

CODIFICAÇÃO BACK-END - SA3

SENAI

SUMÁRIO

| | |
|---|----|
| PARA COMEÇAR | 3 |
| SITUAÇÃO-PROBLEMA | 4 |
| DESAFIO 1..... | 4 |
| SEGURANÇA DA INFORMAÇÃO | 5 |
| PILARES..... | 6 |
| PRÁTICAS DE SEGURANÇA | 8 |
| CONFIGURAÇÕES DE SEGURANÇA NO SERVIDOR..... | 10 |
| NA PRÁTICA | 12 |
| LEI GERAL DE PROTEÇÃO DE DADOS | 14 |
| NESTE DESAFIO..... | 15 |
| DESAFIO 2..... | 16 |
| REQUISITOS | 16 |
| SOFTWARE REQUIREMENTS SPECIFICATION (SRS) | 20 |
| VALIDAÇÃO DE SISTEMAS | 22 |
| RASTREABILIDADE..... | 23 |
| NESTE DESAFIO..... | 25 |
| DESAFIO 3..... | 26 |
| SISTEMA WEB | 27 |
| SERVIDOR | 30 |
| TIPOS DE SERVIDOR | 32 |
| HOSPEDAGEM | 35 |
| NESTE DESAFIO..... | 36 |
| PARA CONCLUIR..... | 37 |
| REFERÊNCIAS | 38 |
| CRÉDITOS..... | 39 |

PARA COMEÇAR

Este material aborda conceitos relacionados à **segurança da informação, documentação de implementação, validação e implementação de sistemas.**

Esperamos que você desenvolva, no decorrer de seus estudos, as seguintes capacidades:

- Aplicar técnicas para segurança da informação;
- Configurar políticas de segurança no servidor;
- Aplicar procedimentos técnicos para documentação da implantação, conforme exigências de rastreabilidade;
- Reconhecer as características de hardware e software requeridas para o sistema web;
- Reconhecer as etapas do processo de implantação do sistema web;
- Aplicar, no servidor, as configurações requeridas pelo sistema web;
- Aplicar procedimentos de validação do sistema web;
- Aplicar procedimentos técnicos para instalação, migração e atualização do sistema web.

Para desenvolver tais capacidades, você deverá estudar os seguintes temas:

- **Segurança da informação:**
 - Políticas de segurança da informação;
 - Criptografia;
 - Perfis de usuários;
 - Proteção de dados pessoais.
- **Documentação de implantação.**
- **Validação de sistemas:**
 - Escolha da estratégia de validação de software;
 - Aspectos funcionais e não funcionais do software.
- **Implantação de sistemas:**
 - Características de hardware e software;
 - Configurações de servidores;
 - Parametrização de protocolos.

O estudo desses temas será necessário para que você resolva a situação-problema a seguir. Então, avance para conhecê-la.

SITUAÇÃO-PROBLEMA

A **Insurity** é uma consultoria que fornece serviços de segurança de tecnologia da informação para empresas, visando aumentar a confiabilidade e a proteção dos dados de seus contratantes. Ela atua implementando configurações e regras de segurança e desenvolve a documentação de processos.

A **Hatomus**, empresa que oferece cursos online na área de desenvolvimento de software, não possui regras de segurança da informação para sua plataforma de divulgação de cursos de ensino a distância. Com as novas leis de políticas de uso de dados, a Hatomus contratou a Insurity para aplicar essas novas regras de segurança, considerando os aspectos visuais e funcionais da aplicação, para garantir a viabilidade de uso dessa plataforma.

Você, como programador Back-End da Insurity, ficou responsável por essa demanda. Para isso, deverá resolver os seguintes desafios:

Clique nos botões a seguir para conhecê-los:

Desafio 1

Aplicar procedimentos de segurança para a validação de usuários e restrição de acessos..

Desafio 2

Desenvolver a documentação, conforme as exigências de rastreabilidade.

Desafio 3

Aplicar procedimentos para validar e implantar o sistema proposto.

DESAFIO 1

Nesta etapa, você deverá resolver o desafio 1:

- Aplicar procedimentos de segurança para a validação de usuários e restrição de acessos.

Para isso, você estudará os seguintes conteúdos:

- Segurança da informação;
- Políticas de segurança da informação;
- Criptografia;
- Perfis de usuários;
- Proteção de dados pessoais.



SEGURANÇA DA INFORMAÇÃO

Segundo a definição do Computer Security Resource Center,¹ a Segurança da Informação, também conhecida como infosec, é:

"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability."

Na tradução literal:

"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."

¹ Centro de Recursos de Segurança Informática.

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.

Você sabia?



Diferença entre dados e informações

Dados são os recursos isolados que não possuem valor relevante para a tomada de decisão ou o embasamento de conclusões. Por exemplo, em um determinado mês, 100 pessoas visitaram um site; isso é um dado. A Informação, por sua vez, é a organização dos dados com o objetivo de ter compreensão sobre um determinado contexto. Os dados, quando organizados e processados, tornam-se informações úteis. Por exemplo, em um determinado mês, 100 pessoas visitaram um site e, no mês seguinte, após a divulgação do site em redes sociais, esse número aumentou para 160 pessoas. Podemos concluir que houve um aumento de 60% no número de acessos.

Portanto, um dado é um recurso que compõe uma informação.

PILARES

A segurança da informação está fundamentada em alguns pilares, que podem variar entre 3 a 5 (dependendo da literatura), para garantir seu objetivo. Neste desafio, você vai conhecer os pilares: disponibilidade, confidencialidade e integridade.



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).

Exemplo de comprometimento da disponibilidade: você precisa acessar um determinado sistema para concluir e fechar a folha de pagamento do mês e o sistema não está disponível.

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.

Exemplo de comprometimento da integridade: ao enviar um e-mail para o departamento de compras com um desconto de 5%, alguém intercepta o e-mail e remove ou altera o desconto.

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.

Exemplo de comprometimento de confidencialidade: você não pode divulgar uma informação que contenha dados internos de vendas ou números referentes ao crescimento da empresa.

Saiba mais



A norma ISO 27001:2013 estabelece os requisitos para implementar, manter e melhorar, continuamente, um sistema de gestão de segurança da informação. Acesse o link: <https://www.27001.pt/index.html> e saiba mais

PRÁTICAS DE SEGURANÇA

As práticas de segurança envolvem ações (técnicas ou físicas) individuais ou coletivas para garantir a segurança e menor vulnerabilidade a situações adversas, como políticas de segurança, controles de acesso lógicos e físicos, auditórias e criptografia.

POLÍTICAS DE SEGURANÇA

Os dados das empresas são considerados ativos importantes e imensuráveis. A política de segurança da informação (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). Exemplos:

- 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

A segurança da informação não visa somente restringir o acesso e a visualização de uma informação no sistema, mas também envolve a proteção física. Nesse sentido, o controle de acesso 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

O 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

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

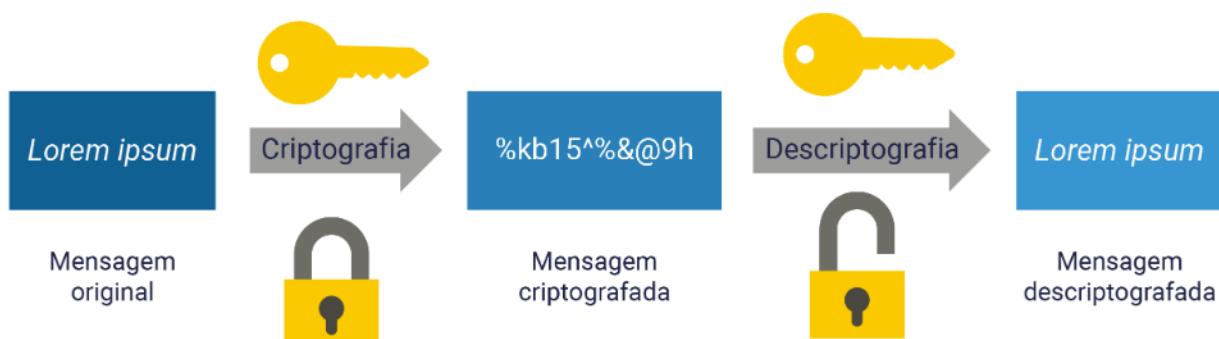
Auditorias

Trata-se de uma 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

Do grego *kriptos* (oculto) e *grafo* (escrita), a 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, conforme mostra o esquema abaixo. Dessa maneira, consegue-se manter os três atributos básicos da segurança da informação (confiabilidade, integridade e disponibilidade).

As assinaturas digitais em documentos são exemplos de utilização da criptografia para a proteção das informações.



PDF

Acesse seu material complementar e entenda como uma chave assimétrica é gerada

Arquivo: 01_chave_assimetrica.pdf

Saiba mais



Codificar funciona como traduzir uma mensagem de um idioma para outro. Quem conhece o segundo idioma poderá entender a mensagem final. Criptografar, por sua vez, é o processo de transformação da mensagem em um código que somente poderá ser lido depois de descriptografado com a chave correta. Esse processo é feito por meio de algoritmos.

Acesse o link: <https://docs.microsoft.com/pt-br/sql/relational-databases/security/encryption/choose-an-encryption-algorithm?view=sql-server-ver15> para saber mais sobre criptografia em banco de dados.

As moedas digitais, ou criptomoedas, utilizam a criptografia como elemento de segurança. A tecnologia que está por trás das transações que envolvem criptomoedas, como o Bitcoin, é a Blockchain.

Aproveite e faça, gratuitamente, o curso ofertado pelo SENAI-SP "Desvendando a Blockchain". Para mais informações, acesse: <https://online.sp.senai.br/curso/87241/483/desvendando-a-blockchain>

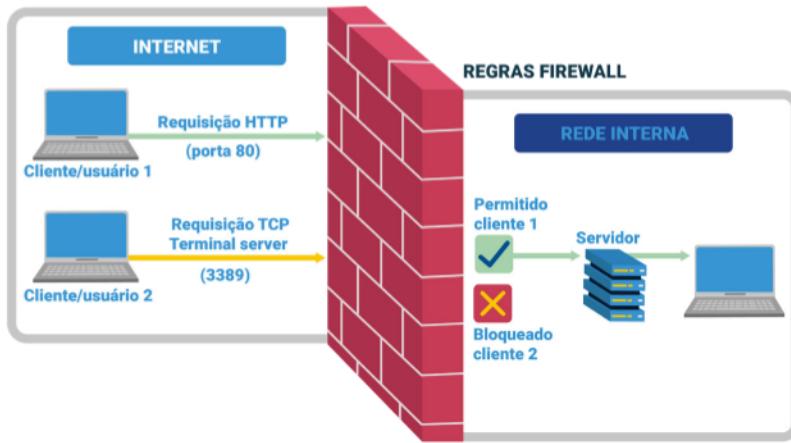
CONFIGURAÇÕES DE SEGURANÇA NO SERVIDOR

Garantir a segurança do servidor de uma organização é primordial, pois protege seus dados e sistemas de pessoas mal-intencionadas que podem utilizá-los em benefício próprio ou para a venda de informações. Para evitar falhas de segurança, que podem acarretar tanto prejuízos financeiros quanto de imagem da organização, a configuração de firewalls, VPNs e backups são mais algumas das medidas aplicadas na proteção de sistemas.

Firewall

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

O esquema a seguir mostra como funciona um firewall:



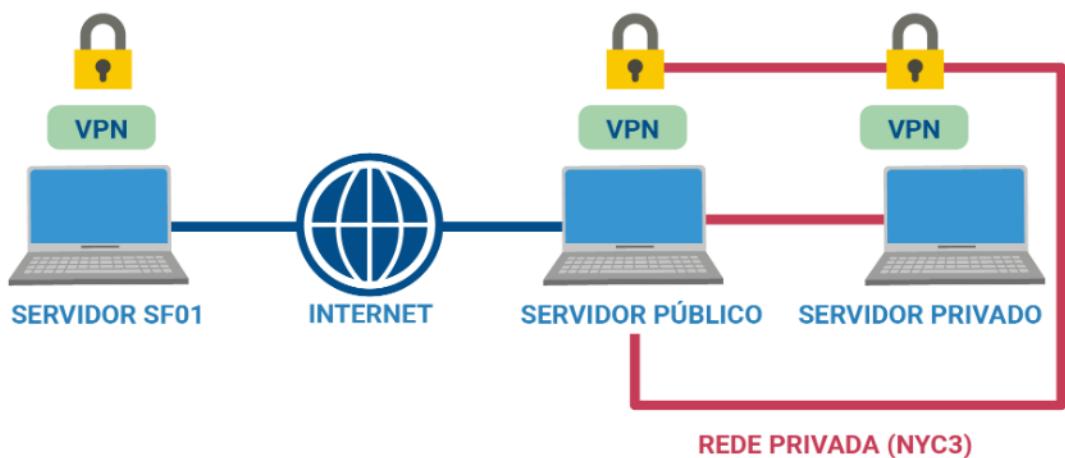
VPN

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.

A seguir conheça como a Rede Privada Virtual (VPN) é estruturada:



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.

Independentemente do tipo, o backup, assim como as medidas já citadas (políticas, controle de acesso, auditoria, criptografia, firewalls e VPNs), é uma prática recomendada para assegurar que dados e informações sejam preservados.

Saiba mais



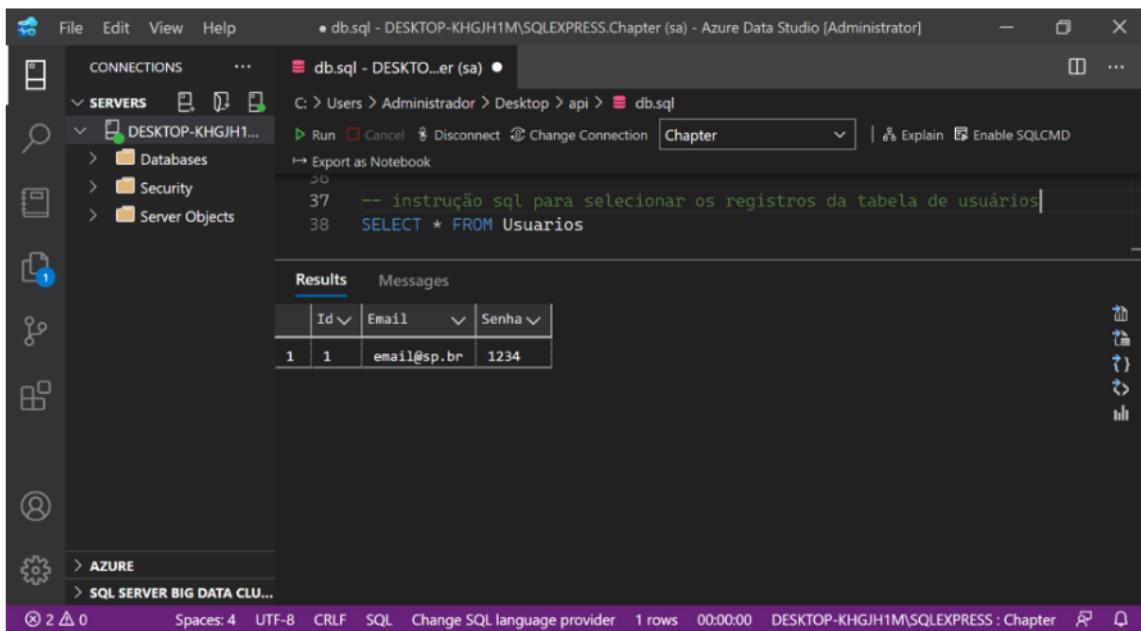
Acesse o link: <https://canaltech.com.br/mercado/Sony-e-multa-em-250-mil-libras-por-vazamento-de-dados-pessoais-em-2011/#:~:text=A%20Sony%20foi%20multada%20nesta,online%20do%20Playstation%20em%2011> para saber mais sobre como falhas de segurança podem afetar uma empresa ou instituição.

NA PRÁTICA

Para assegurar que as informações de usuário e senha não estarão facilmente disponíveis para leitura na base de dados da aplicação, podemos melhorar a segurança implantando modelos que validem usuários e restrinjam acessos. A seguir, conheça como implementar um modelo para proteção de senha de perfil.

PROTEÇÃO DE SENHA DE PERFIS

Você pode armazenar senhas, mas se uma pessoa não autorizada invadir a sua base de dados, ela pode consultar e selecionar os registros e acessar informações como e-mail e senha dos usuários cadastrados. A seguir, conheça um exemplo de código, em que, na linha 38, a instrução **SELECT * FROM Usuarios** está selecionando todos os usuários da base de dados. Os usuários possuem um identificador (Id), e-mail e senha; contudo, ao selecionar diretamente esses registros da base, verifica-se que as senhas estão disponíveis para leitura.



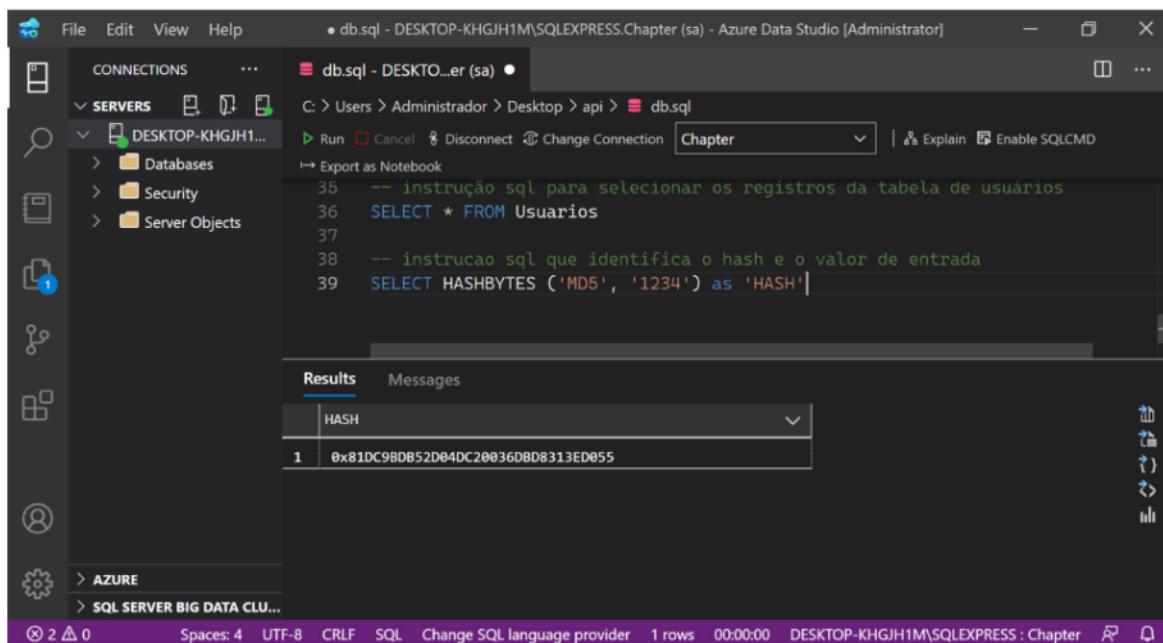
A screenshot of the Azure Data Studio interface. The left sidebar shows connections, servers (DESKTOP-KHGJH1M), databases, security, and server objects. The main area shows a SQL script window with the following code:

```
37 -- instrução sql para selecionar os registros da tabela de usuários
38 SELECT * FROM Usuarios
```

The results pane shows a table with three columns: Id, Email, and Senha. There is one row with values: 1, email@sp.br, and 1234.

Você pode utilizar funções criptográficas para criptografar as senhas e outros dados e informações, se necessário. Algumas funções, como **ENCRYPTBYPASSPHRASE** e **DECRYPTBYPASSPHRASE**, armazenam essa informação e recuperam o valor salvo original.

Quanto maior a segurança do algoritmo, menor a chance de uma informação ser "quebrada" ou recuperada indevidamente. Um exemplo é o **HASHBYTES**. Na imagem, estamos selecionando o resultado do **hash** gerado, a partir do algoritmo de **hash** a ser utilizado e do valor informado.



A screenshot of the Azure Data Studio interface, similar to the previous one. The left sidebar shows connections, servers (DESKTOP-KHGJH1M), databases, security, and server objects. The main area shows a SQL script window with the following code:

```
35 -- instrução sql para selecionar os registros da tabela de usuários
36 SELECT * FROM Usuarios
37
38 -- instrucao sql que identifica o hash e o valor de entrada
39 SELECT HASHBYTES ('MD5', '1234') as 'HASH'
```

The results pane shows a table with one column labeled HASH. There is one row with the value: 0x81DC98DB52D04DC20036DBD8313ED055.

Você sabia?

As **funções de Hash** têm como objetivo gerar valores que são praticamente impossíveis de serem revertidos, sendo muito utilizadas para ocultar senhas e em assinaturas digitais.



LEI GERAL DE PROTEÇÃO DE DADOS

O governo federal define o escopo da Lei Geral de Proteção de Dados, também conhecida como LGPD, do seguinte modo:

“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.

Dica!

O SENAI-SP oferece gratuitamente o curso “Privacidade e proteção de dados (LGPD)”. Para se inscrever, acesse: <https://online.sp.senai.br/6884/privacidade-e-protecao-de-dados-lgpd>



A prática de proteção de dados envolve tanto o lado do desenvolvimento (elaboração de códigos e configurações segurança) quanto o lado comercial/negócios, para que

a organização não sofra sanções legais, como multas e suspensão do site ou serviço prestado.

Neste sentido, os desenvolvedores possuem papel importante a desempenhar, a fim de contribuir para o cumprimento das diretrizes da LGPD, no que se refere à prevenção de perdas ou exposição de dados e informações e à captura de dados desnecessário.

NESTE DESAFIO...

SITUAÇÃO-PROBLEMA | DESAFIO 1



Você estudou que a segurança da informação está fundamentada nos pilares da disponibilidade, confidencialidade e integridade. Aprendeu também que, para garantir esses pilares, existem diversas práticas, como políticas, controle de acessos físicos e lógicos, auditorias, criptografia e configurações de segurança no servidor que, por sua vez, envolvem firewall, VPN e backup, bem como proteção de senhas e perfis.

Além disso, você estudou também que, com a implementação da Lei Geral de Proteção de Dados Pessoais, os desenvolvedores possuem papel importante a desempenhar, sobretudo na elaboração de códigos e configurações de segurança, visando a prevenção de perdas, a exposição de dados e informações e a captura de dados desnecessários, para que a organização não sofra sanções legais, como multas e suspensão do site ou serviço prestado.

NO PRÓXIMO DESAFIO...

Você conhecerá como desenvolver a documentação, conforme as exigências de rastreabilidade.

DESAFIO 2

No desafio 1, você conheceu procedimentos de segurança para a validação de usuários e restrição de acessos.

Nesta etapa, você deverá resolver o desafio 2:

- Desenvolver a documentação, conforme as exigências de rastreabilidade.

Para isso, você estudará os seguintes conteúdos:

- **Validação de sistemas:** aspectos funcionais e não funcionais do software;
- Documentação de implantação e rastreabilidade.



REQUISITOS

Quando falamos em sistemas, aplicativos e processos de desenvolvimento de software, é importante lembrar que existem metodologias, técnicas, ferramentas e muitos outros recursos que auxiliam desde o levantamento de uma necessidade de negócio ou de um usuário até a própria criação do negócio em si.

O **levantamento de requisitos** é uma das técnicas aplicadas para se ter clareza sobre o que será desenvolvido em um projeto.



Fonte: Pexels

O que são requisitos?

Imagine que, para você construir uma casa, é necessário ter a dimensão do espaço e a visualização da aparência final; por exemplo: qual é o tamanho dos cômodos? Será feita de tijolo? Qual será a cor da parede? Além disso, antes de iniciar, você precisa pensar em todos os detalhes internos da casa e que precisarão existir para que ela cumpra seu objetivo. Esses são os requisitos, ou seja, maneiras formais de especificar os seus desejos para o responsável pela construção, que, por sua vez, apresentará a você uma planta baixa como sendo o documento final da obra.

Com o desenvolvimento de sistemas, softwares ou sites não é diferente. As informações, os objetivos, os padrões, as solicitações e as especificações são os requisitos; detalhá-los torna o objetivo mais claro e o tempo de entrega do produto (sistema, software ou site) mais preciso, pois as necessidades de implementação já estarão conhecidas.

Segundo Azevedo Jr e Campos (2008), 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.

É importante documentar os requisitos para manter o registro de tudo o que foi solicitado pelo cliente, bem como do que foi implementado.

Usualmente, os requisitos são divididos em **funcionais e não funcionais**.

Requisitos Funcionais (RF)

Esse tipo de requisito 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.

| Requisitos funcionais (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

Os requisitos não funcionais estão associados a características que permitirão que o software funcione adequadamente, não necessariamente associadas a funções do sistema de modo direto. A seguir, conheça três exemplos de requisitos não funcionais:

Banco de Dados

As regras de backup de um sistema não impactam diretamente suas funcionalidades, mas sua confiabilidade, integridade e consistência dos dados.

Tempo de resposta

Ao solicitar uma informação ao sistema, o número de ações para atender à solicitação deve ser o menor possível.

Interface famigável

Um software pode conter as funções e os componentes esperados, mas sua interface não proporcionar a melhor experiência, tanto em relação à compreensão quanto à utilização.

Há uma diversidade de requisitos; inclusive, você pode encontrá-los nas categorias (dependendo da literatura) **produto final, organizacionais e externos**.

A seguir conheça mais sobre cada categoria:

Produto final

Comportamento do software:
tempo de resposta,
consistência e
velocidade de
execução.

Externos

Não relacionados diretamente ao produto: LGPD e políticas de segurança.

Organizacionais

Políticas da empresa:
infraestrutura e
criptografia.

Para compreender os requisitos funcionais e não funcionais, vamos utilizar dois tipos de exemplos: as redes sociais e os aplicativos de transporte privado.

Redes sociais

Um dos requisitos similares entre as redes sociais é a publicação de imagens em seu perfil (não precisa entrar no detalhamento de data de publicação, curtidas e descrição). Esse é um requisito funcional de uma ação que o usuário realiza. O

sistema performa e gera um resultado esperado. Um outro exemplo de requisito funcional é visualizar as imagens de amigos e páginas que você segue. Um requisito não funcional, baseado nesse exemplo, é a espera do retorno da lista ao solicitar mais imagens para visualizar. Imagine que você terminou de ver as 10 postagens de seu colega e deseja solicitar mais 10. Se essa espera for muito longa, você provavelmente vai para outra rede social.

Aplicativos de transporte privado

Assim como acontece entre aplicativos de transporte privado, um requisito funcional é a capacidade do aplicativo identificar sua localização, solicitar e analisar o custo prévio de uma viagem. Já um requisito não funcional seria a capacidade do aplicativo retornar a resposta do motorista mais próximo, para atender à sua solicitação em menos de 15 segundos. Imagine que você esteja em um local desconhecido e deseja ter uma breve resposta do aplicativo. Se ele demorar 5 minutos para responder sua solicitação, você continuaria utilizando? Claro que outros recursos como sua localização, dia, horário e quantidade de carros disponíveis afetariam sua usabilidade, mas, em um cenário em que todos esses eventos possuem eficácia, a resposta do aplicativo deve ser breve.

SOFTWARE REQUIREMENTS SPECIFICATION (SRS)

A especificação de requisitos de software (do inglês, Software Requirements Specification - SRS) é um 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. Os boxes a seguir mostram sua utilidade e os itens principais que devem constar em seu conteúdo.

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:

Elementos de documentos SRS

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

Não se preocupar em determinar e documentar adequadamente os requisitos pode ocasionar a construção de um sistema que não atende às especificações dos clientes, gerando problemas quanto à usabilidade do produto e, consequentemente, acarretando retrabalhos futuros.

Dica!



Acesse o seu material complementar e faça o download de um template para documento SRS. Arquivo template_SRS.pdf

VALIDAÇÃO DE SISTEMAS

Após implementar o projeto, a partir da especificação dos requisitos, é hora de validá-lo. O processo de validação, em linhas gerais, deve verificar e validar o que o sistema entrega para que o usuário consiga realizar as ações que deseja.

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.

A verificação inclui a realização de testes para encontrar erros, enquanto a validação verifica se as expectativas do cliente estão sendo atendidas. Nesse momento, são identificados alguns atributos, como validade, consistência e ambiguidade.



Validade

O sistema é válido 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.

Portanto, validar e verificar se todos os requisitos estão sendo correspondidos são ações imprescindíveis para a garantia da qualidade e sustentabilidade do projeto. Uma falha encontrada tardeamente pode ocasionar sérias consequências, trazendo prejuízos à organização.

RASTREABILIDADE

Durante o desenvolvimento de um sistema, podem ocorrer alterações no escopo do projeto, acarretando mudanças de requisitos. Além disso, no mundo do desenvolvimento, em razão do avanço do mercado tecnológico, novas tecnologias e demandas por novos sistemas surgem a todo momento.

Essas mudanças, estejam elas relacionadas ao contexto de negócio, às técnicas ou ao escopo, impactam diretamente o ciclo de desenvolvimento, acarretando alterações nos requisitos existentes, gerando novas demandas e aumentando ou diminuindo o tempo de desenvolvimento e a estimativa de custo do projeto.

Neste sentido, é necessário desenvolver documentos de rastreabilidade, visando conhecer a trajetória de um determinado objeto e quais foram as edições ou modificações realizadas durante o ciclo de desenvolvimento e após sua implementação.

Importante!

A **rastreabilidade** é, portanto, o 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*² riscos.

Exemplo de documentação de Rastreabilidade

A documentação de rastreabilidade parte de uma matriz que ajuda a garantir que os requisitos adicionam valor de negócio por meio da sua ligação aos objetivos do projeto, conforme mostra o exemplo a seguir:

Matriz de rastreabilidade

| Nome do Projeto: | | | | | | | |
|------------------|------------|-------------------------|-----------|----------|-------------------|-----------------|-------|
| Centro de custo: | | | | | | | |
| Descrição: | | | | | | | |
| Nº | Requisitos | Necessidades de negócio | Objetivos | Entregas | Design de produto | Desenvolvimento | Teste |

Fonte: Adaptado de *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*, 2014.

Os atributos associados a cada requisito devem ser registrados na matriz, para auxiliar na definição de informações-chave a respeito do requisito.

² Tornar mais brando, em nosso caso, agir de maneira preventiva para minimizar impactos e efeitos de um problema.

NESTE DESAFIO...

Situação-Problema | Desafio 2



Neste desafio, você estudou que definir os requisitos funcionais e não funcionais é essencial para que o projeto se desenvolva com plenitude.

Você estudou também a importância da documentação de rastreabilidade para estar preparado para possíveis mudanças e adaptações no decorrer do desenvolvimento.

No próximo desafio...

Você estudará procedimentos para validar e implementar sistemas.

DESAFIO 3

A proposta de um sistema pode impactar diretamente a escolha do servidor e dos serviços necessários para o atendimento do objetivo desse sistema, ou vice-versa. O custo de um recurso para hospedar ou utilizar um serviço online, por exemplo, pode impactar a escolha de uma tecnologia.

A partir de agora, você estudará um pouco desse contexto: o que é um sistema web, quais são suas características e como realizar uma publicação e um serviço online.

Nesta etapa, você deverá resolver o desafio 3:

- Aplicar procedimentos para validar e implantar o sistema proposto.

Para isso, você estudará os seguintes conteúdos:

Validação de sistemas:

- Escolha da estratégia de validação de software.

Implantação de sistemas:

- Características de hardware e software;
- Configurações de servidores;
- Parametrização de protocolos.



SISTEMA WEB

Sistemas ou aplicações web são soluções (softwares) disponibilizadas na internet, em que qualquer usuário cadastrado pode acessá-las, por meio de um navegador. Tais sistemas são desenvolvidos para tornar processos (compartilhamento de dados, comunicação etc.) mais simples, rápidos e eficazes.

Conheça, a seguir, duas vantagens que o sistema web oferece:

FLEXIBILIDADE

- Possibilita a utilização em qualquer ambiente com internet;
- Não requerer instalação ou configuração local;
- Não tem dependência direta do sistema operacional.

CUSTO

- Sua atualização não exige tanto custo, pois aplica-se a alteração para todos que a utilizam e não por usuário.

Importante!

Qual é a diferença entre sistema web, aplicativo e site?



Site é um conjunto de páginas web armazenadas em uma pasta num servidor, acessível pela internet por meio de um navegador (Google Chrome, Internet Explorer, Safari etc.), por qualquer pessoa. Um exemplo é o site do SENAI-SP (<https://www.sp.senai.br/>).

Um sistema web é um software hospedado em servidores, também acessível pela internet por meio de um navegador, mas somente por usuários cadastrados, geralmente por meio de um login e uma senha; além disso, há um sistema completo de informações, incluindo um banco de dados. A plataforma Trello é um exemplo de sistema web.

Já um aplicativo é um software que precisa ser instalado em um smartphone para funcionar diretamente no sistema operacional Android, iOS etc.

O infográfico interativo a seguir apresenta a arquitetura de uma aplicação web.



1

O usuário interage com o Front-End e solicita uma pesquisa em um site, por exemplo. O computador do usuário, que pode ser um desktop, table, smartphone etc., é chamado de **cliente**.

2

O Front-End do cliente (usualmente estruturado por meio das linguagens HTML, CSS e JavaScript) faz uma requisição ao Back-End (servidor) pela rede, utilizando, por exemplo, o protocolo HTTP.

3

O Back-End (que contém a lógica do sistema) consulta o banco de dados e devolve a resposta, que é customizada pelo Front-End e apresentada ao usuário. As mensagens de resposta às requisições, geralmente, têm o formato de arquivo XML ou JSON (JavaScript Object Notation), pois ambos apresentam os dados de modo simplificado (no formato texto), o que facilita a manipulação por outras aplicações.

Características de hardware e software requeridas para o sistema web

Resumindo, para funcionarem, os sistemas web exigem:

1. **um servidor web**, uma vez que os sistemas web não possuem instalações físicas nos computadores dos usuários, dependem de um servidor de armazenamento do banco de dados.

2. **um computador** (cliente) conectado ao servidor, para que os usuários realizem solicitações que serão consultadas no banco de dados;

3. **linguagem ou protocolo** padrão, por meio da qual o cliente se comunica com o servidor. Normalmente, utiliza-se o HTTP, mas há outros protocolos envolvidos em aplicações web, como:

- FTP (transmissão de arquivos);
- SMTP (envio de mensagens para um servidor de e-mail);
- POP e IMAP (acesso a mensagens de e-mail eletrônico).

Além disso, há características que também devem ser consideradas na implementação de um sistema web, por exemplo: regras de segurança, firewall, VPN (Rede Privada Virtual), balanceamento de carga (divisão do processamento entre dois ou mais servidores), recuperação após situações ou cenários inesperados (como erro humano ou desastres naturais) e necessidade de serviço de banco de dados. Também é importante pensar em:

- **Escalabilidade:** capacidade do sistema em se adaptar e atender necessidades de crescimento, sem perder qualidade, e com baixo aumento de custos. Por exemplo, uma empresa divulga uma promoção na mídia, logo, espera-se que seus sistemas estejam preparados para o aumento considerável de requisições.
- **Performance:** está relacionada ao desempenho do sistema, como rapidez em que uma requisição realizada pelo cliente é respondida pelo servidor.

Alguns dados devem ser observados:

| |
|---|
| Nome do domínio – www.meusite.com.br |
| Tecnologias envolvidas – é um site estático ou dinâmico? Quais são linguagens utilizadas na construção? |
| Banco de dados para armazenar suas informações |
| Necessidade de banco de dados |
| Número de visitantes por dia/mensais |
| Sistemas operacionais |

Requisitos mínimos de hardware: processador, CPU, memória RAM

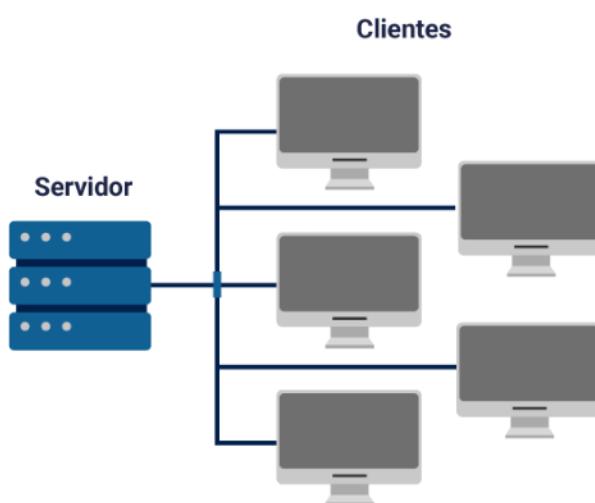
Todas essas características impactam a escolha do servidor que será utilizado. Por exemplo, se a aplicação necessita utilizar um banco de dados *SQL*³, deve-se escolher um servidor que atenda a esse requisito.

SERVIDOR

Um servidor é um computador centralizado, com grande poder de processamento, destinado a prover serviços e informações para outros computadores (clientes), como execução de programas, armazenamento e compartilhamento de arquivos, entre outros. Os usuários podem se conectar ao servidor por meio de uma rede local (LAN) ou remota/web (WAN). Por isso, a arquitetura do sistema web é chamada “cliente-servidor”.

Servidores locais: rede LAN

LAN significa Local Area Network ou Servidores de Rede Locais, em português. 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, conforme mostra a imagem.



³ Structured Query Language, ou Linguagem de Consulta Estruturada, em português; trata-se de uma linguagem padrão para banco de dados relacional.

Servidores Remotos: rede WAN

WAN significa *Wide Area Network* ou Rede de Longa Distância, em português. 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*⁴ conforme mostra a imagem ao lado, e prestam serviços como:

- hospedagem de sites;
- distribuição de e-mails;
- propagação de conteúdo em áudio e vídeo



Fonte: Pixabay

Em máquinas de uso pessoal, você até pode configurar o servidor para disponibilizar pastas e arquivos em rede local ou configurar um ambiente para disponibilizar o sistema web, mas computadores pessoais não foram projetados para realizar uma grande quantidade de transações (requisições do cliente, processamentos do servidor e respostas ao cliente).

É preciso lembrar que um sistema web e outros tipos de compartilhamentos, como o de arquivos e pastas, têm dedicação 24 horas por dia, 7 dias por semana (24/7). Assim, os servidores têm elementos de hardware com maior capacidade, prontos para realizar esses, uma vez que são equipados com um ou mais processadores, bancos de memória, portas de comunicação, softwares e, ocasionalmente, sistema para armazenamento de dados, além de fonte de energia redundante.

⁴ Centro de processamento de dados ou data center é um local onde estão concentrados os sistemas computacionais de uma organização.

Os servidores utilizam sistemas operacionais como Linux, Microsoft Windows Server ou macOS Server, que possuem configurações especiais e projetadas para lidar com uma quantidade massiva de requisições.

TIPOS DE SERVIDOR

Os servidores podem ter diferentes funcionalidades e também podem conter mais de uma funcionalidade dentro de um mesmo escopo. Conheça a seguir alguns tipos:

Servidor de arquivos (*File server*)

Utilizado para o compartilhamento de pastas e arquivos em uma rede local, com definição de acessos a grupos de usuários: comercial, financeiro etc. Centralizando os arquivos, tem a vantagem de realizar cópias e backups de segurança de cada computador da equipe.

Servidor de banco de dados (*Database servers*)

Utilizado para armazenar e gerenciar dados de maneira estruturada. Têm, portanto, duas características: armazenar uma grande quantidade de dados e responder a uma quantidade significativa de solicitações de clientes.

Servidor de aplicação (*Application server*)

Utilizado para executar aplicações corporativas e atender vários usuários em diversas estações de trabalho simultaneamente.

Servidor de mídia (*Media server*)

Utilizado para transmitir conteúdo de áudio ou vídeo via internet, por meio de streaming. Netflix, Amazon Prime e Youtube são exemplos empresas que utilizam esse tipo de tecnologia.

Servidor de e-mails (*Mail server*)

São configurados para armazenar e transferir e-mails.

Servidor web (*Web server*)

Utilizado para hospedar programas que executam aplicações e disponibilizam conteúdo via internet. Os servidores web comuns incluem servidores web Apache, servidores Nginx e servidores Microsoft Internet Information Services (IIS).

Os servidores Apache e Nginx são gratuitos, de código livre (pode ser modificado por qualquer pessoa), disponibilizando páginas, envio de e-mails, mensagens, compras online e diversas outras funções acessíveis pela internet.

Já o IIS permite hospedar um ou vários sites web no mesmo computador, bem como mídias e aplicações streaming; é escalável e distribui arquivos utilizando o protocolo FTP.

Servidor backup (*back-up server*)

Utilizados para realizar cópias de segurança e serviços de recuperação de dados de outros dispositivos computacionais.

Servidor em nuvem

Além dos servidores citados acima, existem os servidores em nuvem. A computação em nuvem é o serviço disponibilizado pela internet, que inclui servidores, armazenamento, bancos de dados, rede, software, análise e inteligência, para oferecer inovações mais rápidas, recursos flexíveis e economias de escala.

Com os servidores em nuvem, a organização pode minimizar os custos associados a compras, gerenciamento de infraestrutura, energia e espaço. Em um ambiente “virtualizado” compartilhado, usualmente, paga-se pela quantidade de espaço utilizado, realizando o balanceamento de carga e utilização.

A seguir, conheça alguns motivos pelos quais as organizações estão adotando os serviços de computação em nuvem:

Capacidade e abrangência

A capacidade de 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.

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.

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.

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.

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.

Velocidade

A maior parte dos serviços de computação em nuvem é fornecida por autoserviço 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.

Saiba mais

Há, ainda, outros tipos de servidores de impressão, DNS, virtuais, proxy, entre outros. Pesquise e conheça mais sobre cada um deles.



Além do tipo de servidor, escolher o serviço de hospedagem correta é essencial, pois interfere na velocidade de carregamento e escalabilidade para o tráfego de dados. A seguir, vamos conhecer os servidores dedicado e compartilhado.

HOSPEDAGEM

O servidor de hospedagem faz todo o trabalho de identificar e converter os dados online em palavras e imagens, assim como distribuir essas informações na internet. Nesse sentido, é um computador de alto desempenho que tem a função de oferecer serviços para outros computadores, podendo ser **dedicado ou compartilhado**.

SERVIDOR DEDICADO

Servidor físico, adquirido ou alugado, utilizado normalmente por grandes organizações para o atendimento de uma necessidade específica, ou seja, 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 performance.

SERVIDOR COMPARTILHADO

O servidor compartilhado, literalmente, compartilha os recursos de hardware com outras empresas, pessoas ou organizações.

A hospedagem compartilhada é popular, porém limitada. É mais recomendado para websites simples, que não exigem aplicações complexas, não possuem muitas requisições e não necessitem de proteções mais seguras, além de escalabilidade e desempenho.

Hospedando e publicando a aplicação no IIS local

Agora, você conhecerá como instalar e configurar um sistema web que disponibiliza como recurso uma lista de livros em formato JSON para visualização.

PDF

Acesse seu material complementar e conheça como realizar a hospedagem e publicação no IIS local.

Arquivo: 01_aplicacao_IIS_v1.pdf

⁵ Sigla para *Customer Relationship Management*, em português, Gestão de Relacionamento com o Cliente.

Publicando na Azure

O sistema local que foi publicado para apresentação também pode ser publicado em ambientes online que possuem recursos. Grandes empresas do mercado atuam nesse cenário, como AWS, Azure e Google. Vamos apresentar a publicação do projeto no ambiente da Azure.

PDF

Acesse seu material complementar e conheça como realizar a publicação no ambiente da Azure

Arquivo: 02_azure_v1.pdf

A seguir faça o download das pastas que contêm os projetos necessários para realizar essa publicação.

Pasta ZIP

Acesse seu material complementar e faça o download do Chapter.FrontEnd para o projeto Front-End.

Arquivo: Chapter.FrontEnd.zip

Acesse seu material complementar e faça o download do Chapter para o projeto Back-End.

Arquivo: Chapter.zip

NESTE DESAFIO...

SITUAÇÃO-PROBLEMA | Desafio 3



Você estudou como os sistemas web oferecem soluções de negócios para tornar processos, como o compartilhamento de dados e de informações, mais simples e baratos.

Estudou também que, para funcionarem, os sistemas web exigem um servidor web. Trata-se de

um computador centralizado que fornece serviços a uma rede de computadores, local ou remota, e tem configurações especiais para lidar com uma quantidade massiva de requisições, próprias dos sistemas web.

PARA CONCLUIR...

Parabéns, você concluiu a etapa de Codificação Back-End!

No desafio 1, você estudou práticas de segurança da informação, como políticas, controles de acesso físicos e lógicos, auditorias, criptografia e configurações de segurança no servidor, o que envolve firewall, VPN e backup, a fim de aplicar procedimentos de segurança para validação de usuários e restrição de acessos.

No desafio 2, conheceu como definir os requisitos funcionais e não funcionais e desenvolver a documentação, conforme as exigências de rastreabilidade.

E, no desafio 3, estudou como aplicar procedimentos para validar e implantar um sistema web.

Continue estudando e aprimorando-se sempre. Até breve e sucesso!

REFERÊNCIAS

ABNT. **ISO/IEC 27000**: Norma internacional de segurança da informação é revisada. Revista eletrônica. Disponível em: <http://www.abnt.org.br/noticias/5777-iso-iec-27000-norma-internacional-de-seguranca-da-informacao-e-revisada>. Acesso em: 12 jun. 2021.

AZEVEDO JR, D.; CAMPOS, R. **Definição de Requisitos de Software Baseada Numa Arquitetura de Modelagem de Negócios**. Produção, São Paulo, v. 18, n.1, p. 026-048, jan-abr 2008.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**/Tribunal de Contas da União. – 4. ed. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.

"IEEE / EIA 12207.1-1997", Guia IEEE / EIA para Tecnologia da Informação - **Processos do ciclo de vida do software** - Dados do ciclo de vida. Online. Disponível em: <https://ieeexplore.ieee.org/document/720574/references#references>. Acesso em: 17 jun. 2021.

MICROSOFT. Azure. **O que é computação em nuvem?**. Online. Disponível em: <https://azure.microsoft.com/pt-br/overview/what-is-cloud-computing/>. Acesso em: 20 jun. 2021.

Créditos

| CONFEDERAÇÃO NACIONAL DA INDÚSTRIA -CNI | SENAI - DEPARTAMENTO REGIONAL DE SÃO PAULO |
|---|--|
| <i>Robson Braga de Andrade</i> Presidente | <i>Ricardo Figueiredo Terra</i> Diretoria Regional |
| DIRETORIA DE EDUCAÇÃO E TECNOLOGIA - DIRET | <i>Cassia Regina Souza da Cruz</i> Gerência de Educação |
| <i>Rafael Esmeraldo Lucchesi Ramacciotti</i> Diretor de Educação e Tecnologia | <i>Izabel Rego de Andrade</i> Supervisão do Centro SENAI de Tecnologias Educacionais |
| SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL – SENAI Conselho Nacional | <i>Claudia Baroni Savini Ferreira</i> Coordenação do Desenvolvimento do Curso |
| <i>Robson Braga de Andrade</i> Presidente | <i>Helena Strada Franco de Souza</i> Elaboração de Conteúdo |
| SENAI - Departamento Nacional <i>Rafael Esmeraldo Lucchesi Ramacciotti</i> Diretor-Geral | <i>Adilson Moreira Damasceno</i> Orientação de Práticas de Educação a Distância |
| <i>Gustavo Leal Sales Filho</i> Diretor de Operações | <i>Paula Cristina Bataglia Buratini</i> Coordenação da Produção do Curso |
| SENAI – DEPARTAMENTO NACIONAL UNIDADE DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA – UNIEP | <i>Cristina Yurie Takahashi</i> <i>Katya Martinez Almeida</i> Design Educacional |
| <i>Felipe Esteves Morgado</i> Gerente Executivo | <i>Luana Dorizo de Melo</i> Diagramação |
| <i>Luiz Eduardo Leão</i> Gerente de Tecnologias Educacionais | <i>Cleriston Ribeiro de Azevedo</i> <i>Fabiano José Moura</i> <i>Juliana Rumi Fujishima</i> Ilustrações |
| <i>Anna Christina Theodora Aun de Azevedo Nascimento</i> <i>Adriana Barufaldi</i> <i>Bianca Starling Rosauro de Almeida</i> <i>Laise Caldeira Pedroso</i> Coordenação Geral de Desenvolvimento dos Recursos Didáticos Nacionais | <i>Camila Ciarini Dias</i> Produção e Edição de Vídeos |
| | <i>Rafael Santiago Apolinário</i> Programação |
| | <i>Aldo Toma Junior</i> Web Design |