Proteção de Dados e Segurança de Sistemas de Informação na Saúde

Agenda

Exercícios Práticos de BrainStorming

Desafio

Definir uma política de gestão de passwords de uma unidade de saúde.

Quais os requisitos de segurança que devem ser identificados?

Gestão de passwords – Exemplo de requisitos

- Obrigatoriedade de alteração da password temporária
- Tamanho mínimo para a composição da password é de 8 caracteres
- Obrigatório o uso de regras de complexidade nas passwords
- A password não deve corresponder a uma palavra do dicionário da língua portuguesa
- A password não deve ser o nome de uma pessoa ou personagem
- A password não deve conter nenhum padrão facilmente identificável, tal como “aaaabbb”, “1234”, entre outros.
- Forcar a alteração das passwords de entrada no domínio a cada 3 (três) meses.
- Não permitir a reutilização das ultimas 3 (três) passwords.

Desafio

Definir uma política de gestão de pedido de acessos a um sistema de informação.

Criar uma definição de matriz de acessos.

Que dados deve conter?

Gestão de Pedido de Acessos – Exemplo de requisitos

- Quando possível utilizar uma aplicação destinada a este efeito;

- Identificação correta do profissional a ter acesso:
  - Número mecanográfico;
  - Nome completo do profissional;
  - Nome profissional;
  - Grupo Profissional;
  - Serviço destino;
  - Descrição das funções a desempenhar;
  - Definição dos acessos a parametrizar;
  - Número da Ordem, quando aplicável;
  - Especialidade, quando aplicável;
  - Superior hierárquico.

Envio de email para responsável para a atribuição dos acessos.

Exercício Prático

1. Descreva o tipo de informação que acede e necessita para realizar as suas tarefas diárias (pode recorrer a texto introdutório, diagramas, etc). No caso de vários tipos de informação escolha as que são mais importantes no seu dia a dia ou se liguem entre si. (Deverá tentar representar os diferentes casos de uso).

2. Categorize o tipo de informação que descreveu de forma individual, como informação publica, privada, confidencial ou outra nomenclatura que se adeque.

3. Para cada tipo de informação categorize como sendo dados pessoais ou não, defina um período de retenção máxima de dados, e justifiquei o seu propósito de recolha bem como de processamento.

Exercício Prático

4. Defina o tipo de acesso que tem à informação descrita, se leitura, se pode apagar, etc.

5. Defina um grupo de utilizadores ou características de acesso a informação que definiu em 1.

6. Defina mecanismos de autenticação e autorização para acesso a informação descrita em 1.

7. Descreva que tipo de ameaças (físicas e digitais) que essa informação poderá sofrer.

Exercício Prático

8. Descreva quais os riscos e consequências dessas ameaças nas suas atividades e no contexto geral do seu trabalho.

9. Descreva mecanismos de proteção para as ameaças descritas anteriormente.

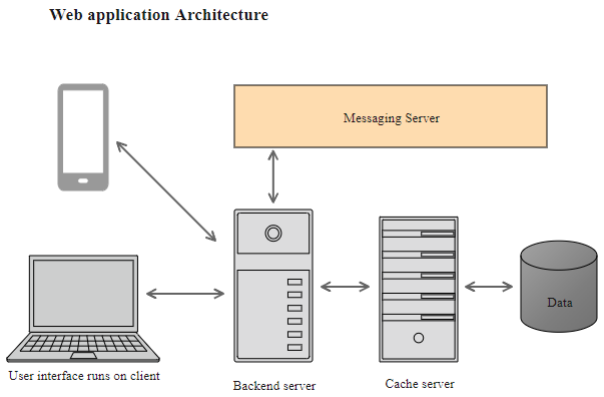
10. Defina estratégias para garantir a CIA (confidencialidade, Integridade e disponibilidade) dos dados.

11. Imagine que é um atacante, como planearia e executaria um ataque a informação apresentada em 1? E o que poderia fazer com ela?

Exercício Prático

12. O sistema de informação que suporta a informação descrita em 1 foi violado, o que deve fazer? Detalhe o máximo possível qual etapa.

13. Desenhe um esquema de comunicação de informação que represente o sistema de informação do seu caso de estudo incluindo os mecanismos de autenticação.



(Exemplo de objetos que poderá usar no seu diagrama)

Proteção de Dados e Segurança de Sistemas de Informação na Saúde