FORNETIX

LGPD
A lei que vai trazer proteção aos dados

A LGPD é uma realidade e acompanha uma tendência crescente em todo mundo. Seu objetivo é proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. O desafio é estabelecer uma estratégia, processos e controles para assegurar o direito do cidadão ao controle, e assim, à proteção de seus dados pessoais e íntimos.

Neste contexto da transformação digital, a LGPD é um desafio que todas as empresas precisam enfrentar. Atenta a essas necessidades, a Fornetix oferece uma solução única, que consolida numa só ferramenta a criptografia nativa para VM´s, a soberania sobre seus dados, a criptografia de bases de dados (estruturados ou não) e na nuvem, o BYOK (Bring Your Own Key), aliada à automação e distribuição do ciclo de validade dos certificados digitais. Evite custos desnecessários e o risco de erro humano na gestão das suas chaves e do ambiente criptográfico.

- Criptografia de Base de dados Oracle, SQL, Mongo, MySQL, DB2, etc.
- Criptografia de VMs, fundamental para LGPD, VMware, OpenStack, Nutanix
- Anonimização e Pseudo-Anonimização
- Criptografia de Kubernetes, Openshift, FullDisk
- O gerenciamento centralizado de chaves permite ao usuário controle efetivo de milhões de chaves, dispositivos e identidades
- Agendamento eficiente da renovação de chaves e certificados digitais
- Automação do ciclo de distribuição de certificados digitais
- Maior controle e drástica redução de ocorrências de erros no manuseio de segredos e chaves
- Informações consolidadas para auditoria
- Painel central de gestão

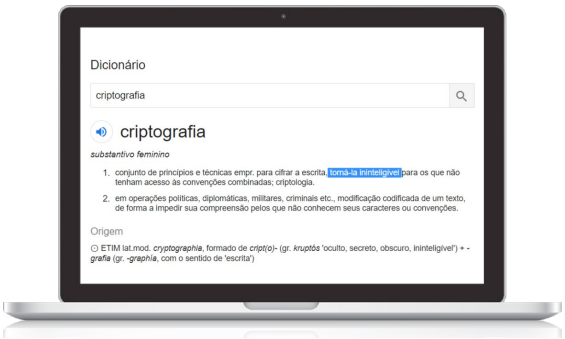
» Por que usar o VaultCore na LGPD?

CAPÍTULO VII
DA SEGURANÇA E DAS BOAS PRÁTICAS
ART46

- a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
- b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
- c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; periódicas

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

O que são dados ininteligíveis?



Como será sua política de acesso às chaves?
O Vaultcore é uma console de gestão unificada que guarda dos seus segredos - as chaves - num local único, sob um forte esquema de segurança e gerenciado por políticas de uso definidas, permitindo inclusive a destruição dos dados quando necessário. Este requisito está na lei. Será necessário adotar as boas práticas e ferramentas apropriadas, pois não adianta criptografar os dados e deixar as chaves desprotegidas. Seria o mesmo que fechar a porta e deixar a chave na fechadura.

Como começar a sua estratégia de proteção no dado com criptografia?

Vamos fazer por etapas, primeiro pelo o mais fácil e abrangente, usando as soluções que funcionam nativamente, por exemplo em certos casos criptografando suas VMs, cerca de 90 % dados estarão cifrados e protegidos contra ataques de Ransonware, e outros de acesso privilegiados, com baixíssimo custo e nativas, ou seja você já tem em sua infra e talvez não saiba como implementar.

1. Criptografar suas máquinas virtuais

INTEGRAÇÃO: Transparente e Nativa
TEMPO: 5 MIN P/ VM
TIME: Somente o pessoal de infra e segurança
PROTEÇÃO DE: arquivos dentro da VM, VSAN, VMotion.
CONTRA: RANSONWARE, ROUBO DADOS, Clear BACKUPS
CUSTO: Muito Baixo (Sem custo dependendo do provedor)

2. Soberania de Dados

INTEGRAÇÃO BYOK: Transparente via conector com AWS, GOOGLE, e AZURE
TEMPO: 30 MIN
TIME: Somente o pessoal de infra e segurança
PROTEÇÃO DE: SOBERANIA DE DADOS, BYOK.
CONTRA: Resoluções de cloud pública, perda de chaves
CUSTO: Muito Baixo (Sem custo dependendo do provedor)

3. Transparente data encryption (TDE)

INTEGRAÇÃO: Diretamente nas bases de dados
TEMPO: Muitas HORAS (pode ter downtime) depende da Base, DBA
TIME: Pessoal de infra, DBA e segurança
PROTEÇÃO DE: Dados nas colunas, arquivos das bases, permissão controlada de usuários.
CONTRA: Usuário DBA (alguns casos), acesso indevido ao arquivo das bases.
CUSTO: Algumas bases o serviço não tem custo, mas há alguma que cobram, porém nã há perda de suporte pelo fabricante.

4. Na Aplicação

INTEGRAÇÃO: Chamadas REST
TEMPO: DIAS, exige desenvolvimento.
TIME: Pessoal de infra, DBA, Desenvolvimento e segurança
PROTEÇÃO DE: Dados granulares, máxima proteção independente da base, performance.
CONTRA: Usuário DBA, acesso indevido ao arquivo das bases como um todo.
CUSTO: Alto, backlog de desenvolvedores, tests

Será que sua estratégia de Anonimização estará completa?

Como garantir a integração de bases deixando-as anonimizadas ou pseudo-anonimizadas sem o poder da criptografia? Quanto vai custar isso? É possível usar ferramentas para transfomar os dados, para desenvolvimento e testes.

Podemos dispor de ferramentas e técnicas de abstração de dados, com custo muito baixo e que disponibilizarão dados anonimizados para as analises de BI.

Você vai automatizar a Criptografia?

Além disso como será o gerenciamento de criptografia após a implementação, as centenas de chave e certificados digitais, em dezenas de servidores, tudo manualmente?

Quantas pessoas serão necessárias para gerenciar as chaves, sem contar os riscos de esquecimento e transporte de segredos por email.
Já pensou que pode ter problemas de estresse dos usuários nestas obrigações?

O VaultCore vai realizar esta tarefa de forma programática, sem interferência humana, muito rapidamente, em segundos, os certificados serão gerados e distribuídos em sua infraestrutura.

Sobre a Fornetix

Fornetix se concentra no gerenciamento, distribuição e federação das chaves de criptografia, resultando em uma coordenação de segurança e disponibilidade de dados para clientes de diversas soluções de mercado, isso permite implementar uma estratégia com pouco impacto no desempenho. Fornecendo aos usuários uma solução de gerenciamento de chave de criptografia que combina a automação dos certificados digitais e a criptografia com controles granulares de acesso do usuário entre dados em repouso e em movimento, tornando-o o parceiro ideal para utilizar a funcionalidade de segurança habilitada por design pela solução muitas vezes já implementada, de forma transparente.