Atividade 1 – Desenvolvimento de Políticas de Segurança da Informação para uma Pequena Empresa

Este trabalho tem como objetivo propor um conjunto de políticas básicas de segurança da informação voltadas para uma pequena empresa fictícia chamada InfoTech Solutions, que atua com suporte técnico e gestão de sistemas em nuvem. A ideia é apresentar políticas realistas e aplicáveis, refletindo o que foi aprendido ao longo do segundo semestre, com auxílio de ferramentas de inteligência artificial e pesquisa independente.

1. Política de Acesso e Controle de Usuários

O controle de acesso deve ser estruturado de forma que cada colaborador tenha apenas as permissões necessárias para executar suas atividades. As senhas devem ser individuais, com autenticação multifator sempre que possível, e atualizadas periodicamente. Contas de ex-funcionários precisam ser desativadas imediatamente após o desligamento. A empresa também deve manter um registro de acessos para auditoria e segurança.

Essa política é essencial porque reduz a possibilidade de acessos indevidos e ajuda a identificar rapidamente comportamentos anormais.

2. Política de Uso de Dispositivos Móveis e Redes

Os dispositivos móveis que acessam dados da empresa devem possuir bloqueio de tela, criptografia e antivírus atualizados. É proibido o uso de dispositivos pessoais em redes corporativas sem autorização formal. Para conexões externas, deve-se utilizar uma VPN segura e autenticada. A rede Wi-Fi corporativa deve usar protocolos de segurança modernos, como WPA3, e senhas complexas.

Essas medidas são fundamentais para mitigar os riscos associados ao uso de dispositivos móveis e conexões sem fio, que frequentemente são alvo de ataques cibernéticos.

3. Diretrizes para Resposta a Incidentes de Segurança

Todos os funcionários devem ser instruídos a relatar imediatamente qualquer suspeita de incidente de segurança. Deve existir um plano formal de resposta a incidentes, com definição clara das etapas de detecção, contenção e recuperação. Após a resolução, a

equipe deve elaborar um relatório de lições aprendidas e revisar as políticas para evitar reincidências.

Essa diretriz é importante porque ajuda a empresa a reagir rapidamente, minimizando danos e prevenindo futuros ataques.

4. Política de Backup e Recuperação de Desastres

Os backups devem ser realizados de forma automatizada e armazenados tanto localmente quanto em nuvem. É essencial testar regularmente os backups para verificar sua integridade. A empresa precisa manter um plano de recuperação de desastres documentado, definindo prazos de restauração e responsabilidades.

Ter uma política de backup sólida é vital para garantir a continuidade das operações e evitar perdas de dados críticas.

Atividade 2 – Comparativo de Certificações em Segurança da Informação

Nesta segunda atividade, foi realizado um comparativo entre duas certificações amplamente reconhecidas: ISO/IEC 27001 e PCI DSS. O objetivo é compreender como cada uma atua em diferentes contextos e de que forma podem contribuir para a segurança e a credibilidade das empresas. As informações foram obtidas por meio de pesquisa acadêmica e análise de fontes confiáveis, com auxílio de ferramentas de IA para sintetizar os dados.

1. Requisitos para Certificação

A ISO/IEC 27001 é uma norma voltada para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI), enquanto a PCI DSS é mais específica para empresas que lidam com dados de cartões de pagamento. A ISO 27001 exige a definição de políticas, controles e auditorias internas contínuas, enquanto a PCI DSS impõe requisitos técnicos obrigatórios, como uso de firewall, criptografia e controle rigoroso de acesso.

2. Setores de Atuação

A ISO/IEC 27001 pode ser aplicada em qualquer tipo de empresa, independentemente do setor, sendo muito utilizada por instituições financeiras, organizações públicas e empresas de tecnologia. Já a PCI DSS é obrigatória para negócios que processam, armazenam ou transmitem dados de cartões, como lojas virtuais, bancos e operadoras de pagamento.

3. Benefícios das Certificações

Entre os principais benefícios da ISO/IEC 27001 estão a melhoria da governança corporativa, o fortalecimento da confiança de clientes e a conformidade com legislações como a LGPD. Já a PCI DSS traz benefícios mais técnicos, como a redução de fraudes em transações e a conformidade com normas internacionais de pagamento.

Ambas as certificações reforçam a imagem da empresa como comprometida com a segurança da informação e a proteção de dados.

4. Diferenças na Gestão de Riscos

A ISO/IEC 27001 adota uma abordagem baseada na gestão de riscos organizacionais, utilizando o ciclo PDCA (Planejar, Fazer, Verificar e Agir). A PCI DSS, por sua vez, é mais prescritiva e técnica, definindo controles mínimos obrigatórios para proteção de dados sensíveis. Enquanto a ISO permite certa flexibilidade, a PCI exige conformidade estrita com seus requisitos.

Conclusão

As duas certificações são complementares: a ISO/IEC 27001 oferece uma base ampla de gestão da segurança, enquanto a PCI DSS garante uma camada de proteção técnica focada em dados financeiros. Com o avanço da transformação digital, as empresas que buscam ambas as certificações conseguem aliar segurança estratégica e conformidade operacional, fortalecendo a confiança de seus clientes e parceiros.

Gustavo Jaccon Franquini

RA: 825150548