ATIVIDADE 06 – Parte 01

Docente: Robson Calvetti
UC: Sistemas Computacionais e Segurança – SCS

Marinna Pereira Carneiro da Silva - RA: 824142121
Mariana Hildebrand Danta - RA: 824118462
Christian Batista de Lima - RA: 824126605
Mayara Fernandes dos Santos – RA: 824227938
Victor Pinas Arnault – RA: 82215768

Análise e Desenvolvimento de Sistemas - ADS

ATIVIDADE 06 (Parte 01) - Desenvolvimento de Políticas de Segurança para uma Pequena Empresa

Objetivo: Os alunos do grupo devem se colocar no papel de consultores de segurança e criar um conjunto básico de políticas de segurança da informação para uma pequena empresa fictícia composto por:

- Políticas de acesso e controle de usuários;
- Política de uso de dispositivos móveis e redes;
- Diretrizes para resposta a incidentes de segurança;
- Política de backup e recuperação de desastres.

Entrega: Documento com as políticas propostas, detalhando as justificativas de cada uma.

EMPRESA FICTICIA – TRAVEL SAVVY AGENCY

Empresa de viagens que oferece pacotes personalizados e consultorias de viagens. Mantém dados de clientes, itinerários e informações de pagamento.

CONJUNTO BASICO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Políticas de acesso e controle de usuários;

- Autenticação Dupla do Usuário: Todos os usuários devem utilizar autenticação forte, com senhas complexas que devem ser criptografadas e alteradas a cada 90 dias e uma verificação em duas etapas.

Justificativa: Prevenir a invasão e coleta de dados confidenciais com acesso logins dos usuários.

Política de uso de dispositivos móveis e redes;

- Uso de Redes: O acesso a dados sensíveis deve ser feito apenas de redes seguras. O uso de VPN é obrigatório quando os funcionários acessam a rede da empresa fora do escritório.

Justificativa: Proteger contra ataques de invasores maliciosos como por exemplo: MAN IN THE MIDDLE, DDOS.

Diretrizes para resposta a incidentes de segurança;

- Registo de Incidentes: Todos os incidentes devem ser documentados em um sistema de registro, incluindo data, hora, tipo de ocorrência e ações tomadas.

Justificativa: A documentação de incidentes é relevante para termos o histórico e assim saber como se proteger de futuros ataques semelhantes e identificar melhorias no processo.

Política de backup e recuperação de desastres.

- Armazenamento Seguro: Os backups devem ser armazenados em um local seguro, como uma solução de armazenamento em nuvem confiável.

Justificativa: Manter backups dos dados é fundamental para recuperação sejam perdidos ou apagados em possíveis invasões.