ATIVIDADE 1

Atividade: Desenvolvimento de Políticas de Segurança para uma Pequena Empresa

Objetivo: O grupo deve atuar como consultores de segurança, desenvolvendo um conjunto básico de políticas de segurança da informação para uma pequena empresa fictícia. As políticas abordam o controle de acesso, uso de dispositivos, resposta a incidentes e backup.

Estrutura Sugerida:

1. Política de Acesso e Controle de Usuários

- Objetivo: Definir quem tem acesso aos recursos da empresa e como esse acesso é gerenciado.
- Justificativa: O controle de acesso reduz os riscos de acesso não autorizado a informações sensíveis, assegurando que apenas usuários autorizados possam acessar os sistemas e dados da empresa.
- Diretrizes:
- Uso de autenticação multifator (MFA) para todos os usuários.
- Diferenciação clara de permissões, com perfis de usuário para diferentes funções (administração, TI, funcionários gerais).
- Revisão periódica dos acessos (trimestralmente ou após a saída de colaboradores).
- Senhas devem ser complexas e atualizadas a cada 90 dias.

2. Política de Uso de Dispositivos Móveis e Redes

- Objetivo: Regular o uso de dispositivos móveis e o acesso à rede da empresa para proteger dados fora do ambiente controlado.
- Justificativa: Dispositivos móveis e o trabalho remoto podem introduzir vulnerabilidades; essa política mitiga riscos de vazamento de dados e ataques em redes públicas.
- Diretrizes:
- Dispositivos móveis que acessam a rede da empresa devem estar protegidos por senhas e criptografia.
- Uso de VPN (Rede Privada Virtual) obrigatório para acesso remoto.
- Proibição de conexão a redes Wi-Fi públicas sem VPN.
- Instalação de softwares antivírus e de rastreamento remoto para controle e limpeza de dados em caso de perda ou roubo.

3. Diretrizes para Resposta a Incidentes de Segurança

- Objetivo: Estabelecer um plano para identificar, gerenciar e mitigar incidentes de segurança da informação.
- Justificativa: Uma resposta rápida a incidentes pode minimizar danos e garantir a continuidade do negócio, além de facilitar a recuperação de sistemas comprometidos.
- Diretrizes:
- Designar uma equipe de resposta a incidentes (formada por TI e gestores).
- Notificação imediata à equipe de TI em caso de suspeita de violação ou incidente.
- Planos de contenção, erradicação e recuperação de incidentes de segurança.
- Documentação detalhada de cada incidente para análise posterior.
- Revisão e simulação de resposta a incidentes semestralmente.

4. Política de Backup e Recuperação de Desastres

- Objetivo: Garantir a continuidade dos serviços e proteção dos dados da empresa em caso de falha grave, ataque cibernético ou desastre natural.
- Justificativa: Backups regulares e um plano de recuperação eficaz são essenciais para prevenir a perda de dados críticos e a paralisação prolongada da empresa.
- Diretrizes:
- Backup automatizado de todos os dados críticos, com frequência diária.
- Armazenamento de backups em locais separados (em nuvem e fisicamente fora do ambiente de trabalho).
- Testes de recuperação de dados realizados trimestralmente para garantir a eficácia.
- Definição de um plano de recuperação de desastres, com processos claros para restaurar operações em casos de falhas graves.

ATIVIDADE 2

Certificações Escolhidas:

- ISO/IEC 27001 (Sistema de Gestão da Segurança da Informação)
- PCI DSS (Padrão de Segurança de Dados para a Indústria de Cartões de Pagamento)

Estrutura do Estudo Comparativo:

1. Requisitos para Certificação

ISO/IEC 27001:

- Estabelecimento de um Sistema de Gestão de Segurança da Informação (SGSI).
- Realização de análise de riscos e definição de controles adequados (anexo A da ISO/IEC 27001 traz uma lista de controles recomendados).
- Políticas de segurança, responsabilidades organizacionais, gestão de incidentes e continuidade dos negócios.
- Auditorias internas e externas para garantir conformidade com a norma.

PCI DSS:

- Focada em empresas que armazenam, processam ou transmitem dados de cartões de crédito.
- 12 requisitos principais, incluindo controle de acesso, monitoramento de redes, criptografia de dados, e teste regular de sistemas de segurança.
- Realização de avaliações anuais por auditores qualificados (QSA – Qualified Security Assessors).

2. Setores de Atuação

ISO/IEC 27001:

- Aplicável a qualquer organização, independentemente do tamanho ou setor.
- Usada amplamente em empresas de tecnologia, serviços financeiros, setor público, telecomunicações, saúde e qualquer empresa que manuseie informações sensíveis.

PCI DSS:

- Aplicável principalmente à indústria de cartões de pagamento.
- Empresas que aceitam, processam, armazenam ou transmitem dados de cartões de crédito e débito, como bancos, adquirentes, comerciantes, processadores de pagamento, entre outros.

3. Benefícios de Obter Cada Certificação

ISO/IEC 27001:

- Melhoria contínua na gestão de riscos e segurança da informação.
- Aumento da confiança de clientes e parceiros, ao garantir a proteção das informações.
- Vantagem competitiva e cumprimento de regulamentações relacionadas à privacidade e proteção de dados (como a LGPD ou GDPR).
- Redução de riscos operacionais e financeiros por incidentes de segurança.

PCI DSS:

- Garantia de conformidade com os requisitos das bandeiras de cartões, permitindo que as empresas processem pagamentos com cartões de crédito/débito.
- Redução de fraudes relacionadas a dados de pagamento.
- Melhoria da postura de segurança cibernética em áreas críticas relacionadas a dados financeiros.
- Evita penalidades financeiras por não conformidade e aumenta a confiança dos consumidores.

4. Diferenças na Abordagem de Gestão de Riscos

ISO/IEC 27001:

- Baseada em uma abordagem de gestão de riscos abrangente e contínua, onde os riscos são identificados, avaliados e tratados de forma sistemática.
- A organização define seus próprios critérios de avaliação de riscos, de acordo com o contexto de negócios, e implementa controles com base na necessidade específica.

PCI DSS:

- Enfatiza o controle de riscos específicos relacionados a dados de pagamento.
- Focada em requisitos prescritos para proteger dados de cartões de crédito, com controles rígidos e práticas de segurança que devem ser seguidas.
- A abordagem é mais técnica e centrada em evitar falhas e vulnerabilidades de segurança em ambientes de pagamento.

5. Conclusão do Comparativo

O estudo destaca que, enquanto a ISO/IEC 27001 oferece uma abordagem holística e flexível para a segurança da informação em qualquer tipo de organização, a PCI DSS é mais específica e voltada para a proteção de dados sensíveis em transações

financeiras. Cada uma tem seus benefícios e aplicações distintas, dependendo do contexto e setor de atuação da empresa.