD impõe às empresas

LGPD

A Lei Geral de Proteção de Dados, que entrou em vigor em 18 de Setembro de 2020, regulamenta o tratamento, a privacidade e a proteção dos dados pessoais com o intuito de impor limites que respeitem a intimidade da vida privada. Controladores de dados - que determinam o propósito e os meios de tratamento de dados pessoais - e Operadores, que tratam esses dados em nome dos Controladores, serão afetados pelo requerimentos da nova lei.

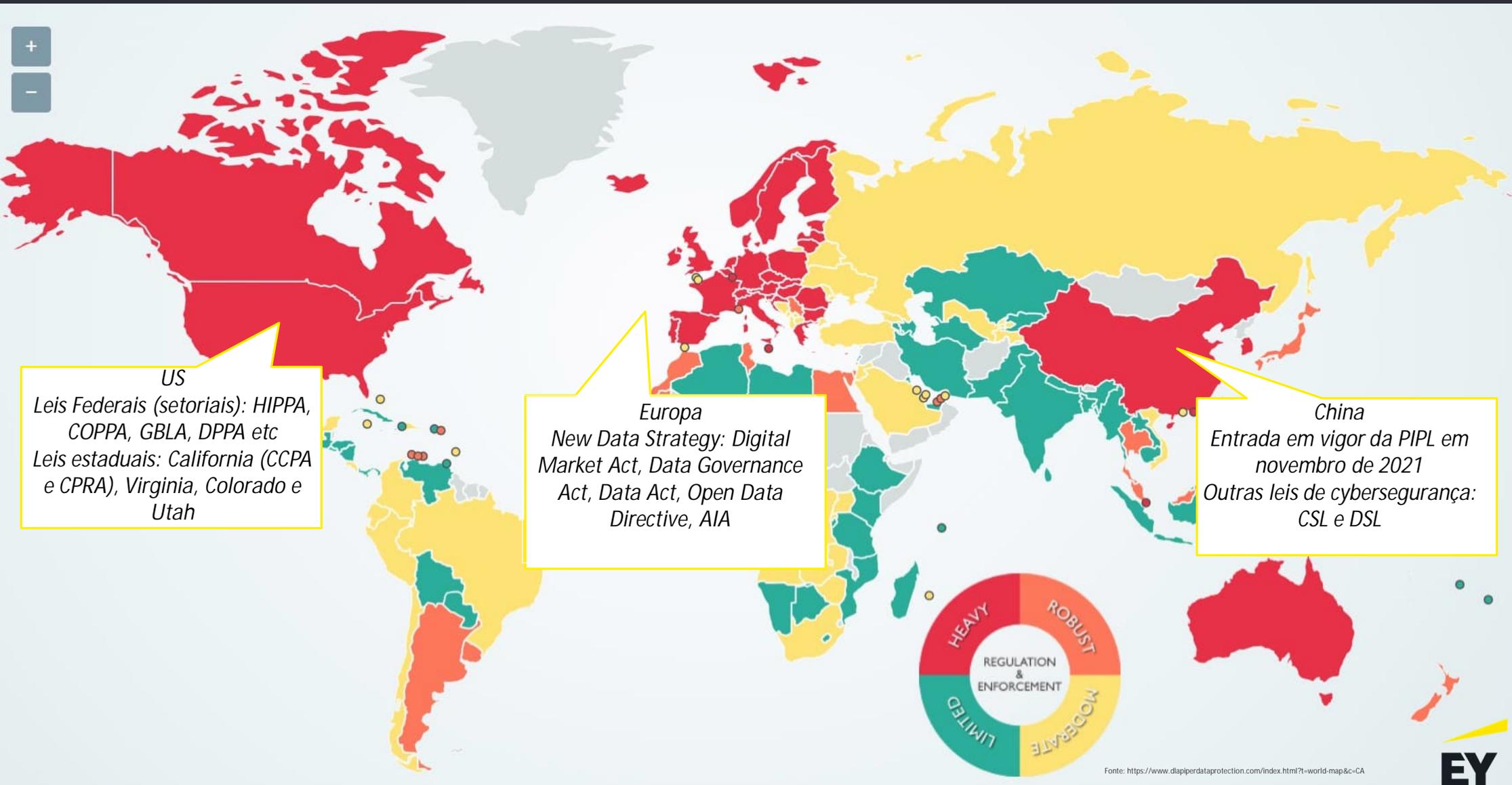
Penalidades

As penalidades se iniciam com simples advertências, bloqueio de dados e podem chegar ao limite de até 2% da receita anual da empresa, até o teto de R\$50 milhões por evento de infração.

Quem é impactado

Organizações que oferecem bens ou serviços ou que monitoram o comportamento de indivíduos naturais, bem como empresas que tratam ou mantêm sob custódia dados pessoais de indivíduos naturais do Brasil.





O estado atual de privacidade

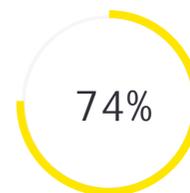
Em 2019, elaboramos em parceria com a Associação Brasileira de Empresas de Software (ABES) uma autoavaliação de conformidade com a LGPD composta por 70 perguntas que cobrem aspectos jurídico-regulatórios, tecnológicos e de governança, capaz de produzir uma qualificação percentual de aderência acompanhada de um plano estratégico de adequação. Este projeto se tornou uma referência nacional para o acompanhamento da maturidade de conformidade do mercado brasileiro. (<https://diagnosticolgpd.abes.org.br/>)

Self-assessment
de Conformidade
LGPD

Fonte: ABES



Dos respondentes sofreram incidentes de violação nos últimos 2 anos.



Dos respondentes realizam a coleta de dados pessoais considerados sensíveis

* ABES (Associação Brasileira de Empresas de Software)

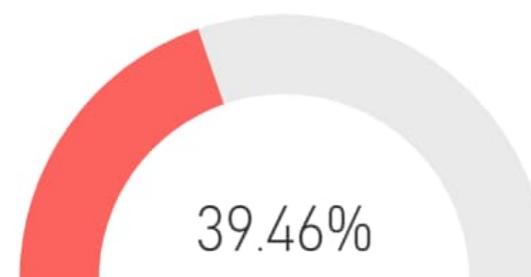
O último relatório da Autoavaliação LGPD ABES/EY realizado por mais de 31.116 empresas apresenta baixo nível geral de maturidade, reflexo da confusão conceitual sobre a multidisciplinaridade do tema e a necessidade de uma abordagem modular e gradual amparada por boas práticas de gestão de riscos que considere controles, prioridades e legítimos limites corporativos.



LEI GERAL DE PROTEÇÃO DE DADOS

●	PROCESSOS	36.15%
●	PESSOAS	35.35%
●	TECNOLOGIA	40.06%

MÉDIA GERAL DE IMPLEMENTAÇÃO DOS REQUISITOS DA LGPD



39.46% dos requisitos da LGPD são atendidos pelas empresas respondentes

acesso em 07/2021

Outros direcionadores de negócio...

Impacto dos incidentes de perda de dados:

- Multas
- Danos à reputação
- Perda de confiança do investidor
- Perda direta de negócios
- Ação legal
- Impacto negativo na retenção e recrutamento de funcionários



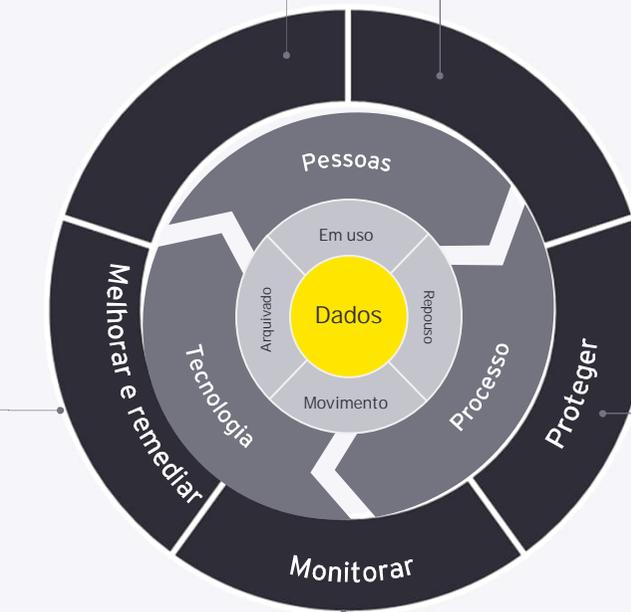
Sua jornada de proteção

Entender quais são os dados de maior criticidade, incluindo os dados pessoais, e pessoais sensíveis

Classificar todos os dados à medida que são criados, usando rótulos claros e significativos. classifique os sistemas com base nos dados que armazena e processa.

Revisar e aprimorar o programa de proteção de dados continuamente para acompanhar as ameaças emergentes.

Proteger todos os dados baseados em controles definidos em um esquema de classificação.



Monitorar o ambiente por meio do uso de tecnologias

Issues comuns

Nessa jornada de Privacidade, alguns controles somente são endereçados de forma efetiva, por meio de tecnologia.



Qual a precisão do meu inventário de dados pessoais? Todas as bases de dados estão mapeadas?



Como certificar que não tenho eventos de vazamento de dados em andamento?



Será que algum funcionário descontente pode estar manipulando dados pessoais de forma indevida?



Como assegurar que as informações estão sendo adequadamente manipuladas, se elas não estão rotuladas?



Os meus controles de LGPD continuam sendo atendidos? Os controles automatizados podem ser verificados de uma forma mais efetiva?

Cobertura das soluções

Inventário de Dados (Data discovery)	Vazamento de informações	Análise comportamental	Classificação das Informações	Monitoramento controles
				
				
Azure Purview Microsoft Information Protection	Data Loss Prevention	Insider Risk Management	Azure Information Protection	Compliance Manager
<ul style="list-style-type: none">Ferramenta de governança de dados unificada que permite o gerenciamento e controle dados locais, multivem e SaaS (software como serviço), e o inventário de informações.	<ul style="list-style-type: none">Ferramenta responsável pela proteção de informações consideradas confidenciais pela organização impedindo divulgação indevida.	<ul style="list-style-type: none">O insider risk management ajuda a detectar, investigar e tomar medidas para mitigar riscos internos em sua organização a partir de cenários, incluindo roubo de dados por funcionários, vazamento intencional ou não de informações confidenciais e comportamento ofensivo.	<ul style="list-style-type: none">Ferramenta utilizada para restrição e bloqueio no compartilhamento externos de documentos classificados por sensibilidade(ex.: Dados sensíveis para a organização).	<ul style="list-style-type: none">Ferramenta que realiza a avaliação do seu ambiente em nuvem do Microsoft 365 e Azure através de requisitos de conformidade de diversas regulamentações globais

Framework Data Protection...

Data Governance

Policies & standards

Identification

Risk assessment

Classification

Architecture

Quality

Data protection controls

Focus areas

Data in motion

Perimeter security

Network traffic monitoring/blocking

Web content filtering

Data collection and exchange

Messaging (Email, IM)

Remote access

Structured data

Data in use

Privileged user monitoring

Workstation restrictions

Application controls

Data labelling/tagging

Removable/external media control

Export/clipboard/print control

Data at rest

Encryption

Obfuscation/tokenization

Mobile device protection

Network/server repository control

Physical media control

Data archiving/disposal

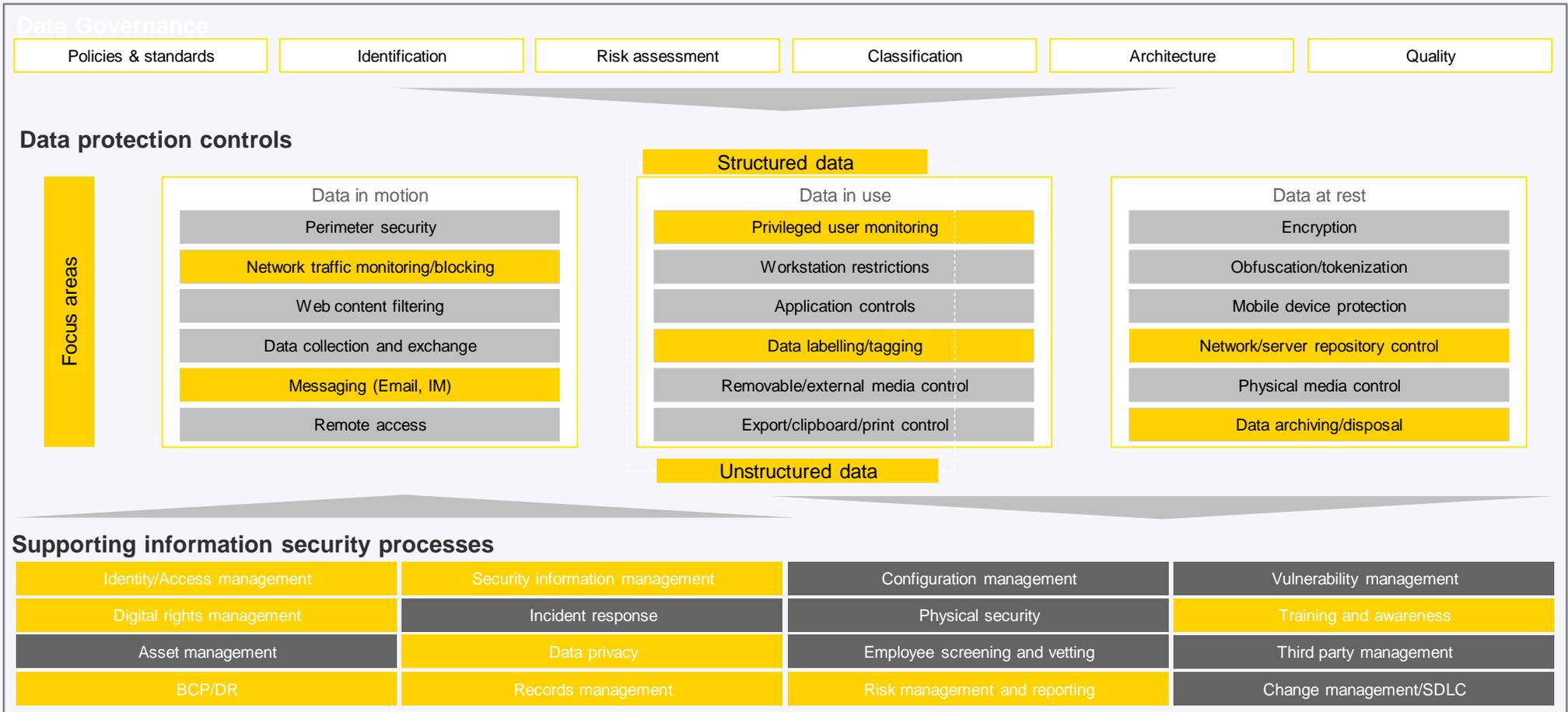
Unstructured data

Supporting information security processes

Identity/Access management	Security information management	Configuration management	Vulnerability management
Digital rights management	Incident response	Physical security	Training and awareness
Asset management	Data privacy	Employee screening and vetting	Third party management
BCP/DR	Records management	Risk management and reporting	Change management/SDLC



...e a cobertura dos controles pelas tecnologias

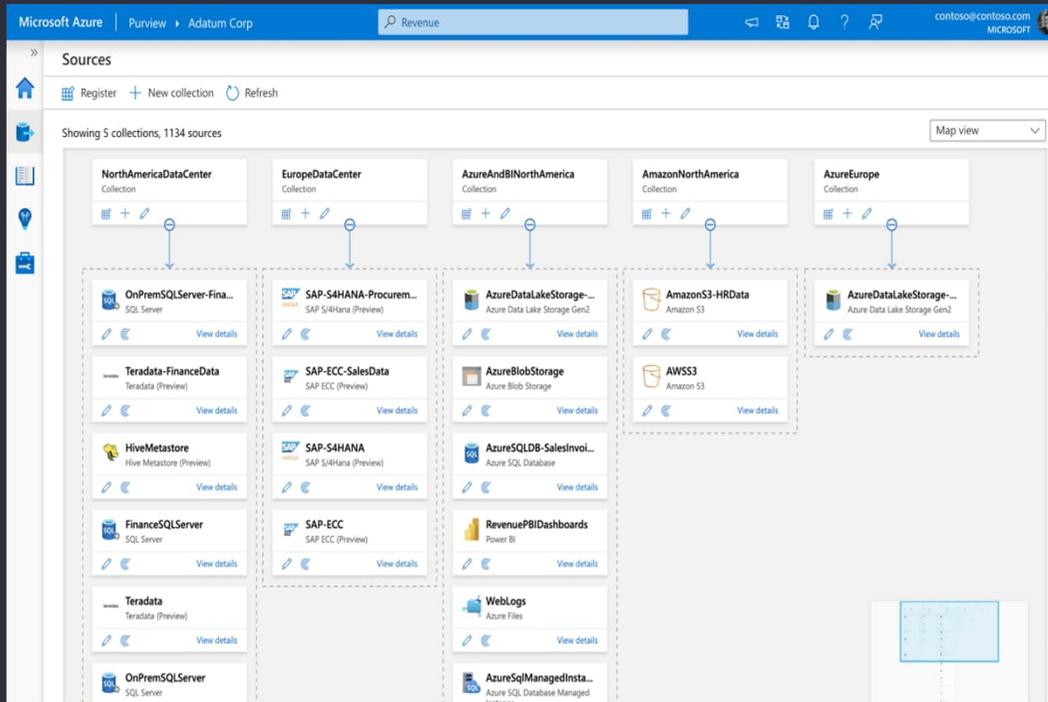


Azure Purview



Ferramenta de governança de dados unificada que permite o gerenciamento e controle dados locais, multinuvem e SaaS (software como serviço).

Permite criação de **mapas holísticos** que permitem a visibilidade do cenário atual dos dados pessoais;



Permite:

- Criar **rótulos de dados** (ex.: público, interno, confidencial etc.) que serão utilizados pelo Purview para identificar dados dentro do ambiente;
- Realizar **pesquisas** dentro de cenários híbridos (on-premises e em nuvem);
- Obter **insights** sobre locais e movimentações de dados confidenciais.
- Integração com o Microsoft 365 e Information Protection

- Exemplos de bases
- SQL Server
 - Sharepoint Online
 - Azure
 - Microsoft 365
 - Power BI
 - AWS
 - Oracle
 - SAP



Rodrigo Monteiro

GBB Data & Analytics

Um resumo da nossa jornada

Passado, presente e futuro

A estratégia de proteção deve contemplar os diversos momentos e "estados" dos dados

Tendências e Inovações

A adoção de novas formas de negócio, demanda outros mecanismos de proteção

Pessoas: elo fundamental

Ampliar a conscientização dos colaboradores e partes envolvidas é essencial nessa jornada.

Regulamentação

Estar atento as alterações nas legislações.

O volume de dados que precisam ser protegidos é cada vez maior. É preciso uma abordagem integrada e compromisso de todas as partes para assegurar a proteção dos dados.

Obrigado (a) !

