Atividade 03 - Política de Segurança da Informação

izaell.oficial@uni9.edu.br Mudar de conta

Seu e-mail será registrado quando você enviar este formulário.

* Indica uma pergunta obrigatória

Política de Segurança da Informação

Nesta atividade, vocês devem desenvolver um escopo de Política de Segurança da Informação. Para isso, selecione um dos temas listados a seguir e responda as perguntas de 01 a 08:

Temas - Política de Segurança da Informação *

Information Security Policy

- ( ) Backup e Segurança Física;
- ( ) Controles de Acesso;
- (•) Uso de Internet / Intranet / Redes Wireless
- ( ) Uso do Email Corporativo
- ( ) Uso de Equipamentos da Organização (Dentro e Fora da Empresa)
- ( ) Classificação da Informação
- ( ) Uso dos Softwares Corporativos;
- ( ) Criação, Manuseio, Transporte, Armazenamento e Descarte das Informações

01: Introdução da Política de Segurança da Informação * 1 ponto

- Atual Cenário (Um problema que deve ser resolvido totalmente ou parcialmente com uma Política de Segurança da Informação)

No cenário atual, a utilização inadequada da Internet, Intranet e Redes Wireless dentro das organizações representa um risco significativo para a segurança da informação. Problemas como conexões Wi-Fi desprotegidas, acesso a sites maliciosos, uso de redes externas inseguras e a ausência de monitoramento podem resultar em invasões, vazamento de dados e prejuízos à imagem institucional. Essa política busca minimizar tais riscos estabelecendo normas e boas práticas para o uso seguro das redes.

02: Objetivo da Política de Segurança da Informação * 1 ponto

- Objetivo da Política de Segurança da Informação (O que se deseja Resolver)

O objetivo desta política é definir diretrizes para o uso correto e seguro da Internet, Intranet e Redes Wireless, assegurando a proteção das informações corporativas, prevenindo acessos não autorizados, evitando incidentes de segurança e garantindo que os recursos tecnológicos sejam utilizados de forma ética, eficiente e alinhada às necessidades da organização.

03: Escopo da Política de Segurança da Informação. * 1 ponto

O escopo de uma Política de Segurança da Informação deve conter quem e o quê será afetado por sua Implantação, incluindo:

- Áreas;
- Times;
- Pessoas Estratégicas;
- Recursos computacionais;
- Fornecedores;
- Terceirizados;

A política se aplica a todas as áreas da organização, abrangendo:

Áreas: todos os departamentos que utilizam redes e sistemas conectados;

Times: equipes administrativas, técnicas e operacionais;

Pessoas Estratégicas: gestores, diretores e colaboradores com acesso privilegiado;

Recursos Computacionais: computadores, dispositivos móveis, servidores, roteadores e pontos de acesso wireless;

Fornecedores: empresas parceiras que utilizem ou tenham acesso às redes corporativas;

Terceirizados: consultores, prestadores de serviços e estagiários com acesso aos recursos de rede.

04: Pré-requisitos para a adoção da Política de Segurança da Informação: * 1 ponto

- Descreva os pré-requisitos que justifiquem o funcionamento da política de Segurança da Informação proposta.

Infraestrutura de rede atualizada e com mecanismos de proteção (firewall, IDS/IPS, antivírus corporativo).

Procedimentos de autenticação seguros (uso de senhas fortes, autenticação multifator).

Configuração adequada das redes wireless, com criptografia WPA2/WPA3 e segmentação entre rede corporativa e rede de visitantes.

Definição clara de responsabilidades entre usuários, gestores e equipe de TI.

Programa de conscientização e treinamento contínuo dos colaboradores.

Ferramentas de monitoramento de tráfego e geração de logs.

05: Benefícios da adoção da Política de Segurança da Informação: * 1 ponto

- Descreva os principais benefícios que serão obtidos ao adotara Política de Segurança da Informação.

Redução significativa de riscos de invasão, roubo de dados e ataques cibernéticos.

Maior confiabilidade e disponibilidade das redes corporativas.

Proteção das informações estratégicas e dados sensíveis da empresa.

Garantia de conformidade com normas e regulamentações de segurança.

Fortalecimento da cultura de segurança da informação entre colaboradores.

Preservação da imagem institucional e aumento da confiança de clientes e parceiros.

06: Critérios e Diretrizes da Política de Segurança da Informação: * 1 ponto

- Descreva as diretrizes que serão estabelecidas pela Política de Segurança da Informação.
- Classifique as diretrizes em: Estratégico, Tático ou Operacional

Estratégico:

Definir a segurança da Internet, Intranet e Redes Wireless como prioridade da organização.

Garantir que todos os acessos sigam normas internacionais e regulatórias.

Tático:

Estabelecer regras para uso da Internet (bloqueio de sites maliciosos ou não relacionados ao trabalho).

Segmentar redes (corporativa, administrativa, visitantes) com diferentes níveis de acesso.

Adotar VPN e autenticação multifator para acessos remotos.

Operacional:

Exigir troca periódica de senhas e utilização de senhas fortes.

Configurar roteadores e pontos de acesso com criptografia atualizada (WPA3).

Monitorar tráfego de rede e manter logs de acessos.

Realizar treinamentos práticos de conscientização em segurança para os colaboradores.

07: Leis, Políticas e Normas de Segurança da Informação * 1 ponto

- Descreva quais Leis, Normas ou Políticas estão relacionadas com esta Política de Segurança da Informação.

A Política de Segurança da Informação referente ao uso de Internet, Intranet e Redes Wireless está relacionada com as seguintes legislações, normas e diretrizes:

Leis:

LGPD (Lei Geral de Proteção de Dados – Lei nº 13.709/2018): regula o tratamento de dados pessoais e exige medidas de segurança adequadas para proteção das informações.

Marco Civil da Internet (Lei nº 12.965/2014): estabelece princípios, garantias, direitos e deveres no uso da Internet no Brasil.

Lei de Crimes Cibernéticos (Lei nº 12.737/2012 – Carolina Dieckmann): tipifica crimes como invasão de dispositivos, roubo de dados e acessos não autorizados.

Normas Técnicas (ISO/IEC):

ISO/IEC 27001: gestão de segurança da informação.

ISO/IEC 27002: boas práticas e controles de segurança.

ISO/IEC 27033: segurança em redes de comunicação.

Políticas Internas:

Política de Uso Aceitável da Internet e Intranet.

Política de Acesso Remoto e VPN.

Política de Conectividade Wireless Segura.