LGPD – LEI GERAL DA PROTEÇÃO DE DADOS

Andrei Rubino - https://www.linkedin.com/in/andrei-rubino-4a43746b/

Manual prático LGPD

Objetivo

O objetivo deste documento é fornecer informações sobre como aplicar a LGPD, o documento não consiste em um passo a passo detalhado, mas sim em apontar as principais etapas e breves dicas sobre técnicas e ferramentas que poderão ser utilizadas para a adequação. Me coloco a disposição para debatermos sobre o assunto.

Referências

Grande parte do conteúdo deste documento foi anotações a quais fiz assistindo o curso do Daniel Donda (link abaixo), recomendo como um ótimo curso.

https://www.udemy.com/course/lgpd-na-pratica/

1. Definir papéis

Controlador, Operador, Encarregado e ANPD.

2. Definição da finalidade do uso

- Consentimento
- Obrigação legal
- Administração Pública
- Estudos por órgão de pesquisa
- Contratos
- Proteção da vida

3. Planejamento do ciclo de vida da informação/dados(tratamento de dados)

1. Coleta

2. Análise/Processamento
3. Tratamento
4. Armazenamento
5. Transferência/Compartilhamento
6. Descarte

4. Criar controlador de domínio na rede corporativa

- um grupo para os controladores
- um grupo para os operadores
- um grupo para os agentes de tratamento (neste grupo add como membro os controladores e operadores)

5. Descoberta dos dados (data discovery)

É necessário listar os locais onde existem os dados dos clientes.

Ex: servidores de banco de dados, backups (fitas etc), estações de trabalho (celulares, notebook, desktop etc), servidores de arquivos, arquivos físicos. Após a descoberta é necessário identificar (dados pessoais, dados pessoais sensíveis, etc).

Quando as informações/dados não forem mais utilizadas elas devem ser apagado.

Lista de softwares que podem auxiliar na busca

- BIG ID
- Data radar
- Keepabl
- Egnyte
- Archu
- Octopai

6. Descoberta e classificação de arquivos

É necessário buscar os dados em conteúdos de arquivos para classificá-los.

No windows temos uma ferramenta FSRM que busca, gerencia e classifica os arquivos, através desta ferramenta é possível criar padrões de busca e classificações. São criados propertys e rules onde são definidos o escopo de pesquisa, diretórios etc.

Através das rules é possível configurar um regex para pesquisas em conteúdos de arquivos. Também é possível configurar o servidor para:

- Enviar emails/notificações
- Quando executar?
- Gerar log
- Gerar relatórios

7. Mapeamento dos Dados pessoais (planilha)

-- Solicitar planilha via contato.

8. Término do tratamento de dados

O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

- Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
- Fim do período de tratamento;
- Comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público; ou
- Determinação da autoridade nacional, quando houver violação ao disposto na Lei.

Quando e finalizado o término do tratamento de dados os dados devem ser deletados/destruídos.

Lista de softwares que podem auxiliar na exclusão dos dados, esses softwares utilizam vários algoritmos de exclusão como o **gutmann** e o **DODS5220.22-M**.

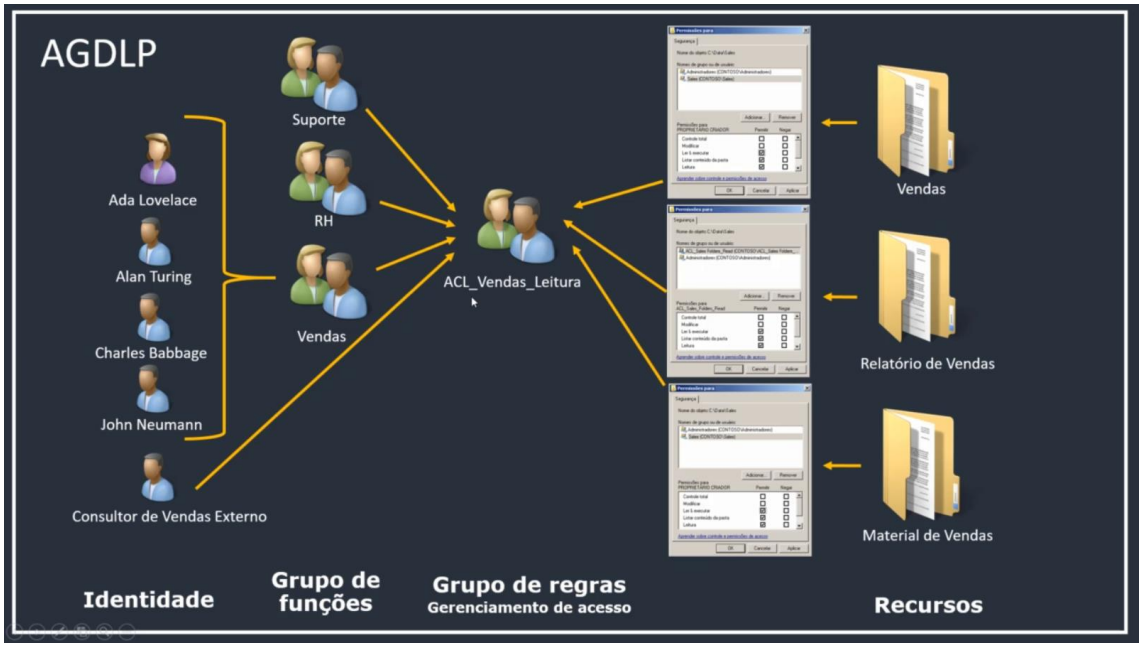
Como descartar equipamentos físicos?

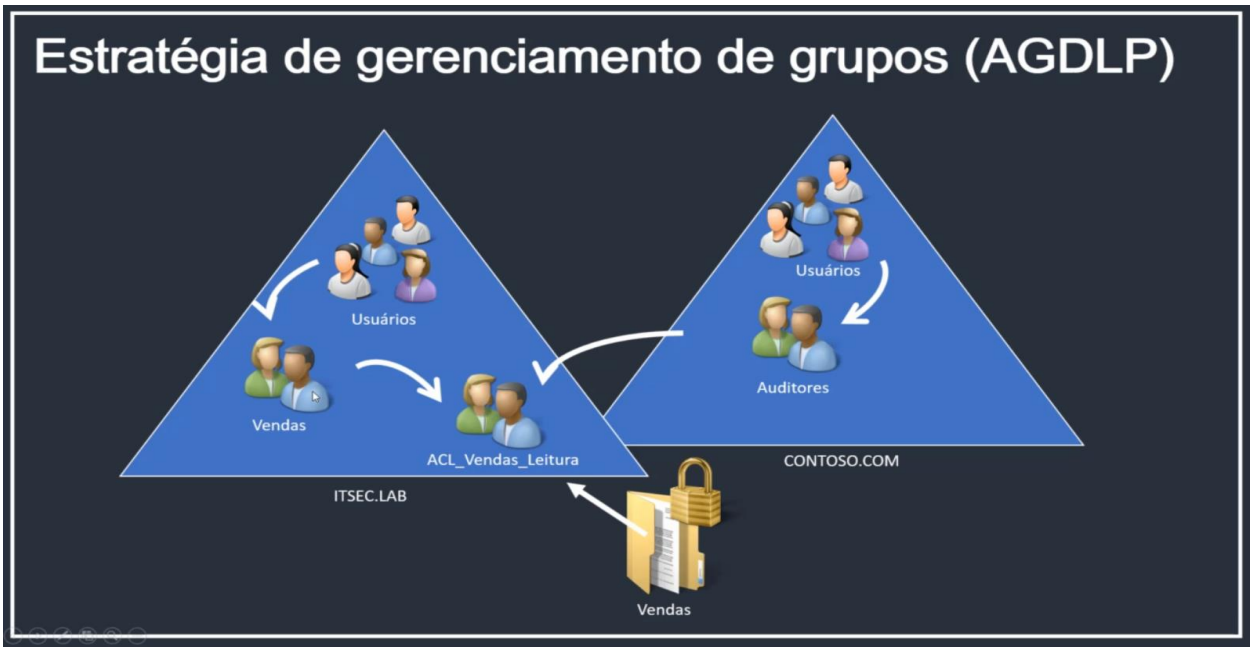
Além de garantirmos que os dados sejam excluídos os equipamentos físicos devem ser descartados de maneira ecológica e segura. Existem empresas especializadas em fazer este descarte.

9. Mapear acessos a arquivos e diretórios

- Devemos criar usuários, grupos e permissões de acesso, visualização, edição etc. Estes usuários terão acesso as informações, é importante documentar o máximo de dados possíveis desses usuários.
- No windows temos o padrão AGDLP (account, global, domain local, permission) onde definimos usuários, grupos e permissões de acesso podendo ser compartilhados entre domínios.
- Podemos utilizar um file server para verificar todas as permissões de compartilhamento.
- Com os arquivos já identificados devemos restringir os acessos aos diretórios por grupos de usuários.

Exemplo abaixo:





10. Proteção dos dados

- Controle de login
- Firewall
- Criptografar dados
- Criar regras de acesso a bancos de dados, e criptografar/bloquear acesso às colunas?
- Criptografia nativa windows (EFS)

  É um recurso que pode criptogradas arquivos em uma partição com formato NTFS utilizando chaves privadas e públicas

11. DPIA(Data Protection Impact Assessment) / RIPD (Relatório de Impacto à Proteção de Dados)

Para a LGPD o que diz respeito ao Relatório de Impacto à Proteção de Dados (RIPD), de acordo com o inciso XVII do artigo 5º, que faz alusão a esse relatório como sendo a “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”.

Etapas da DPIA / RPID

- Identificação da necessidade.
- Descrever o fluxo de informações.
- Descrever a natureza, o escopo, o contexto e os propósitos do processamento.
- Identificar os riscos para os direitos e liberdades dos titulares de dados.
- Identificar soluções para reduzir ou eliminar esses riscos.
- Assine os resultados do DPIA e RIPD.
- Integrar soluções de proteção de dados no projeto.

12. Ameaças, Vulnerabilidades e Riscos

Ativos: É qualquer item de valor para a organização. Ex:

- Dados e informações
- Rede
- Servidores
- Estações
- Softwares
- Pessoas

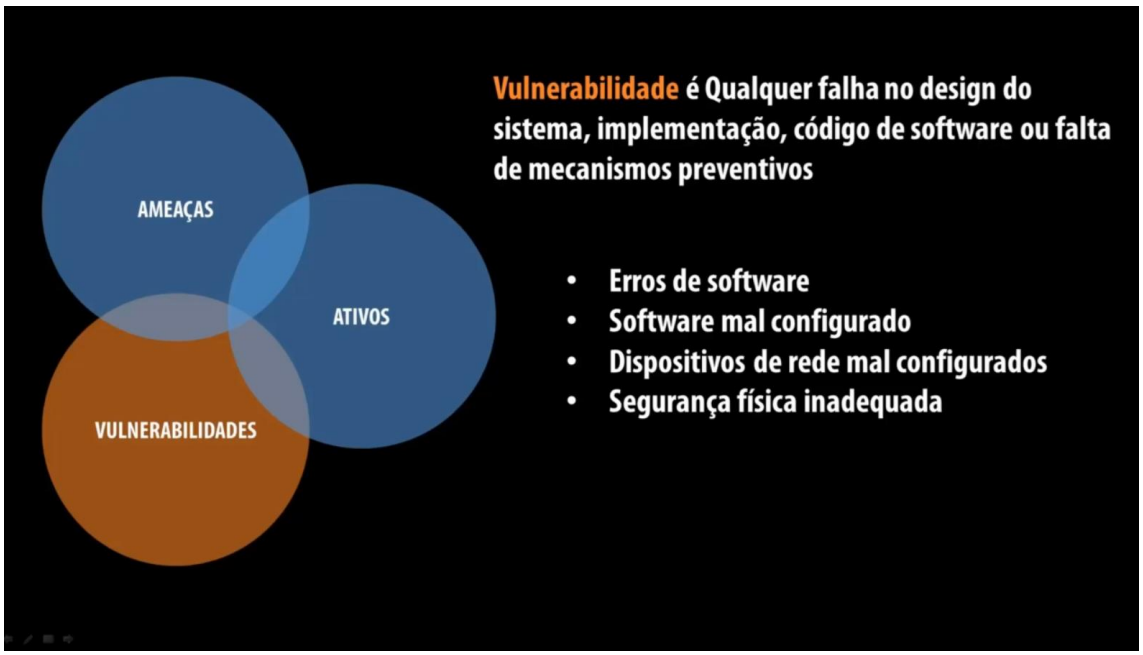
Ameaças: É qualquer tipo de confissão que pode causar dano, perda, ou comprimento de um ativo. Ex:

- Desastres naturais
- Ataques cibernéticos
- Violação da integridade dos dados
- Vazamento dos dados
- Malwares
- Insiders

As ameaças não são controláveis, mas sim mitigáveis.

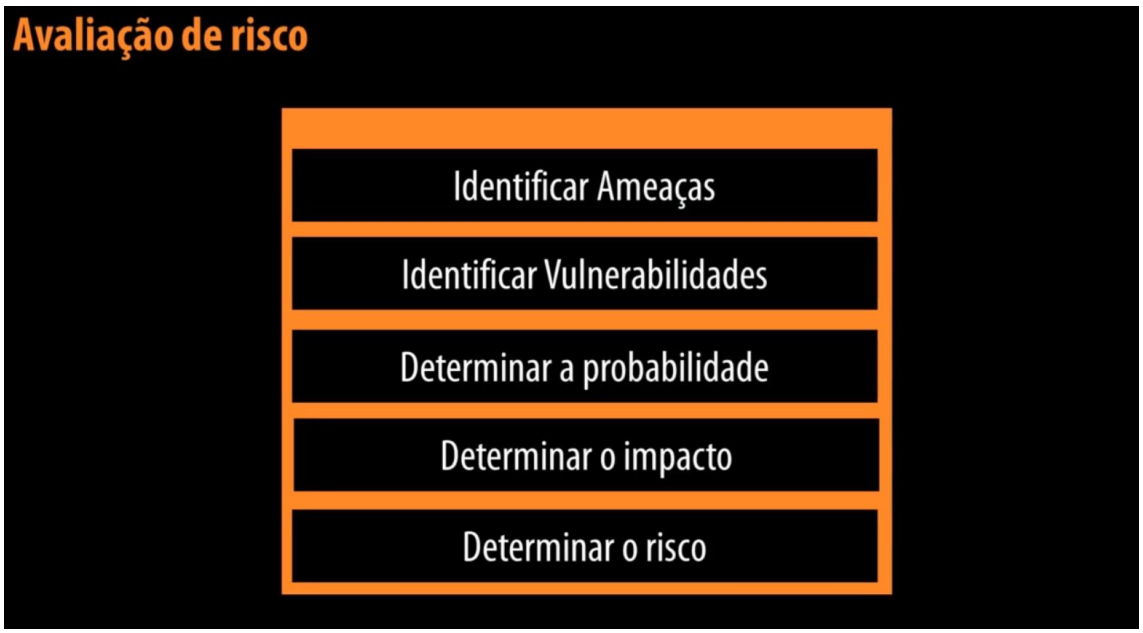
Vulnerabilidade: É qualquer falha no design do sistema, implementações código de software ou falta de mecanismos preventivos. Ex:

- Erros de software
- Software mal configurado
- Dispositivos de rede mal configurado
- Segurança física inadequada



Avaliação de risco na prática

- Identificar ameaças
- Identificar Vulnerabilidades
- Determinar probabilidade (baixo/medio/alto)
- Determinar impacto (baixo/medio/alto)
- Determinar o risco (baixo/medio/alto impacto)



13. Senhas e LGPD

Melhores práticas para criação de senhas

- Nunca usar a mesma senha
- Alterar a senha frequentemente
- Utilizar uma senha forte/ Não utilizar senhas comuns
- Utilizar duplo fator(tokens,sms,email,etc)
- Separar usuários comuns e contras administrativas

Ferramentas de Segurança de Senha

- One Identity safeguard serve como um cofre de senhas, onde quando eu preciso acessar algum recurso é validado neste servidor se tenho permissão e por quanto tempo. Quem faz as liberações neste software são os gestores assim os usuários não possuem acesso as senhas, gerando mais segurança.

Políticas de segurança de senhas:

- Duração em dias da senha / Obrigar a troca da senha a cada x dias
- Quantidades e tipos de caracteres
- Bloquear acesso a cada x tentativas de login invalidas

Obs: Nos EUA pequenas e médias empresas somam 70% dos ataques.

14. Estrutura de um ataque

- Reconhecimento

Busca identificar o máximo possível de informações do alvo, algumas técnicas de reconhecimento são footprint, engenharia social, sniffing. Na fase de reconhecimento é descoberto um host e através deste host ele busca identificar contas administrativas.

- Escaneamento e Acesso

  Aqui acontece os ataques

- Manter o acesso

  Para continuar roubando informações/dados

- Limpar os rastros

Após encontrar as contas leva-se em torno de 24 a 48h para quebrar a senha e neste momento os dados já podem ser extraídos.

Leva-se em média 11 a 14 meses para ser descoberto um ataque

15. Principais tipos de ataque

- Man-in-the-middle

Man-in-the-middle é um nome genérico para qualquer ataque virtual em que alguém fica entre você e o que você está fazendo.

Ex: Os alvos mais comuns de ataques são:

- Sites de compras online
- Sites de serviços bancários online
- Sites em que você precisa fazer login antes de acessar a conta ou dados de cartão de crédito
- Case: Luptons / Venda Casa / Advogado + Email + Transferencia bancaria 333U$

Tipos de ataque Man-in-the-middle

- Sniffing
- Eavesdropping (bisbilhotar)
- DNS Spoofing

O código para envenenamento de cache de DNS é normalmente encontrado em URLs enviadas via e-mails de spam. Esses e-mails tentam assustar os usuários para que cliquem na URL fornecida que, por sua vez, infecta seu computador.

- SQL Injection

  Ataques a aplicações a fim de descobrir dados e até mesmo se conectar ao servidor.

- Trojan / Spyware / keylogger

Muito utilizados em e-mails e em ataques sociais através de dispositivos como pen drive ou outro a qual se conectam ao computador.

- DOS / DDOS

É uma tentativa de fazer com que aconteça uma sobrecarga em um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores. Para isso, o atacante utiliza técnicas enviando diversos pedidos de pacotes para o alvo com a finalidade de que ele fique tão sobrecarregado que não consiga mais responder a nenhum pedido de pacote. Assim, os utilizadores não conseguem mais acessar dados do computador por ele estar indisponível e não conseguir responder a nenhum pedido

- Shoulder surfing

É um tipo de técnica de engenharia social usada, o hacker de alguma forma observa a vitima a digitar sua senha para depois fazer o ataques. Este ataque pode acontecer na observação pessoal, sistema de câmeras etc.

- XSS Cross-site-scripting

É um tipo de vulnerabilidade do sistema de segurança de um computador, encontrado normalmente em aplicações web que ativam ataques maliciosos ao injetarem client-side script dentro das páginas web a fim de capturar informações/dados.

- Buffer Overflow

Acontece quando um programa informático excede o uso de memória assignado a ele pelo sistema operacional, passando então a escrever no setor de memória contíguo.

Essas falhas são utilizadas por cibercriminosos para executar códigos arbitrários em um computador, o que possibilita muitas vezes aos atacantes controlar o PC

- 0 day (zero day)/ Exploit /

Exploração de “dia zero” é um ataque virtual que ocorre no mesmo dia em que um ponto fraco do software é descoberto. Então, ele é explorado antes que o fornecedor disponibilize uma correção. Ex: Quando são descobertos falhas em sistemas do windows ou outros softwares e os fornecedores ainda não lançaram patchs de atualização.

- Quebra de senha (Password cracking)

É uma técnica onde consiste em quebrar a senha através de algoritmos que forçam senhas comuns ou até mesmo algo mais pessoal onde o atacante já possui informações da vítima. Ex: nomes de familiares, animais de estimação etc

- Engenharia Social

Quando os próprios usuários acabam fornecendo dados para o atacante através de ataques phishing e spear phishing . É uma maneira desonesta que cibercriminosos usam para enganar você a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem isso enviando e-mails falsos ou direcionando você a websites falsos.

- Data Exfiltration

Ocorre quando um malware e / ou um agente malicioso realiza uma transferência de dados não autorizada de um computador. Também é comumente chamado extrusão ou exportação de dados

Projeto de segurança para aplicações web: www.owasp.org

16. Softwares de Análise de vulnerabilidade

Os softwares abaixo fazem análise de vulnerabilidades de sites e sistemas listando ocorrências e gerando relatórios. Com isso podemos implementar medidas de segurança.

- Acutenix
- Openvas
- Ecotrust
- Kace

17. Auditoria e Relatórios

- Quem?
- O que?
- Quando?
- Onde?
- Origem?

No windows server temos uma auditoria nativa com auditoria de logon, diretórios, de acesso a objetos, etc.

O software Change auditor é um software nativo do windows que gerencia arquivos realizando uma auditoria.

Ex: Falhas de acesso a arquivos e diretórios.

Abertura, criação, edição, delete de arquivos e diretórios.