## Amanda Vitória de Assunção Sousa 31/07/2024

ASSUNTO: Segurança da Informação

Atividade 03

1. O que é a NBR ISO/IEC 27002 e qual seu objetivo principal?

R=É um documento com recomendações para gerenciar riscos enfrentados pelas organizações, podendo ser personalizado para qualquer contexto .A ISO 27002 objetiva principalmente fornecer as diretrizes necessárias para implementar a segurança da informação nas empresas, visando também mantê-la e melhorá-la ao longo do tempo.

1. Quais são as principais seções da NBR ISO/IEC 27002?

R= Política de segurança da informação,organizando a segurança da informação,gestão de ativos,segurança em recursos humanos,segurança física e do ambiente,gestão das operações e comunicações,controle de acesso,aquisição, desenvolvimento e manutenção de sistemas de informação.

1. Explique a importância da seção de Políticas de Segurança da Informação na NBR ISO/IEC 27002.

R=Fundamental para consolidar um SGSI, a ISO 27002 garante a continuidade e a manutenção dos processos de segurança , alinhados aos objetivos estratégicos da organização. Nesse sentido, a norma traz um guia prático completo de implementação e descrição do modo como os controles podem ser aplicados.

1. Como a Gestão de Ativos contribui para a segurança da informação de uma organização?

R= Garanti que as informações críticas da organização estejam protegidas contra ameaças internas e externas, incluindo hackers, malwares e outras formas de ataques cibernéticos.

1. Qual é o objetivo dos controles de Criptografia na NBR ISO/IEC 27002?

R=Prevenir a ocorrência de erros, perdas, modificações não autorizadas ou mau uso de informações em aplicações.

1. Descreva a importância da Segurança Física e do Ambiente segundo a NBR ISO/IEC 27002.

R= Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.

1. Quais são os objetivos da Gestão de Incidentes de Segurança da Informação?

R=Reduzir a probabilidade ou as consequências de incidentes. Assegurar uma gestão consistente e eficaz das evidências relacionadas a incidentes de segurança da informação para fins de ações disciplinares e legais.

1. Por que é importante implementar controles de Segurança nas Comunicações?

R= Porque favorece a integridade, a confidencialidade e a disponibilidade das informações.

1. Explique a relevância de definir papeis e responsabilidades na Organização da Segurança da Informação.

R=Grande parte dos incidentes envolvendo perda de dados ou vazamento de informações é causada pelos funcionários da própria empresa. Essa estatística aponta para uma necessidade de ação urgente: estabelecer uma política de controle de acesso que seja capaz de inviabilizar — ou pelo menos minimizar — essa possibilidade.

1. Como a seção de Relações com Fornecedores pode impactar a segurança da informação de uma organização?

R= Um fornecedor que atrase a prestação de um serviço, por exemplo, impede que determinada rotina seja executada. Consequentemente, o consumidor sente os problemas, que descreva o processo de planejamento de continuidade de negócios e sua importância para a segurança da informação. Estratégias, acordos e arranjos, com o objetivo de prevenir, preparar e responder adequadamente a situações de disrupção do negócio, que podem levar a crises ou desastres.

1. O que deve ser considerado ao implementar um controle de acesso baseado na NBR ISO/IEC 27002?

R= Criptografia.SIEM (Gerenciamento e Correção de Eventos) DLP (Prevenção de Perda/Vazamento de Dados) AIM (Gestão de Identidades)

1. Explique a importância da auditoria de conformidade em segurança da informação.

R= Através de um processo estruturado e contínuo, as empresas podem identificar e mitigar riscos, fortalecer sua postura de segurança e garantir a proteção de seus ativos críticos.

1. Como a conscientização e o treinamento dos funcionários podem ajudar na segurança da informação?

R=Treinamentos regulares podem educar os colaboradores sobre as diferentes formas de ataques.

1. Qual a importância de se ter uma política de uso aceitável de ativos?

R=Documento que define como os recursos computacionais de uma instituição podem ser utilizados .