**Tema** -” Dê outros exemplos, no mínimo 5 (cinco), de aplicações dos conteúdos de base que serão estudados na UC Sistemas Computacionais e Segurança – SCS, explicando cada um deles”

1. **Criação de Dados**

* Aplicação: Proteção de senhas e transações financeiras online.
* Explicação: Quando você acessa o seu banco online ou faz compras pela internet, a criptografia atua para proteger suas informações. Por exemplo, quando você escreve a senha ou o número do cartão de crédito, esses dados são "embaralhados" por meio de um algoritmo criptográfico, como o AES (Advanced Encryption Standard) Isso significa que, se alguém interceptar esses dados, só verá uma sequência sem sentido, a menos que tenham a chave certa para descriptografar. É como se as informações estivessem dentro de um cofre digital que só o banco ou o sistema podem abrir. Sem a criptografia, seria muito fácil para hackers roubarem dados enquanto eles são enviados entre o seu dispositivo e o servidor do banco, o que poderia causar graves problemas, como roubo de identidade ou fraudes financeiras.

1. **Autenticação Multifator**

* O aplicativo é utilizado no WhatsApp e outros aplicativos para impedir que contas sejam hackeadas. Para proteger suas contas, muitas plataformas estão adotando a autenticação multifator (MFA) Isso funciona com uma camada extra de segurança: depois de digitar sua senha, você precisa fornecer outra prova de que é você mesmo. Pode ser um código enviado por mensagem de texto, um aplicativo de autenticação (como o Google Authenticator) ou até mesmo sua impressão digital ou reconhecimento facial. Isso é crucial porque, se um hacker conseguir descobrir sua senha, ainda assim ele não terá acesso à sua conta sem essa segunda camada de verificação. Essa técnica é bastante usada em aplicativos de mensagens, como o WhatsApp, que oferece a opção de configurar um PIN, além da senha, para proteger a conta.

1. **Firewall e Proteção de Redes**

* Aplicação: Utilizado em empresas para proteger seus sistemas de ataques de terceiros.
* Explicação: Um firewall é uma barreira que monitora e controla o tráfego que entra e sai da rede de uma organização. Pense nele como um porteiro em um edifício, que só deixa passar quem tem autorização. Se alguém tentar acessar a rede de fora, mas não tiver a permissão necessária, o firewall impede essa tentativa. Isso é crucial para proteger os servidores e computadores de ataques, como tentativas de hackers de invadir o sistema. Em companhias, isso é ainda mais grave, pois ataques podem causar a perda de dados, o comprometimento de dados confidenciais e até paralisar a operação de toda a organização. Existem diversos tipos de firewalls: alguns são instalados em servidores, enquanto outros podem ser dispositivos físicos conectados à rede.

1. **Proteção em Aplicações Web**

* Aplicação para proteger contra-ataques de SQL Injection em sites.
* Explicação: Sites e aplicativos na internet são frequentemente alvos de ataques. Um dos mais frequentes é o SQL Injection, no qual um hacker tenta inserir código malicioso em campos de entrada (como formulários) para controlar o banco de dados. Ao invés de digitar seu nome de usuário, o invasor pode tentar inserir um comando que force o banco de dados a liberar informações confidenciais. Se o site não estiver bem protegido, o hacker pode ter acesso às informações dos clientes, como senhas, endereços e até números de cartão de crédito. Para evitar isso, os desenvolvedores devem analisar com cautela os dados que os usuários inserem e usar técnicas como consultas parametrizadas, que impedem que comandos maliciosos sejam executados.

1. **Monitoramento de Redes**

* Aplicação: A detecção de atividades suspeitas nas redes corporativas.
* Explicação: As ferramentas de monitoramento monitoram o tráfego da rede em tempo real, identificando padrões anômalos que podem indicar tentativas de invasão ou a presença de malware. Ao identificar essas atividades, a equipe de segurança pode agir de forma rápida, evitando possíveis ameaças e reduzindo prejuízos. Isso possibilita uma abordagem mais eficaz para garantir a integridade e a proteção da rede.