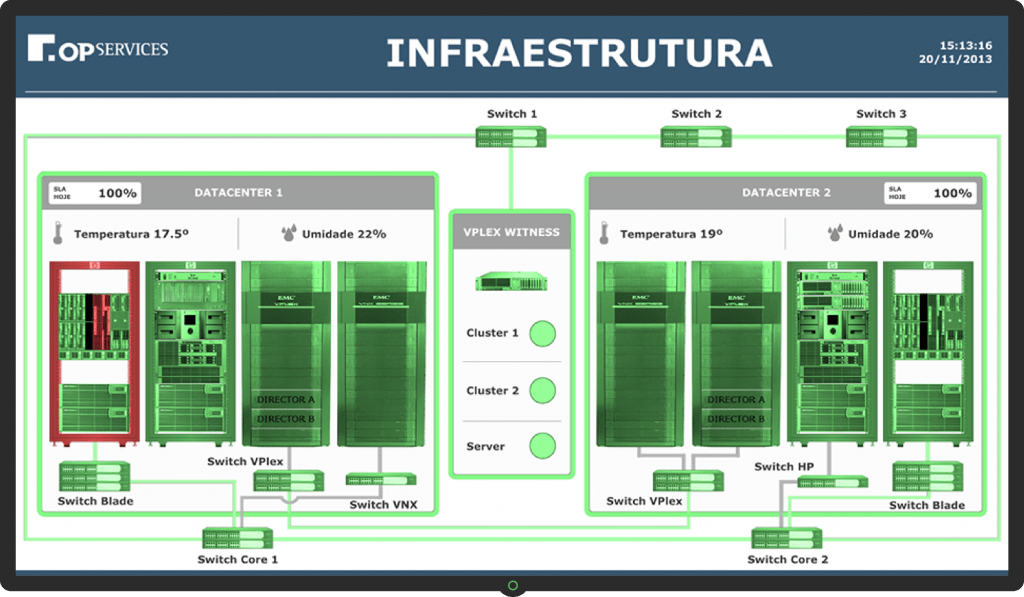
**UC – Sistemas Computacionais e Segurança – Atividade 00**



1. **Administração e Configuração de Servidores:**

**Aplicação:** O administrador da rede/servidores implementa políticas de backup regulares para garantir que os dados estejam seguros e possam ser recuperados em caso de falhas de hardware, desastres ou ataques cibernéticos.

**Exemplo:** Um funcionário responsável pelos backups da rede da empresa realiza backups híbridos onde ele utiliza um backup dedicado no servidor da empresa e utiliza do recurso de backup em nuvem (AWS, OneDrive, Google Cloud) para ter versatilidade, praticidade e segurança da rede, tendo ampla variedade e com isso maior garantia da efetividade em manter os dados intacto.



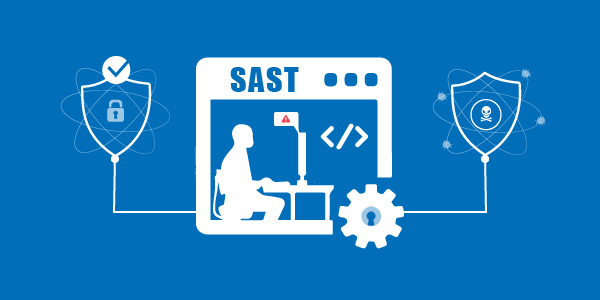
1. **Gerenciamento de Redes e segurança:**

**Aplicação:**

Vigilância contínua da rede para identificar irregularidades/intrusos e lidar com incidentes de segurança, por meio de ferramentas de análise de tráfego e inteligência artificial.

**Exemplo:**

Um funcionário tenta entrar em um site suspeito ou malicioso onde por meio das diretrizes da empresa é bloqueado.



1. **Desenvolvimento Seguro de Software:**

**Aplicação:**

Utilização de ferramentas automatizadas de SAST para detectar vulnerabilidades no código-fonte durante o desenvolvimento.

**Exemplo:**   
No decorrer do processo de criação de um sistema financeiro, os desenvolvedores utilizam uma ferramenta de análise estática, como o SonarQube, a fim de examinar o código-fonte em busca de possíveis vulnerabilidades, tais como problemas de autenticação ou permissões inapropriadas. O software identifica pontos fracos, como variáveis desprotegidas ou falhas de lógica vulneráveis a ataques, de forma automática. Dessa forma, os programadores resolvem as brechas de segurança antes do lançamento do software, reduzindo as chances de ataques virtuais.



1. **Análise de Vulnerabilidades e Testes de Penetração: Aplicação:**

Executar testes de penetração em redes empresariais para examinar a segurança de infraestrutura física e lógica, detectando vulnerabilidades em servidores, dispositivos e pontos de entrada.

**Exemplo:**

Um estudante pode empregar programas como Wireshark e Aircrack-ng para executar um teste de invasão em uma rede Wi-Fi empresarial, analisando a segurança das opções de criptografia e identificando possíveis falhas que possam resultar em ataques de interceptação de tráfego (man-in-the-middle). O exame pode indicar o emprego de protocolos de segurança deficientes, como o WEP, ou a presença de dispositivos conectados suscetíveis a ataques, possibilitando aprimorar a proteção da rede por meio de configurações mais sólidas, como o WPA3 e políticas de segurança extras.



1. **Criptografia e Proteção de Dados:**

#### **Aplicação:**

Emprego de códigos secretos para assegurar a privacidade e genuinidade de informações em locais de guarda e transmissão.

**Exemplo:**

Realizar a aplicação de criptografia em repouso em um banco de dados empresarial, empregando tecnologias como AES (Padrão de Criptografia Avançada) para proteger arquivos e informações armazenadas. Por exemplo, é possível configurar o banco de dados para criptografar todas as informações confidenciais, como dados de transações financeiras e clientes, antes de serem armazenadas no disco. Isso assegura que, mesmo que um invasor acesse o disco rígido, os dados permaneçam seguros e ilegíveis sem a chave de criptografia correta.  
  
Adicionalmente, é possível empregar o TLS (Transport Layer Security) como forma de assegurar a proteção dos dados em movimento, assegurando que todas as interações entre servidores e clientes sejam cifradas, impedindo assim que agentes externos possam interceptar ou modificar as informações durante a transmissão.

**BIBLIOGRAFIA**

**https://www.opservices.com.br/gerenciamento-de-servidores/**

**https://www.strongboxit.com/what-is-sast/**

[**https://www.welivesecurity.com/pt/recursos-e-ferramentas/teste-penetracao-iniciantes-5-ferramentas-para-comecar/**](https://www.welivesecurity.com/pt/recursos-e-ferramentas/teste-penetracao-iniciantes-5-ferramentas-para-comecar/)

[**https://csrc.nist.gov/publications/detail/fips/197/final**](https://csrc.nist.gov/publications/detail/fips/197/final)

**https://chatgpt.com/c/66e20b2c-99f4-8000-84a8-cbd8bf6ac285**