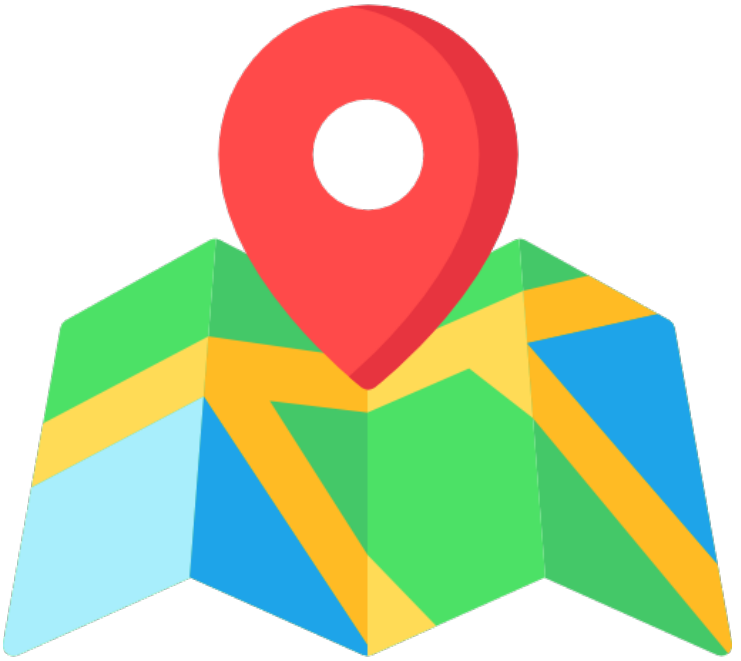
Introdução à Segurança da Informação

Prof. Dr. José Augusto de Sena Quaresma

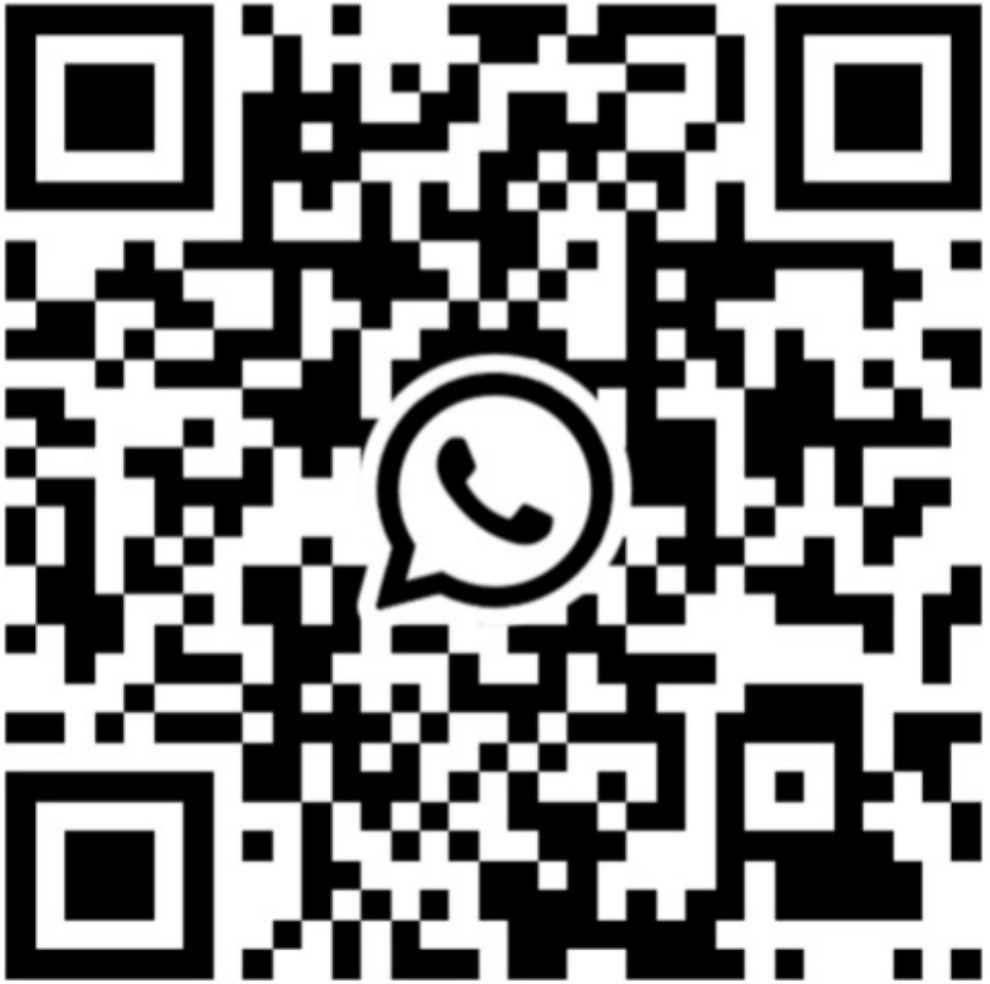
Jq.quaresma12@gmail.com

Agenda

- Revisando o trabalho
- Questões de concurso
- Apresentação da disciplina
- Normas de Segurança
- Atividade para a próxima aula



Nosso grupo no Whatsapp



Importância da Segurança da Informação

Atividade

Atividade – em grupo

- Pesquise na internet casos reais de falhas de segurança em empresas, especialmente de tecnologia ou financeiras.
- Escolha dois casos e discuta em equipe primeiramente quais princípios básicos de segurança foram violados e depois aprimore para o Hexagrama Parkeriano.
- O trabalho pode ser entregue de maneira escrita ou em apresentação para a turma.

Questões de concurso

Banca – FAUEL – 2024

- Qual dos princípios de segurança da informação listados a seguir envolve a garantia de que as informações sensíveis sejam acessadas apenas por pessoas autorizadas, normalmente sendo alcançado por meio de sistemas de autenticação, controle de acesso e criptografia?
- A – Integridade
- B – Não Repúdio
- C – Disponibilidade
- D – Confidencialidade

Banca – FAUEL – 2024

- Resposta:

- Letra D

Banca – IBADE - SESDEC-RO – 2024

- Das alternativas abaixo, qual é considerada uma ferramenta que garante o Princípio da Disponibilidade, na segurança da informação?
- A – Assinatura digital
- B – Criptógrafia
- C – Biometria
- D – Nobreak

Banca – IBADE - SESDEC-RO – 2024

- Resposta:

- Letra D

Banca – FUNDEF-PR – 2024

- Quais são os elementos fundamentais que compõem os atributos da segurança da informação?
- A – Confidencialidade, Paridade, Inviolabilidade e Privacidade.
- B – Confidencialidade, Integridade, Disponibilidade e Autenticidade.
- C – Integridade, Inviolabilidade, Autenticidade e Privacidade.
- D – Disponibilidade, Acessibilidade, Praticabilidade e Inviolabilidade
- E – Exploit, Vulnerability, Encryption e Data Breach.

Banca – FUNDEF-PR – 2024

- Resposta:

- Letra B

Conceitos da aula anterior

Revisão

- Importância da Segurança da Informação
- Princípios da segurança da Informação
- Ciclo de vida da informação
- Princípios fundamentais
  - Confidencialidade
  - Integridade
  - Disponibilidade
- Hexagrama Parkeriano
  - Confidencialidade – Posse
  - Disponibilidade – Utilidade
  - Integridade – Autenticidade

Normas de Segurança
Ameaças e Vulnerabilidades

Norma ISO/IEC 17799:2005

- Diretrizes e princípios para melhorar...
  - Gestão de Segurança da Informação da empresa (BS 7799)
- Objetivo:
  - Controles a implementar em função de requisitos levantados em uma Análise de Risco.
- Norma pode servir como um guia prático
  - Desenvolvimento dos procedimentos de segurança
  - Elaboração de políticas
- Foi incorporada à ISO/IEC 27002

Norma ISO/IEC 27002

- Código de Prática para a Gestão de Segurança da Informação (GSI)
- Objetivo
- Estabelecer diretrizes e princípios iniciais, com o intuito de Iniciar, implementar e melhorar a GSI da organização

Norma ISO/IEC 27002 – Tópicos

- Política de Segurança da Informação
  - Formalizada em documento e comunicada claramente; deve ser revisada periodicamente
- Organizando a Segurança da Informação
  - Deve haver uma estrutura gerencial envolvendo representantes estratégicos de diversas áreas.
  - Estabelece acordos de sigilo
- Gestão de Ativos
  - Manter e proteger ativos (Identificar, catalogar e organizar)

Norma ISO/IEC 27002 – Tópicos

- Segurança em Recursos Humanos
  - Descrições de cargos e termos de contratação devem ser explícitos no que tange às responsabilidades de Segurança da Informação.
- Segurança Física e do Ambiente
  – Controle rigoroso, com proteção de equipamentos

Norma ISO/IEC 27002 – Tópicos

- Gestão das Operações e Comunicações
  - Procedimentos e responsabilidades operacionais
  - Diretrizes para gerenciamento de terceirizados
  - Diretrizes para segurança em redes e comunicações
- Controles de Acessos
  - Mecanismos do controle e responsabilização
  - Aspectos sobre computação móvel e teletrabalho
  - Passam por políticas e gerenciamento de privilégios

Norma ISO/IEC 27002 – Tópicos

- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
  - Definição de requisitos para aplicações
  - Uso de controles criptográficos
  - Diretrizes de segurança de arquivos e desenvolvimento
- Gestão de Incidentes de Segurança da Informação
  - Gestão e comunicação de fragilidades
  - Coleta de evidências e mecanismos de análise

Norma ISO/IEC 27002 – Tópicos

- Gestão da Continuidade do Negocio
  - Diretrizes para prevenir interrupção do negócio
  - Recuperação e retomada em tempo mínimo
- Conformidade
  - Orientações para evitar violações legais
  - Diretrizes para identificar a legislação vigente:
    - Proteção de registros e direitos de Propriedade Indústria
    - Proteção de dados e informações pessoais
    - Prevenção de mau uso dos recursos
    - Regulamentação de criptografia

Norma ISO/IEC 27002 – SGSI

- Requisitos para um Sistema de Gestão de Segurança da Informação (SGSI)
  - Deve ser compatível com ISO 9001:2000 e ISO 14001:2004
  - Abordagem de riscos de negócio
  - Norma é trabalhada por processos
  - Ciclo PDCA (Plan, Do, Check e Action)

Conceitos para norma e legislação – Segurança da Informação

Vulnerabilidade

- É uma fraqueza em um sistema, processo, aplicativo ou protocolo que pode ser explorada por uma ameaça para comprometer a segurança do sistema.
- Uma falha que um atacante pode utilizar para burlar o sistema e ter acessos/ privilégios indevidos.
- Tipos de Vulnerabilidade

Tipos de Vulnerabilidade – Software

- São defeitos na programação de um software ou aplicativo que podem ser explorados por um atacante para ganhar acesso não autorizado ao sistema ou executar comandos maliciosos.
- Podem estar presentes em sistemas operacionais, bibliotecas, aplicativos e plug-ins.

Tipos de Vulnerabilidade – Hardware

- Falhas ou fraquezas físicas nos componentes de hardware de um sistema de computador que podem ser exploradas por atacantes para comprometer a segurança do sistema.

Tipos de Vulnerabilidade – Configuração

- Falhas na configuração de sistemas, redes, aplicativos ou dispositivos que podem ser exploradas por atacantes para comprometer a segurança.

Tipos de Vulnerabilidade – Erro humano

- Falhas humanas que permitem exposição do sistema
- Engenharia social
- Não seguir procedimento da empresa
- Levar dispositivos pessoais para o ambiente corporativo

Tipos de Vulnerabilidade – Procedimentos

- Referem-se a lacunas, falhas ou inadequações nos processos e procedimentos implementados por uma organização para garantir a segurança da informação e dos sistemas.
- Essas vulnerabilidades podem resultar em exposição a riscos de segurança significativos.
- Ex: não ter a validação da rotina de backup

Risco

- Refere-se a possibilidade de algo prejudicial acontecer dentro de uma organização
- Tipos de riscos
  - Internos
  - Externos
  - Tecnológicos
  - Físicos
  - Regulatórios e de conformidade

Tipos de Risco – Interno

- Vem de dentro da organização.
- Ações maliciosas de funcionários.

Tipos de Risco – Externo

- Fontes externas a organização

Tipos de Risco – Tecnológicos

- Relacionados a falhas em sistemas, infraestrutura de TI, softwares desatualizados ou mal configurados e dispositivos não seguros.

Tipos de Risco – Físicos

- Relacionados a desastres naturais, incêndios, inundações, roubos e sabotagens.

Tipos de Risco – Regulatórios

- Desafios e ameaças enfrentados pelas organizações devido ao não cumprimento ou violação de regulamentos, leis e normas governamentais ou setoriais.
- Esses riscos podem resultar em penalidades financeiras, litígios, perda de reputação e danos à marca

Incidente

- Evento indesejado que compromete a confidencialidade, integridade ou disponibilidade de dados ou sistemas de informação.
- Estes incidentes podem variar em gravidade e impacto, desde pequenas violações de segurança até grandes incidentes cibernéticos que afetam negativamente uma organização

Tipos de Incidente – Violação de Dados

- Acesso não autorizado a informações confidenciais, como dados pessoais de clientes, informações financeiras ou segredos comerciais.

Tipos de Incidente – Ransomware

- Um tipo de malware que criptografa os dados de uma organização e exige um resgate para restaurar o acesso aos arquivos.

Tipos de Incidente – DDoS

- Ataque de Negacão de Servico (DDoS): Um ataque projetado para sobrecarregar um sistema, rede ou serviço, tornando-o inacessível para usuários legítimos.

Tipos de Incidente – Phishing

- Um ataque que envolve o envio de e-mails fraudulentos que se fazem passar por fontes confiáveis, na tentativa de enganar os destinatários para revelar informações confidenciais, como senhas ou detalhes de cartão de crédito.

Tipos de Incidente – Injeção de SQL

- Uma técnica de ataque na qual um invasor insere comandos SQL maliciosos em uma entrada de formulário da web para obter acesso não autorizado a um banco de dados.

Tipos de Incidente – Ataques de Engenharia Social

- Tentativas de manipular ou enganar os usuários para que divulguem informações confidenciais ou realizem ações que comprometam a segurança.

Tipos de Incidente – Exploração de Vulnerabilidades de Software

- Aproveitamento de falhas de segurança em sistemas ou aplicativos desatualizados para ganhar acesso não autorizado ou comprometer a integridade dos dados.

Tipos de Incidente – Acesso Não Autorizado

- Tentativas de acessar sistemas, redes ou dados sem permissão adequada, seja por meio de credenciais roubadas, engenharia social ou outros métodos.

Tipos de Incidente – Perda ou Roubo de Dispositivos

- Tentativas de acessar por meio físico os dados sensíveis da organização.

Tipos de Incidente – Violação de Conformidade Regulatória

- A não conformidade com regulamentações de segurança da informação.

Atividade

Em equipes (7 pessoas)

- Levando em consideração as notícias relacionadas no trabalho anterior (Pesquisa sobre incidentes)
- Escolher e classificar quais vulnerabilidades foram utilizadas para gerar o incidente. Justificar.
- Identificar o tipo de incidente que a notícia seria classificada
- Indicar o risco que não foi mitigado
- Identificar os tópicos da norma que estão associados aos incidentes

- Entrega do trabalho é única
- Quantidade de notícias é pelo menos 4
- Prazo em conjunto

Referência

Referencias

- CABRAL, Carlos.; CAPRINO, Willian. Trilhas em Segurança da Informação: caminhos e ideias para a proteção de dados. 1. Rio de Janeiro: Brasport, 2015. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/160689

- HINTZBERGEN, Jule. et. al. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.. 1. Rio de Janeiro: Brasport, 2018. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/160044

- Notas de aula do professor Dr. Daniel Caetano.