CODIFICAÇÃO BACK-END SP3

**SEGURANÇA DA INFORMAÇÃO**

**Também conhecida por INFOSEC**

**Definição: “A proteção da informação e dos sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição, a fim de garantir a confidencialidade, integridade e disponibilidade.”**

**Seu objetivo é reduzir os riscos e prevenir ameaças, garantindo o sigilo das informações e assegurando a confidencialidade dos dados e a saúde/continuidade da instituição**

* **Um DADO é um recurso que COMPÕE uma INFORMAÇÃO**

**PILARES DA SEGURANÇA DA INFORMAÇÃO:**

1. **DISPONIBILIDADE**

**Está relacionada à disponibilidade da informação sem falhas, quando solicitada e para usuários autorizados. Para um sistema ter disponibilidade, deve-se**

**. ter uma infraestrutura com controles de segurança e**

**. ser resiliente contra ameaças, além de**

**. ter recursos contra quedas de energia e falhas de hardware (equipamentos físicos)**

1. INTEGRIDADE

A integridade está relacionada à não modificação ou exclusão durante ou após o envio da informação. Para que esse pilar exista, é

. necessário que a informação original mantenha todas as suas características, sem sofrer nenhuma modificação, desde a origem até as pessoas autenticadas que são destinatárias desses dados

1. CONFIDENCIALIDADE

Os dados devem ser disponibilizados somente para pessoas autorizadas, portanto, não podem ser divulgados a pessoas externas e que não devam ter acesso a eles. Se a informação for enviada pela rede, deve-se utilizar

. criptografia,

em que somente o receptor e o emissor da mensagem possam decifrar as informações

NORMA REGULADORA : ISSO 27001: 2013

PRÁTICAS DE SEGURANÇA

Políticas de Segurança

Controle de acessos lógicos e físicos

Auditorias

Criptografia

* POLÍTICAS DE SEGURANÇA (PSI)

Determina regras e diretrizes para o acesso a dados e informações, além de responsabilidades dos membros da organização, visando atender aos pilares da segurança da informação (confidencialidade, integridade e disponibilidade).

• Não enviar e-mail em nome de outro emissor;

• Não compartilhar senhas;

• Não compartilhar informações internas com empresas parceiras, entre outros.

* CONTROLE DE ACESSO FÍSICO

Está relacionado aos mecanismos que limitarão o acesso de pessoas não autorizadas a áreas físicas da organização, a fim de evitar danificações de equipamentos, modificações não desejadas etc.Exemplo: para entrar na sala do servidor da empresa, é necessário um crachá que contém a permissão para o usuário entrar no local; sem ele, a porta não é aberta

* CONTROLE DE ACESSO LÓGICO

Está relacionado à proteção dos dados, programas e sistema, como logins, biometrias, capturas faciais, entre outros, para que somente usuários autenticados tenham acesso a determinados recursos, por exemplo, o código fonte de um projeto (possibilitando a cópia ou alteração do fluxo lógico do

banco de dados (que contém os dados internos de domínio da empresa), sistemas operacionais e senhas (delimitando regras de implementação e validação)

* AUDITORIAS

Avaliação feita para analisar e identificar pontos em que pode haver violação de segurança, de acordo com um conjunto de critérios pré-estabelecidos. Exemplo: as senhas podem ser descobertas facilmente? Há logs (registros) de quem acessa as informações?

* CRIPTOGRAFIA

Codifica uma informação, deixando-a ilegível ou dificultando a leitura por pessoas não autorizadas. Uma chave criptográfica é aquela que codifica um texto, que só o emissor e o receptor podem decifrar.

CONFIGURAÇÕES DE SEGURANÇA NO SERVIDOR:

1. FIREWALL

Software (ou hardware) que funciona como uma barreira, controlando, bloqueando ou restringindo o acesso às portas, exceto àquelas definidas como públicas

1. VPN (VIRTUAL PRIVATE NETWORK) Rede Privada Virtual

As VPNs criptografam seu tráfego de Internet e disfarçam sua identidade online. As vantagens em utilizar VPNs são:

• Ter acesso seguro a um servidor remoto;

• Criar conexões entre computadores remotos e;

• Apresentar a conexão como se fosse uma rede privada local.

1. BACKUP

Significa cópia de segurança. Essas cópias são guardadas como garantia, a fim de armazenar todos os dados sem nenhuma modificação, caso o arquivo principal precise ser restaurado ou tenha seus dados perdidos

MODELO PARA PROTEÇÃO DE SENHA PARA UM PERFIL

Funções de Hash

LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

“A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.”

Em outras palavras:

A LGPD trata de todos os tipos de dados pessoais, com o objetivo de proteger os direitos fundamentais das pessoas naturais. Ela incide sobre as regras para coleta, tratamento e compartilhamento de informações pessoais. Não importa se seu RG está no cadastro federal de pessoas naturais ou no banco de dados do mercado do seu bairro: todas as organizações têm responsabilidades e deveres ao manipular e guardar informações pessoais

VALIDAÇÃO DE SISTEMAS

REQUISITOS

o levantamento de requisitos é a etapa do desenvolvimento de sistemas de informação responsável por identificar e modelar as necessidades do negócio a serem atendidas pelos sistemas de informação, e é, portanto, uma atividade cada vez mais relevante em um dinâmico cenário

REQUISITOS FUNCIONAIS

especifica o que o sistema deve fazer. É o comportamento de uma função ou de um componente no sistema.

A tabela a seguir mostra uma lista com requisitos funcionais, com identificador e nome.

RF1 – Adicionar usuário pessoa física

RF2 – Modificar usuário pessoa física

RF3 – Consultar usuário pessoa física

RF4 – Apagar usuário pessoa física

RF5 – Adicionar usuário pessoa jurídica

RF6 – Modificar usuário pessoa jurídica

RF7 – Consultar usuário pessoa jurídica

RF8 – Apagar usuário pessoa jurídica

Você pode detalhar um requisito com a seguinte estrutura:

• Identificador: RF1

.• Nome: Cadastrar uma publicação no feed de notícias.

• Data de criação: 21/06/2021.

• Autor: Kátia (profissional que especificou a RF).

• Data da última alteração: 21/06/2021.

• Versão: 1 (a versão inicial é a 1).

• Prioridade: Essencial, importante ou desejável.

• Descrição: Descrição detalhada sobre a funcionalidade de cadastrar uma publicação no feed de notícias

REQUISITOS NÃO FUNCIONAIS

Estão associados a características que permitirão que o software funcione adequadamente, não necessariamente associadas a funções do sistema de modo direto.

Ex.: Tempo de resposta, Backup, Interface gráfica amigável, etc..

CATEGORIAS (NÃO FUNCIONAIS)

* PRODUTO FINAL (Comportamento do software, tempo de resposta, consistência e velocidade de execução)
* EXTERNOS (Não relacionados diretamente ao produto: Ex. LGPD)
* ORGANIZACIONAIS (Políticas da empresa : Infraestrutura e criptografia)

**SOFTWARE REQUIREMENT SPECIFICATIONS (SRS)**

Documento que descreve as necessidades de negócio, os tipos de usuários, as especificidades do produto e como ele deverá funcionar. Esse documento é utilizado como base para estabelecer um acordo entre contratantes e contratados.

Utilidade

• Viabilizar informações a todos os membros da equipe, fornecendo um roteiro e uma descrição sobre o sistema proposto.

• Compartilhar informações com diferentes equipes, visando garantir que os requisitos sejam atendidos e as decisões sejam baseadas em sua análise.

Conteúdo

• Objetivo: o objetivo e as definições do software/sistema que está sendo desenvolvido, bem como seu histórico;

• Descrição geral: regras de negócio e descrição das funcionalidades do produto;

• Requisitos: atributos e requisitos funcionais do sistema.

Um documento SRS inclui, ainda, os seguintes elementos:

Desempenho do software em uma situação de produção

Requisitos não funcionais

Interfaces externas ou como o software irá interagir com o hardware ou outro software ao qual ele deve se conectar

Restrições de design ou limitações do ambiente em que o software será executado

VALIDAÇÃO DO SISTEMA

A verificação de software é um processo de avaliação para garantir que o sistema cumpre os requisitos funcionais e não funcionais especificados. A validação é o processo que garante que o sistema atende às necessidades do usuário

* VERIFICAÇÃO

Inlcui a aplicação de testes para verificar erros

* VALIDAÇÃO

Verifica se as expectativas do cliente estão sendo atendidas

ATRIBUTOS DA VALIDAÇÃO:

Validade

O sistema é valido quando atende às necessidades do usuário e descreve todas as demandas de interesse. Essas demandas incluem requisitos funcionais e de desempenho, restrições e atributos, além de interfaces externas.

Consistência

Um sistema é consistente se nenhum subconjunto de requisitos entra em conflito com os demais requisitos do sistema.

Ambiguidade

Os requisitos são objetivos e não têm ambiguidade.

RASTREABILIDADE

Processo de identificar e documentar a relação direta entre os requisitos e entre outros componentes do sistema.

A rastreabilidade permite:

• Analisar o impacto de uma mudança de requisito.

• Analisar a complexidade de mudança.

• Estimar custos.

• Estimar variações em cronogramas.

• Verificar se a solução tem a especificação correta.

• Gerenciar riscos associados a custos e a prazos, possibilitando a criação de estratégias para mitigar riscos

CARACTERÍSTICAS DE REQUISITOS DE HARDWARE E SOFTWARE PARA UM SISTEMA WEB

1. Servidor Web
2. Um computador
3. Linguagem ou protocolo (HTTP, FTP, SMTP, POP OU IMAP)
4. Regras de Segurança
5. Firewall, VPN
6. Balanceamento de carga
7. Recuperação
8. Serviço de Banco de Dados
9. Escalabilidade
10. Performance
11. SERVIDOR

* REDE LAN:
* São redes restritas a um local físico, que pode ser um escritório, uma empresa, um prédio etc. Os servidores de rede locais são responsáveis por atender às requisições dos computadores clientes da rede local e por executar softwares administrativos e banco de dados,
* REDE WAN:

São redes que abrangem uma área física maior, como uma cidade, um estado etc. Os computadores servidores que atendem a requisições via internet de diferentes localidades, geralmente, ficam instalados em data centers e prestam serviços como:

• hospedagem de sites;

• distribuição de e-mails;

• propagação de conteúdo em áudio e vídeo

TIPOS DE SERVIDOR

1. Arquivos (File Server)
2. Banco de Dados (Database servers)
3. Aplicação (Application Servers)
4. Mídia (Mídia Servers)
5. Emails (Mail Servers)
6. Web (Web Servers)
7. BackUp (Back-up Servers)
8. Em Nuvem (Cloud Computing)

SERVIDOR EM NUVEM (CLOUD COMPUTING)

1. Capacidade de abrangência

Dimensionamento elástico está relacionada ao fornecimento da quantidade adequada de recursos de TI (assim como maior ou menor potência de computação, armazenamento e largura de banda) sempre que necessário e na localização geográfica correta.

1. Confiabilidade

A computação em nuvem facilita e reduz os custos de backup de dados, recuperação de desastre e continuidade dos negócios, já que os dados podem ser espelhados em diversos sites redundantes na rede do provedor em nuvem.

1. Custo

Elimina o gasto de capital com a compra de hardware e software e com a realização de configuração e execução de data centers locais, incluindo racks de servidores, disponibilidade constante de eletricidade e refrigeração.

1. Desempenho

Os serviços de computação em nuvem são executados em uma rede mundial de data centers seguros, que são atualizados regularmente com a mais recente geração de hardware de computação, de modo rápido e eficiente.

1. Segurança

Muitos provedores em nuvem oferecem um amplo conjunto de políticas, tecnologias e controles que fortalecem sua postura geral de segurança, ajudando a proteger os dados, os aplicativos e a infraestrutura contra possíveis ameaças.

1. Velocidade

A maior parte dos serviços de computação em nuvem é fornecida por autosserviço e sob demanda, para que até grandes quantidades de recursos de computação possam ser provisionadas em minutos. Normalmente, bastam alguns cliques para que a empresa tenha flexibilidade e alívio da pressão para elaborar um planejamento de capacidade

HOSPEDAGEM

Servidores DEDICADOS

O computador é dedicado inteiramente para o cenário da organização.Normalmente, sites de alto tráfego, como portais de conteúdo muito visitados, e sistemas online de vendas, como o CRM5, exigem um servidor dedicado, pois ele é mais seguro, escalável e apresenta melhor perfomance

Servidores COMPARTILHADOS

Compartilha os recursos de hardware com outras empresas, pessoas ou organizações. A hospedagem compartilhada é popular, porém limitada.