UC- SISTEMAS COMPUTACIONAIS E SEGURANÇA
Maria Eduarda Medeiro Porto 824144948
ORIENTADOR: Robson Calvetti

PRÁTICA 06- Normas e Políticas de Segurança da Informação

ATIVIDADE 1-

Estudo: Desenvolvimento de Políticas de Segurança para uma Pequena Empresa
Objetivo: O aluno deve se colocar no papel de consultor 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 Acesso e Controle de Usuários

-Autenticação: Todos os usuários devem ter uma conta de usuário única e senha forte para acessar os sistemas e recursos da empresa.

-Autorização: Acessos aos sistemas e recursos serão concedidos com base nas necessidades do trabalho e serão revogados quando o usuário não precisar mais deles.

-Controle de Acesso: O acesso aos sistemas e recursos será controlado por meio de listas de controle de acesso (ACLs) e grupos de segurança.

-Senha: As senhas devem ser alteradas a cada 90 dias e devem ter no mínimo 10 caracteres, incluindo letras maiúsculas e minúsculas, números e caracteres especiais.

-Acesso Remoto: O acesso remoto aos sistemas e recursos será feito por meio de uma VPN (Virtual Private Network) segura.

Política de Uso de Dispositivos Móveis e Redes

-Dispositivos Móveis: Os dispositivos móveis devem ser configurados com senhas e criptografia para proteger os dados da empresa.

-Redes: A empresa utilizará redes Wi-Fi seguras e criptografadas para proteger os dados em trânsito.

-Uso de Redes Públicas: Os funcionários não devem acessar os sistemas e recursos da empresa por meio de redes públicas não seguras.

Diretrizes para Resposta a Incidentes de Segurança

-Identificação: Os incidentes de segurança devem ser identificados e relatados imediatamente ao departamento de segurança.

-Contenção: O departamento de segurança deve conter o incidente para evitar que ele se espalhe e cause mais danos.

-Erradicação: O departamento de segurança deve eliminar a causa raiz do incidente.

-Recuperação: O departamento de segurança deve restaurar os sistemas e recursos afetados ao estado normal.

-Aprendizado: O departamento de segurança deve analisar o incidente e implementar medidas para evitar que ele aconteça novamente.

Política de Backup e Recuperação de Desastres

-Backup: Os dados da empresa devem ser backupados diariamente e armazenados em um local seguro.

-Recuperação de Desastres: A empresa deve ter um plano de recuperação de desastres para restaurar os sistemas e recursos em caso de desastre.

-Testes: O plano de recuperação de desastres deve ser testado regularmente para garantir que ele esteja funcionando corretamente.

-Armazenamento: Os backups devem ser armazenados em um local seguro e acessível apenas por funcionários autorizados.

ATIVIDADE 2 -

Estudo: Comparativo de Certificações em Segurança da Informação;

Objetivo: O grupo deve escolher duas certificações de segurança da informação

(por exemplo, ISO/IEC 27001 e PCI DSS) e fazer um estudo comparativo; Deve ser

abordado:

- Requisitos para certificação;

- Setores de atuação (em que tipo de empresas ou indústrias cada certificação é mais usada);

- Benefícios de obter cada certificação;

- Diferenças na abordagem de gestão de riscos.

1. Requisitos para Certificação

ISO/IEC 27001

-Sistema de Gestão de Segurança da Informação (SGSI): A organização deve implementar um SGSI que atenda aos requisitos da norma.

-Avaliação de Riscos: Realizar uma avaliação de riscos para identificar e tratar riscos à segurança da informação.

-Documentação: Criar e manter documentação adequada, incluindo políticas, procedimentos e registros.

-Auditorias Internas: Realizar auditorias internas regulares para garantir a conformidade com a norma.

-Melhoria Contínua: Implementar um processo de melhoria contínua para o SGSI.

PCI DSS

-Requisitos de Segurança: Atender a 12 requisitos principais que abrangem segurança de rede, proteção de dados do titular do cartão, gerenciamento de vulnerabilidades, monitoramento e teste de redes, e políticas de segurança.

-Avaliação de Risco: Realizar uma avaliação de risco focada em dados de cartões de pagamento.

-Relatórios de Conformidade: Dependendo do volume de transações, as empresas devem preencher um Questionário de Autoavaliação (SAQ) ou passar por uma avaliação de um avaliador qualificado (QSA).

-Treinamento de Funcionários: Garantir que todos os funcionários estejam cientes das políticas de segurança e práticas recomendadas.

2. Setores de Atuação

ISO/IEC 27001

- Setores Diversos: É aplicável a qualquer tipo de organização, independentemente do tamanho ou setor, incluindo tecnologia da informação, saúde, finanças, governo e educação.
- Organizações Globais: Muitas empresas multinacionais adotam a ISO/IEC 27001 para garantir a segurança da informação em suas operações globais.

PCI DSS

- Indústria de Pagamentos: Específico para empresas que processam, armazenam ou transmitem dados de cartões de pagamento.
- Setores Financeiros e Varejo: Comum em bancos, instituições financeiras, e empresas de e-commerce que lidam com transações de cartões de crédito e débito.

3. Benefícios de Obter Cada Certificação

ISO/IEC 27001

- Reconhecimento Internacional: A certificação é reconhecida globalmente, aumentando a credibilidade da organização.
- Melhoria da Segurança: Ajuda a identificar e mitigar riscos à segurança da informação, melhorando a proteção de dados.
- Conformidade Legal: Facilita a conformidade com regulamentações e leis de proteção de dados.
- Confiança do Cliente: Aumenta a confiança dos clientes e parceiros comerciais na segurança das informações.

PCI DSS

- Proteção de Dados: Melhora a segurança dos dados dos titulares de cartões, reduzindo o risco de fraudes.
- Evita Multas: A conformidade ajuda a evitar multas e penalidades associadas a violações de dados.
- Aumento da Confiança: A certificação demonstra compromisso com a segurança, aumentando a confiança dos clientes.
- Melhoria de Processos: Fornece um framework para melhorar processos de segurança e gestão de riscos.

4. Diferenças na Abordagem de Gestão de Riscos

ISO/IEC 27001

- Abordagem Abrangente: Foca na gestão de riscos de segurança da informação de forma holística, considerando todos os ativos de informação da organização.
- Ciclo de Melhoria Contínua: Enfatiza a melhoria contínua do SGSI, permitindo que a organização se adapte a novas ameaças e vulnerabilidades.

PCI DSS

- Foco Específico: Concentra-se na proteção de dados de cartões de pagamento e na conformidade com requisitos específicos relacionados a transações financeiras.
- Requisitos Estritos: Apresenta requisitos rigorosos e específicos que devem ser seguidos, com menos flexibilidade em comparação com a ISO/IEC 27001.

ATIVIDADE 2-

COMPARATIVO DE CERTIFICAÇÕES

SEGURANÇA DA INFORMAÇÃO

ISO/IEC 27001

PCI DSS)

REQUISITOS DE CERTIFICAÇÃO

Requisito	ISO/IEC 27001	PCI DSS
Sistema de Gestão	Implementar SGSI conforme a norma.	Implementar controles de segurança.
Avaliação de Riscos	Avaliar e tratar riscos de segurança da informação.	Avaliar riscos focados em dados de cartões de pagamento.
Documentação	Manter políticas, procedimentos e registros.	Documentar políticas de segurança e vulnerabilidades.
Auditorias Internas	Auditorias internas regulares.	SAQ ou avaliação por QSA, conforme volume de transações.
Melhoria Contínua	Processo de melhoria contínua para o SGSI.	Revisão recomendada das práticas de segurança.
Requisitos de Segurança	Controlar riscos e melhorias.	Cumprir 12 requisitos principais de segurança.
Treinamento de Funcionários	Recomendado, mas não obrigatório.	Obrigatório para todos os funcionários.

SETORES DE ATUAÇÃO

Certificação	Setores Prioritários
ISO/IEC 27001	Tecnologia da Informação (TI), Saúde, Financeiro, Indústria
PCI DSS	Comércio Varejista, Bancos e Fintechs, E-commerce, Pagamentos

BENEFÍCIOS EM COMUM

1. **Melhoria na Segurança da Informação:** Ambas ajudam a implementar controles robustos para proteger dados.
2. **Conformidade Regulatória:** Ajudam as organizações a atender a exigências legais e regulatórias sobre proteção de dados.
3. **Confiança do Cliente:** A obtenção de qualquer uma das certificações melhora a confiança dos clientes e parceiros.
4. **Mitigação de Riscos:** Ajudam na identificação e tratamento de riscos à segurança da informação.
5. **Auditorias Regulares:** Ambas exigem ou recomendam auditorias regulares para manter a conformidade.

DIFERENÇAS

Aspecto	ISO/IEC 27001	PCI DSS
Foco Principal	Segurança da informação em geral (ampla aplicação)	Proteção de dados de cartões de pagamento (específico para dados de pagamento)
Escopo	Aplicável a todos os tipos de informações e setores.	Voltada principalmente para setores que processam pagamentos com cartão.
Gestão de Segurança	Requer a implementação de um Sistema de Gestão de Segurança da Informação (SGSI).	Não exige um SGSI formal, mas requer controles específicos de segurança.
Requisitos de Segurança	Foco em gestão de riscos e melhoria contínua.	Exige cumprimento de 12 requisitos de segurança específicos e rígidos.
Auditorias e Avaliações	Auditorias internas periódicas e auditoria externa para certificação.	Auditorias por avaliadores qualificados (QSA) ou autoavaliação (SAQ).
Setores de Aplicação	Abrange vários setores (TI, saúde, financeiro, indústria).	Foco em varejo, e-commerce, bancos e serviços de pagamento.
Documentação	Exige documentação completa de políticas e procedimentos.	Requer documentação relacionada à segurança de dados de pagamento.