**Revisão-Introdução à segurança da informação**

**1-Qual das redes é mais difícil ser defendida wan-wifi ou wan-cabeada? Quais cuidados devo tomar?**

**Wan-wifi é mais vulnerável sendo mais difícil de ser defendida exigindo criptografia forte e firewalls, wan-cabeada é crucial dispositivos seguros e monitoramento constante**

**2-Qual a diferença de Roteador, Gateway, proxy?**

**Roteador- envia informações da internet e dispositivos pessoais ex:PC, Celular e Tablets.**

**Gateway-Sistema ou equipamento cuja função básica é estabelecer comunicação.**

**Proxy- Um servidor proxy proporciona um gateway entre os usuários e a internet.**

**3-SMTP (servidor e-mail) quais a dificuldades e os maiores cuidados**

**O SMTP apresenta como as principais dificuldades inacessibilidade no servidor e-mail, problemas de autenticação, limite excedidos.**

**E pra tomar maiores cuidados é atualizações regulares de software, filtragem de spam, monitoramento de atividades suspeitas.**

**4-Sequestro físico ocorre quando qual a relação da engenharia social ponte de atenção máximo cuidados com o mundo virtual sempre tem alguém que sabe.**

**Sequestro físico ocorre quando uma pessoa é capturada ou retida contra sua própria vontade, A engenharia social está ligada ao sequestro físico, ressaltando a necessidade de cautela no ambiente virtual, onde indivíduos habilidosos podem explorar vulnerabilidades para acessos indevidos.**

**5-Apartado celular o que seria, qual é a tecnologia de segurança que trabalha tudo separado autenticado.**

**O "apartado celular" refere-se à tecnologia que separa e autentica cada célula individualmente, usando uma técnica conhecida como "zero Trust" ou confiança zero.**

**6-Criptografia porque os modelos são superados sempre?**

**Os modelos de criptografia são superados ao longo do tempo devido ao avanço da tecnologia e à descoberta de novas técnicas e algoritmos que podem comprometer a segurança dos sistemas criptográficos existentes.**

**7-Streaming quantas falhas de segurança causa?**

**O streaming pode causar falhas de segurança devido a transmissão continua pela internet, expondo informações sensíveis a hackers, violação de privacidade, malware e vazamentos de dados.**

**8-Quais são os principais pilares da segurança da informação e explique-os.**

**Confidenciabilidade- A confidencialidade refere-se à garantia de que as informações e os dados sejam acessíveis apenas para pessoas ou entidades autorizadas ou seja significando que informações confidenciais não podem ser acessadas.**

**Disponibilidade-** **A disponibilidade envolve a garantia de que os sistemas de informação e os recursos estejam disponíveis e acessíveis quando necessário, significado que o sistema não deve estar sujeito a interrupções não desejadas.**

**Autenticidade-** **A autenticidade trata da verificação da identidade de pessoas, sistemas ou entidades envolvidas em uma comunicação ou transação. Ela assegura que as partes envolvidas são realmente quem afirmam ser.**

**Integridade- A integridade está relacionada à garantia de que os dados não tenham sido modificados ou corrompidos de forma não autorizada durante a transmissão, armazenamento ou processamento.**

**Não repúdio- não repúdio envolve a capacidade de provar que uma ação ou transação ocorreu e foi realizada por uma determinada pessoa ou entidade, e essa pessoa ou entidade não pode negar ter realizado a ação.**

**9-O que são dados e informações?**

**Os dados são materiais brutos, informações são dados processados em um computador, que gera resultados para um determinado projeto.**

**10-O que é LGPD?**

**Lei geral de proteção de dados.**

**11- O que é ciphertext?**

**É a mensagem original transformada pela criptografia. Ela é ilegível sem a chave apropriada e parece um conjunto aleatório de caracteres.**

**12-O que é descriptografia?**

**É o processo reverso da criptografia, onde o ciphertext é convertido de volta para o plaintext original usando a chave correta.**

**13-O que é a privacidade?**

**protege a privacidade dos usuários, impedindo que terceiros (incluindo provedores de serviços) acessem o conteúdo das mensagens.**

**14-É um tipo de malware feito para extorquir dinheiro da sua vítima, esse cyber ataque irá criptografar os arquivos do usuário e pagamento.**

**Ransonware**

**15- O que são os ataques phishing?**

**são tentativas de enganar os usuários para obter informações confidenciais, como senhas, números de cartão de crédito, detalhes bancários ou informações pessoais, fazendo-se passar por uma entidade confiável.**

**16-O que é o worm.**

**Um "worm" é um tipo de malware (software malicioso) autônomo que se espalha automaticamente pela rede, explorando vulnerabilidades em sistemas e dispositivos não precisando de apps para se propagarem.**

**17-O que é o trojan.**

**Malware que invade seu PC disfarçado como software legítimo, usuário sendo enganados para instalar pensando que está instalando um programa útil, mas nada verdade está comprometendo a segurança do seu sistema.**

**18-O que é spam?**

**E-mails não solicitados que são enviados para milhares de pessoas.**

**19-Porque é quase impossível organizar ou controlar a Deep web?**

**Controlado por uma onion web, possuindo surface, normas, regulamentos, dark web, Deep web e bases militares.**