SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

PUC Minas Virtual

PUC Minas
Virtual

UNIDADE IV – SEGURANÇA DOS DADOS

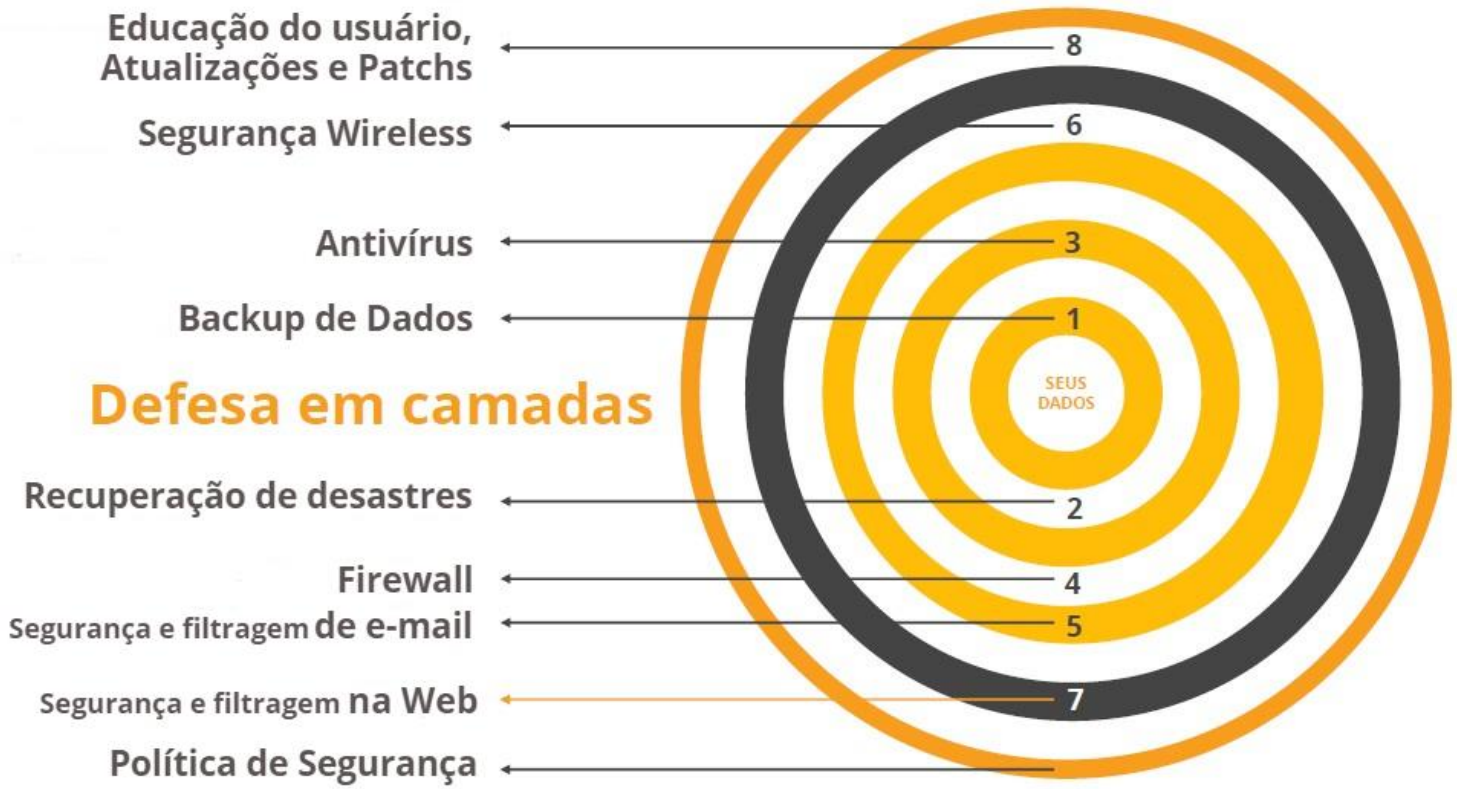
PUC Minas
Virtual

4.2 – TRATAMENTO DE DADOS SENSÍVEIS NAS ORGANIZAÇÕES

PUC Minas
Virtual

4.2.2 – SEGURANÇA DE AMBIENTE E *HARDENING* DE *WEBAPPs*

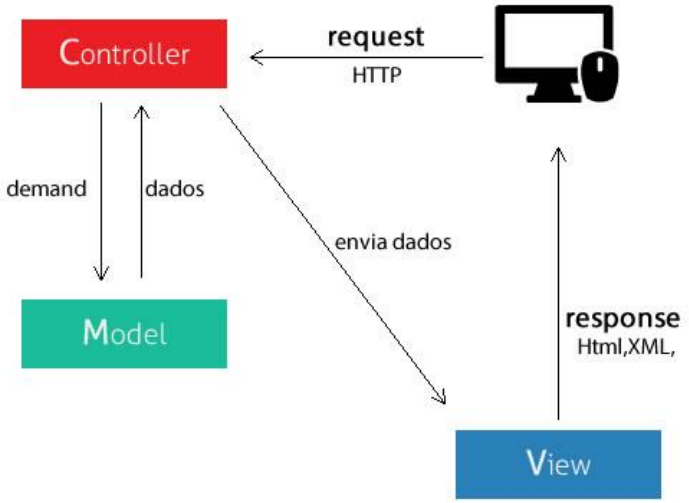
SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS



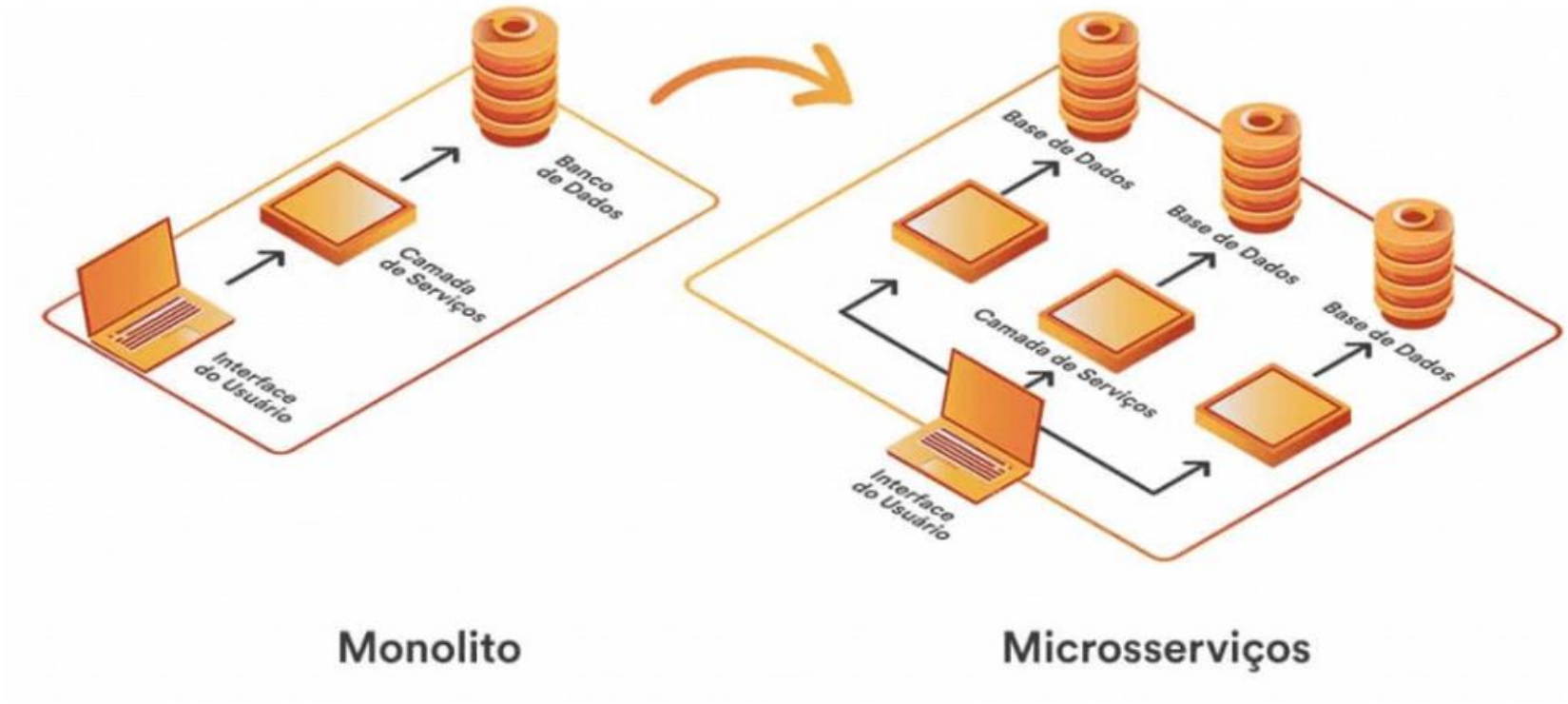
FONTE: GARRATECH,2022.

FONTE: ADDEE,2019.

SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS



FONTE: RAMOS,2022.



FONTE: SUPERO,2020.

OS AMBIENTES

- Em um mundo repleto de *Service Oriented Architecture* **(SOA)**, com todas as integrações e acessos controlados não podemos deixar de olhar para um assunto importante que é a **segregação de ambientes**.

FONTE: BERGAMI,2014.

SEGREGAÇÃO DE AMBIENTES

- É tanto quanto elementar falarmos da segregação do ambiente de produção em detrimento dos demais ambientes.
- No entanto fato importantíssimo a esclarecer é que devemos usar os mesmos argumentos para segregar o ambiente de homologação e de desenvolvimento além do de testes.
- Implantar em produção software defeituoso pode destruir a credibilidade do produto e a reputação da empresa.

SEGREGAÇÃO DE AMBIENTES

- Os desenvolvedores geralmente usam ambientes de desenvolvimento integrados que consistem em várias ferramentas de desenvolvimento e acessos especiais com permissões avançadas para garantir o correto funcionamento do software.

- **Ambiente de produção não se altera! Inclusive os dados! E esta deve ser uma preocupação das empresas pois, imagine só uma empresa terceira tendo acesso a seus dados de produção?**

REFORÇANDO AS APLICAÇÕES WEB

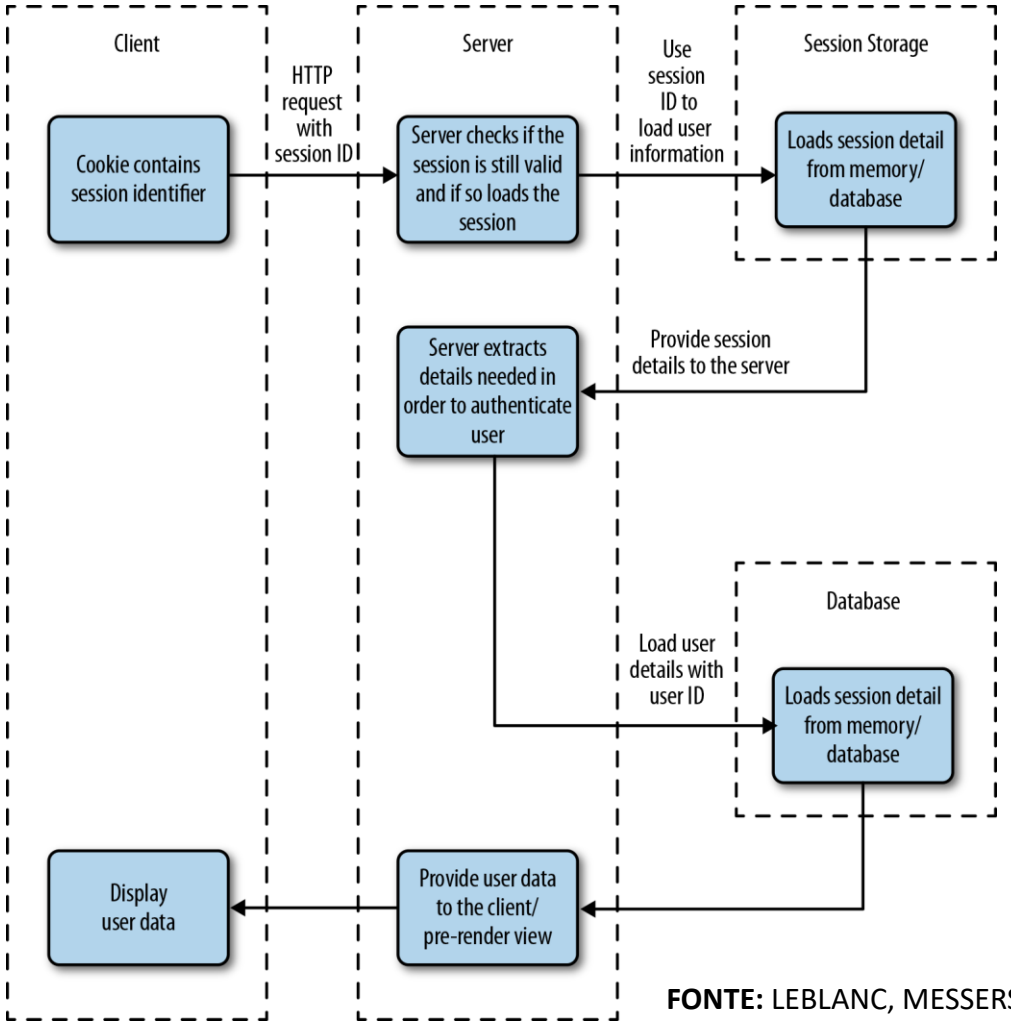
- O outro tipo é o *cross-site scripting* **(XSS)**, que envolvem código malicioso sendo injetado em sites de outra forma confiáveis**.**
- **Como resultado, os scripts maliciosos podem acessar quaisquer cookies, tokens de sessão ou outras informações confidenciais retidas pelo navegador e usadas nesse site.**
- Este tipo de ataque ainda pode ser classificado em três categorias principais — XSS **Armazenado**, XSS **Refletido** e XSS **baseado em DOM.**

SESSÕES

- O controle de sessão dentro dos aplicativos existe para persistir logins de usuários em várias rotas dentro de nosso aplicativo sem a necessidade de reautenticar o usuário solicitando nomes de usuário e senhas repetidamente.
- As sessões precisam atender a determinados requisitos para atender às expectativas de segurança: os IDs de sessão devem ser exclusivos e não sequenciais. Assim como as senhas, as sessões se beneficiam de IDs de sessão longos que diminuem as possibilidades de ataque.

COOKIES

- Cookies armazenam as informações de preferências do usuário, detalhes de autenticação (como nome de usuário e senha) e informações de sessão do lado do cliente.
- **Na prática podem ser vistos como a implementação de sessões do lado do cliente e geralmente são combinados com fortes mecanismos criptográficos para fornecer segurança, integridade e autenticidade dos dados (RFC 2965) .**



FONTE: LEBLANC, MESSERSCHMIDT, 2016.

OS AMBIENTES

- Com a combinação das proteções consegue-se alcançar um nível mínimo de segurança nas aplicações WEB.
- Cookies do lado cliente e Sessões do lado do servidor.
- Mesmo assim ainda podemos ter alguns problemas **(RFC 62653).**

VEJAM O ARCABOUÇO

- HTTPS, OPENSSL, OPENID, URL-Encoding, COOKIES, SESSIONS, CRIPTOGRAFIA, TLS, CA!
- **E tem muito mais!**
- Porém não adianta nada guardar a senha em um repositório aberto do **git,** pergunte para algumas empresas sobre vazamento de dados baseados nesta questão!
- **E vamos evoluindo!**

REFERENCIAS BIBLIOGRÁFICAS

LEBLANC Jonathan. MESSERSCHMIDT, Tim. Identity and Data Security for Web Development. O'Reilly, 2016.

ADDEE,2019. Segurança em camadas: entenda o que é e qual a sua importância. Disponível em: <https://addee.com.br/blog/seguranca-em-camadas/>. Acesso em:14 Nov. 2022.

GARRATECH ,2022. O que é um ataque de cross-site scripting? Definição e explicação. Disponível em: <https://garratech.com.br/sua-empresa-mais-segura-defesa-em-camadas/>. Acesso em: 02 Nov. 2022.

RAMOS ,Allan**.** O que é MVC? Explicando o MVC, um padrão de arquitetura para organizar sua aplicação. Disponível em: <https://tableless.com.br/mvc-afinal-e-o-que/>. Acesso em: 02 Nov. 2022.

REFERENCIAS BIBLIOGRÁFICAS

SUPERO,2020. Microsserviços: conceito, vantagens e desvantagens dessa arquitetura. Disponível em: <https://www.supero.com.br/blog/microsservicos-conceito-vantagens-e-desvantagens-desse-tipo-de-arquitetura/>. Acesso em: 14 Nov. 2022.

BERGAMI, 2014. Qualidade em TI – Segregar para atingir a qualidade. Disponível em: <https://www.tiespecialistas.com.br/qualidade-em-ti-segregar-para-atingir-qualidade/>. Acesso em: 14 Nov. 2022.

TEDESCO, Kennedy**.** Cross-Site Request Forgery (CSRF) e abordagens para mitigá-lo. Disponível em: <https://www.treinaweb.com.br/blog/cross-site-request-forgery-csrf-e-abordagens-para-mitiga-lo>. Acesso em:14 Nov. 2022.

REFERENCIAS BIBLIOGRÁFICAS

SUPERO,2020. Microsserviços: conceito, vantagens e desvantagens dessa arquitetura. Disponível em: <https://www.supero.com.br/blog/microsservicos-conceito-vantagens-e-desvantagens-desse-tipo-de-arquitetura/>. Acesso em: 14 Nov. 2022.

BERGAMI, 2014. Qualidade em TI – Segregar para atingir a qualidade. Disponível em: <https://www.tiespecialistas.com.br/qualidade-em-ti-segregar-para-atingir-qualidade/>. Acesso em: 14 Nov. 2022.

TEDESCO, Kennedy**.** Cross-Site Request Forgery (CSRF) e abordagens para mitigá-lo. Disponível em: <https://www.treinaweb.com.br/blog/cross-site-request-forgery-csrf-e-abordagens-para-mitiga-lo>. Acesso em:14 Nov. 2022.


PUC Minas
Virtual