USJT – UC Sistemas Computacionais e Segurança – Prof. Calvetti – Atividade 1

GRUPO: Acácio, Daniel Silva, Matheus Bolato, Munir

ATIVIDADE 1:

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.

Políticas de Segurança da Informação para a Empresa Fictícia

1. Política de Acesso e Controle de Usuários

- **Princípio do Mínimo Privilégio:** Os colaboradores terão acesso apenas aos sistemas e dados estritamente necessários para o desempenho de suas funções.
- **Gestão de Senhas:** As senhas devem ser complexas, contendo no mínimo 8 caracteres, com uma combinação de letras maiúsculas, minúsculas, números e símbolos. É proibido compartilhar senhas. Cada usuário é responsável pela confidencialidade de sua senha. As senhas de acesso aos sistemas corporativos devem ser alteradas a cada 90 dias.
- **Encerramento de Contrato:** Em caso de saída de um colaborador, todos os acessos (sistemas, e-mail, redes) devem ser revogados no último dia de trabalho.

2. Política de Uso de Dispositivos Móveis e Redes

- **Dispositivos Móveis Corporativos:** Dispositivos (smartphones, tablets) fornecidos pela empresa devem ser utilizados para fins de trabalho e estar protegidos com senha ou biometria. A instalação de aplicativos não relacionados ao trabalho é proibida.
- **Wi-Fi e Conexão de Redes:** É proibido conectar dispositivos pessoais à rede Wi-Fi corporativa. A rede deve ser usada apenas para dispositivos da empresa. Dispositivos da empresa devem se conectar a redes Wi-Fi públicas apenas por meio de uma VPN (Rede Privada Virtual) fornecida pela empresa.
- **Dados Pessoais:** O uso de e-mail corporativo para fins pessoais deve ser limitado.

3. Diretrizes para Resposta a Incidentes de Segurança

- **Identificação do Incidente:** Um incidente de segurança inclui acesso não autorizado, suspeita de vírus, perda de dados ou exposição de informações confidenciais.
- **Relato e Comunicação:** Qualquer colaborador que suspeite de um incidente de segurança deve imediatamente notificar o responsável pela TI ou a liderança da empresa por e-mail ou telefone.
- **Contenção:** O colaborador deve seguir as instruções do responsável pela TI para isolar o problema, como desconectar o dispositivo da rede. Não tente resolver o problema por conta própria.
- **Análise e Recuperação:** Após a contenção, a equipe de TI irá investigar a causa, restaurar os sistemas e dados afetados e implementar medidas para evitar a recorrência do incidente.

4. Política de Backup e Recuperação de Desastres

- **Frequência de Backup:** O backup de todos os dados críticos da empresa será realizado diariamente.
- **Armazenamento:** As cópias de segurança serão armazenadas em um local seguro, fora do ambiente de produção (backup off-site), para proteção contra eventos físicos como incêndios ou inundações.
- **Testes de Recuperação:** O plano de recuperação de desastres será testado anualmente para garantir que os dados possam ser restaurados de forma eficaz em caso de falha de sistema.
- **Recuperação em Caso de Desastre:** Em caso de perda total de dados, a equipe de TI irá seguir o plano de recuperação para restaurar os sistemas e dados a partir da última cópia de segurança disponível.