OOZONE

INTELIGÊNCIA DIGITAL

nDex

LEI GERAL DE PROTEÇÃO DE DADOS

e-Book

PREÂMBULO

- A Lei 13.709/2018
- 3 Domínios: Técnico, Jurídico, Processos
- Gestão de dados
- Gestão de Segurança da Informação
- Anonimização de dados
- Eliminação de dados

- Checkup de Segurança da Informação
- Definição do ENCARREGADO de dados
- Solicitações e eventos de Crise
- Sanções
- PARCEIROS de confiança

OOZONE
INTELIGÊNCIA DIGITAL

A LEI 13.709/2018 - APLICAÇÃO

Aplica-se a quem ?
A **qualquer pessoa** natural ou jurídica de direito público ou privado que realize tratamento de dados pessoais;

O são dados pessoais ?
Qualquer informação que possibilite identificar uma pessoa de maneira direta ou indireta,
por exemplo nome, CPF, endereço, dados de GPS, Cookies, etc

Na prática
É abrangente alcançando todas as atividades B2B e B2C de maneira transversal

OOZONE
INTELIGÊNCIA DIGITAL

A LEI 13.709/2018 – DEFINIÇÕES

Art. 5º Para os fins desta Lei, **considera-se**:

I. **dado pessoal**: informação relacionada a pessoa natural identificada ou identificável;

II. **dado pessoal sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, etc, qualquer dado quando vinculado a uma pessoa natural;

III. **dado anonimizado**: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV. **banco de dados**: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V. **titular**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI. **controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII. **operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII. **encarregado**: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

IX. **agentes de tratamento**: o controlador e o operador;

X. **tratamento**: toda operação realizada com dados pessoais, quaisquer verbos;

A LEI 13.709/2018 – DEFINIÇÕES (continuação)

Art. 5º Para os fins desta Lei, **considera-se**:

XI. **anonimização**: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII. **consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII. **bloqueio**: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV. **eliminação**: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV. **transferência internacional de dados**: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI. **uso compartilhado de dados**: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII. **relatório de impacto à proteção de dados pessoais**: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVIII. **órgão de pesquisa**: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

XIX. **autoridade nacional**: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

OOZONE
INTELIGÊNCIA DIGITAL

A LEI 13.709/2018 – BASES LEGAIS

Art. 7º O **tratamento de dados pessoais somente poderá ser realizado** nas seguintes hipóteses (ao menos uma):

I. Consentimento;
II. Cumprimento de obrigação legal;
III. Execução de politicas publicas;
IV. Estudos de órgãos de pesquisa
V. Execução de contratos;
VI. Exercício regular de direitos;
VII. Prevenção da vida;
VIII. Tutela de saúde;
IX. Interesses legítimos do controlador
X. Proteção ao crédito;

OOZONE
INTELIGÊNCIA DIGITAL

A LEI 13.709/2018 – DIREITOS DO TITULAR

Art. 18. **O titular dos dados pessoais tem direito** a obter do controlador, a qualquer momento e mediante requisição:

I. Confirmação da existência de tratamento;

II. Acesso aos dados;

III. Correção de dados incompletos ou desatualizados;

IV. Anonimização, bloqueio ou eliminação de dados desnecessários;

V. Portabilidade dos dados a outro fornecedor de serviço ou produto;

VI. Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII. Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX. Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei;

OOZONE
INTELIGÊNCIA DIGITAL

3 DOMÍNIOS

Na jornada da conformidade com a nova legislação, sua empresa terá que se adequar em 3 âmbitos, **JURÍDICO**, **PROCESSOS** e **TÉCNICO**.

Este é um tema que não envolve algumas áreas e sim a **ORGANIZAÇÃO** como um todo, inclusive TERCEIROS e PARCEIROS de negócios.

Estabeleça um grupo de trabalho **MULTIDISCIPLINAR**, capaz de cobrir as três frentes:

Criação de novas políticas de privacidade, novos contratos e acordos entre empresa e usuário (que precisa dar o seu consentimento para o uso dos dados).

Revisão de responsabilidades, determinação de quem pode ter acesso a quais dados, levantamento de quais as empresas tercerizadas estão envolvidas no tratamento dos dados, quem será o responsável legal pelos dados dentro da empresa etc.

Análise de quais são os dados pessoais e onde estão eles armazenados, como tratá-los e armazená-los com segurança, quais as soluções existentes no mercado que podem ajudar na gestão, proteção, etc.

OOZONE
INTELIGÊNCIA DIGITAL

GESTÃO DE DADOS

O primeiro passo é identificar quais são os dados pessoais e onde estão armazenados. Normalmente, estão dispersos em diferentes plataformas e será preciso unificar ou gerenciar tudo em um único local, de forma a facilitar o controle de acesso e a segurança destas informações.

Analise os dados não estruturados (documentos, planilhas, e-mails, imagens, etc) e também os dados estruturados bancos de dados relacionais ou não.

Através de uma interface única permitindo que os metadados coletados fiquem acessíveis para que os profissionais autorizados de planejamento, *Analytics* e de *Data Science* obtenham informações e *insights* relevantes para a tomada de decisões e, ao mesmo tempo, estejam de acordo com os requisitos de governança corporativa.

nDex
Data Discovery

Avalia o conteúdo e a estrutura dos dados para consistência e qualidade. O **nDex** usa **algoritmos avançados de Machine Learning & IA** para ajudar a identificar colunas com dados pessoais, outras informações confidenciais e elementos de dados críticos que podem fazer parte de uma estratégia de proteção de dados escopo **LGPD**. Ajudando a melhorar a precisão dos dados sugerindo inferências e identificando anomalias.

nDex
Data Monitoring

O nDex aprimora a capacidade das empresas de criar e manter um **programa forte de governança** e de **gestão de dados**, capaz de transformar dados em informações confiáveis. Permite explorar, compreender e analisar informações e estabelecendo regras de governança e *compliance*. Você pode criar, gerenciar e compartilhar uma linguagem de negócios comum, documentar e aprovar políticas, regras e rastrear a linhagem de dados.

nDex
Insights

Avaliar dados não estruturados de forma profunda, permite encontrar e classificar dados pessoais, gerenciar registros, otimizar o armazenamento e as iniciativas de migração de dados.

OOZONE
INTELIGÊNCIA DIGITAL

GESTÃO DE SEGURANÇA DA INFORMAÇÃO

- ✓ O “EU” não existe em se tratando de Segurança da Informação !
- ✓ Acredite, não existe uma área responsável por Segurança da Informação, TODOS são agentes ativos deste desafio.
- ✓ Faça um levantamento dos usuários e terceirizados e suas respectivas responsabilidades, identificando quem realmente precisa ter acesso aos dados pessoais, considerando a boa prática de Menor Privilégio.
- ✓ Uma plataforma integrada possibilita definir, integrar, proteger e gerenciar informações confiáveis entre sistemas. Assegurando o acesso a dados confidenciais, não estruturados (documentos, imagens, e-mais, etc) ou em bancos de dados relacionais ou não, criando controles de segurança e evitando que estes dados sejam utilizados para outros fins.
- ✓ Além de examinarmos os maiores obstáculos enfrentados pelos profissionais de segurança, temos a obrigação de tornar a comunidade de colaboradores mais consciente sobre a cultura de Segurança da Informação.
- ✓ Converter as "ações" de Segurança da Informação em ações simples e acessíveis à todos os envolvidos, ajudará a garantir a implantação da cultura de segurança dentro da organização.
- ✓ Processos muito complexos tornam-se decadentes e ineficazes !

OOZONE
INTELIGÊNCIA DIGITAL

ANONIMIZAÇÃO DE DADOS

Você vai ouvir muito esse termo: **anonimizar**, ou seja, tornar possível usar dados de forma anônima. Isso permite fazer testes e estudos de comportamento de consumo, por exemplo, usando dados reais, sem que sejam identificadas as pessoas relacionadas a estes dados.

Números de cartões de crédito, endereços, etc podem ser mascarados, porém o significado contextual é mantido. Existem uma variedade de técnicas de transformação que substitui os dados reais confidencias por dados fictícios, permanecendo contextualmente precisos e uteis.

Assim, é possível conduzir testes a partir dados originalmente reais, sem correr risco de exposição ou vazamento dos mesmos.

NÃO CORRA RISCOS ANONIMIZE DADOS DE TESTES !

OOZONE
INTELIGÊNCIA DIGITAL

ELIMINE DADOS DUPLICADOS

Um mesmo usuário (titular) pode ter entradas em diferentes plataformas, com nomes abreviados, incompletos etc. Você precisa identificar as duplicidades e consolidá-las para conseguir resgatá-los caso seja necessário.

Para isso, precisará de uma solução que permita a correta manutenção e compartilhamento de dados entre sistemas e interfaces de entradas.

Uma solução que apresente recursos de *Machine Learning* e *Artificial intelligence* para otimizar os processos é fundamental para acelerar e padronizar operações repetitivas.

OOZONE
INTELIGÊNCIA DIGITAL

CHECKUP DE SEGURANÇA DA INFORMAÇÃO

Um requisito fundamental no tratamento de dados é a CONFIDENCIALIDADE, mantendo-os seguros em todos seus estados seja em trânsito e/ou em repouso (transferência e armazenamento), criando rotinas de verificação dos procedimentos de Segurança da Informação em todos os ambientes, pois este é um tema transversal que deve ser observado em toda organização.

Abaixo algumas boas práticas e *frameworks* de mercado:

Segurança segundo atribuições ou funções
Sistema de senhas para acesso a ambientes digitais de acordo com as permissões associadas à conta do usuário conforme necessidade mínimas e especificas para execução das suas atividades

Autenticação por diretórios (MS AD / LDAP)
Usado com base centralizada para delegar a autenticação de uma conta de usuário externo a um diretório LDAP e para fornecer autenticação usando as mesmas informações de segurança usadas para outras aplicações em sua empresa.

Senha-frase de instalação de sistemas
Durante o processo de instalação, utilize uma frase secreta, com mais de 16 caracteres e altamente segura, que será necessária para iniciar o sistema e acessar informações protegidas.

Política de Senhas
De acordo com as regras de segurança da empresa, incluindo opções como o número de dias que uma senha é válida, tamanho mínimo e complexidade desta senha.

Single Sign On
Autenticação de usuários feita com uma só senha para diferentes aplicações, evitando a criação de várias senhas.

Hardware Security Module (HSM)
Dispositivo de segurança baseado em hardware que gera, armazena e protege chaves criptográficas.

Criptografia
Permite a configuração de uma camada adicional de segurança, além das permissões tradicionais de arquivos e bancos de dados.

Normas ISO/IEC-27000
Implemente os processos e controles descritos nas normas da família ISO27000, pois estes descrevem muitos dos requisitos existentes nas atuais leis de privacidade de dados

Federal Information Processing Standards (FIPS)
Para estar em conformidade com os requisitos de segurança do FIPS 200, as aplicações devem usar módulos criptográficos certificados pelo *Cryptographic Module Validation Program* e compatíveis com FIPS 140-1 ou 140-2.

Protocolo de status de certificado on-line
O protocolo OCSP (*Online Certificate Status Protocol*) é um conjunto de estruturas de dados ASN.1 definidas para solicitar e receber informações sobre o status de revogação de certificado.

Transport Layer Security (TLS)
Uso protocolos de comunicação seguros para dados em transporte com criptografia utilizando TLS 1.2 ou superior somente com cifras fortes

OOZONE
INTELIGÊNCIA DIGITAL

DEFINIÇÃO DO ENCARREGADO DE DADOS

A lei determina que cada organização deve nomear um ENCARREDADO DE DADOS, ou seja, a pessoa que responde pela gestão e salvaguarda dos dados em todo o seu ciclo de vida.

Nos casos de uma eventual violação, quebra de segurança ou vazamento cabe a ele notificar autoridades competentes (Agencia Nacional de Proteção de Dados) sobre qualquer incidente de segurança que venha a ocorrer. Ele atuará como um canal de comunicação com os TITULARES dos dados, respondendo pela supervisão e fiscalização do cumprimento das regras de proteção de dados pessoais.

OOZONE
INTELIGÊNCIA DIGITAL

SOLICITAÇÕES E EVENTOS DE CRISE

A lei define que o cidadão poderá, sempre que desejar, revogar sua autorização de tratamento, bem como pedir acesso, exclusão, portabilidade, complementação ou correção de dados armazenados sobre ele próprio.

Portanto, você precisará criar um plano interno de trabalho para responder a estas demandas que com certeza chegarão. Defina um processo claro, estruturados e quem são os envolvidos. Certifique-se de que todos sabem como proceder.

Estabeleça um processo de resposta a incidentes, com fluxo para a comunicação de um eventual incidente e suas providências, incluindo áreas como jurídico, tecnologia e relações públicas.

Para eventuais necessidades, tenha o registro de todas as atividades de tratamento realizadas, do tipo de dado, prazos de tratamento e a fundamentação para o tratamento, bem como relatórios de impacto à proteção de dados (DPIA).

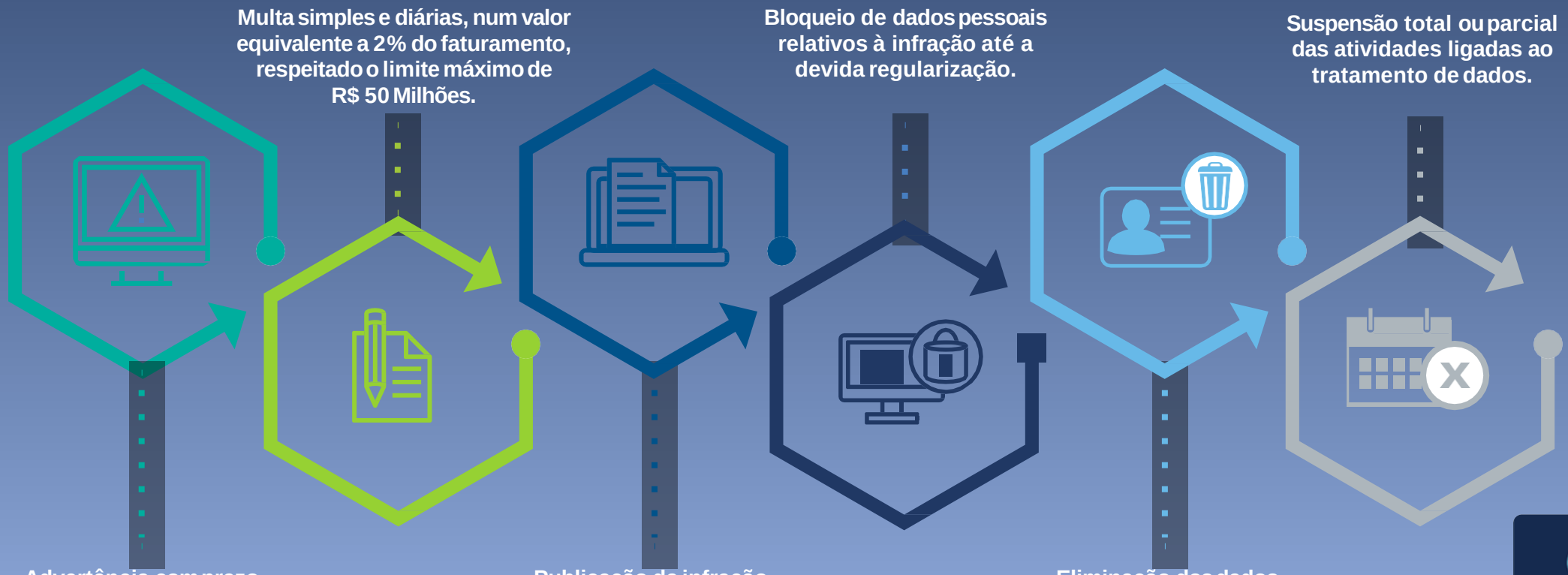
OOZONE
INTELIGÊNCIA DIGITAL

SANSÕES

Consulte a área jurídica e certifique-se que seus processos de coleta e tratamento de dados estão em conformidades, assegure que sua Política de Privacidade está de acordo com a nova lei de forma clara e inequívoca, especialmente nos canais digitais e nos formulários de registro.

As implicações legais são várias, com impactos nas atividades da organização, imagem e financeiros.

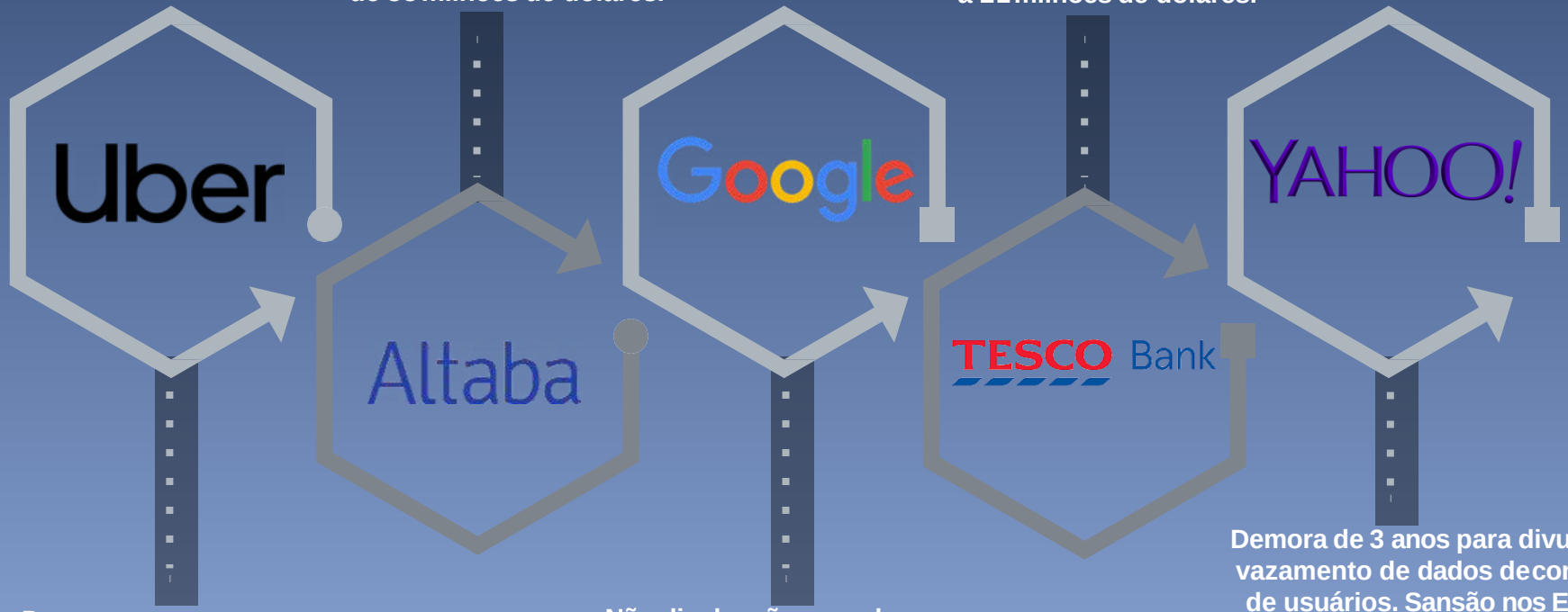
Se comprovada a infração, a empresa poderá receber:



OOZONE
INTELIGÊNCIA DIGITAL

INCIDENTES E SANSÕES

Somente para se ter uma ideia, eis algumas sansões aplicadas a empresas, com base na GDPR (versão europeia da LGPD brasileira) e em outras leis de proteção e privacidade de dados:



OOZONE
INTELIGÊNCIA DIGITAL

CONTE COM PARCEIROS PREPARADOS

Adequar-se à LGPD é um grande desafio para os negócios, pois envolve diversos departamentos, bem como etapas que exigem um conhecimento técnico e ferramental não desenvolvido. Pensando em facilitar a organização das empresas no que diz respeito à governança dos dados e minimizar o volume de tarefas referentes à adequação à LGPD, oferecemos alguns pacotes compostos de soluções que podem ser acompanhados ou não de serviços de consultoria e implementação. Abaixo, você pode conferir os três tamanhos de pacotes que podem auxiliá-lo nos passos 1, 3, 4 e 5 da jornada descrita neste e-book.

OOZONE #1

- Governança sobre dados estruturados.
- Definição, descoberta e mapeamento dos dados estruturados.
- Análise e governança de dados estruturados em banco de dados, Haadop, arquivos CSV etc.
- Registros das atividades de processamento de dados.
- Gestão de direitos de acessos a dados.

Suporte padrão.

Inclui as soluções: nDex A

OOZONE #2

- Governança sobre dados estruturados e não estruturados.
- Definição, descoberta e mapeamento dos dados estruturados.
- Análise e governança de dados estruturados em banco de dados, Haadop, arquivos
- CSV etc.
- Registros das atividades de processamento de dados.
- Gestão de direitos de acessos a dados.
- Análise de dados não estruturados, documentos, e-mails, pdf, imagens.
- Suporte padrão.

Inclui as soluções: nDex A, B

OOZONE #3

- Governança de dados estruturados e não estruturados, *Data Catalog;*
- Análise e governança de dados estruturados em banco de dados, Haadop, arquivos CSV, etc.
- Registros das atividades de processamento de dados.

Gestão de direitos de acessos a dados.

- Análise de dados não estruturados, documentos, e-mails, pdf, imagens.
- Criação de bancos de dados de teste com tamanho correto.
- Mascaramento de objetos de negócios em bancos de dados e aplicativos heterogêneos.
- Suporte padrão.

Inclui as soluções: nDex A, B, C

OOZONE
INTELIGÊNCIA DIGITAL

OBRIGADO

CONTATOS

Rio Grande do Sul / Santa Catarina

Telefones: +55 (51) 9840.4771 / +55 (48) 98461.6157

E-mail: contato@oozone.com.br

OOZONE
INTELIGÊNCIA DIGITAL