Faculdade de Tecnologia e Inovação Senac DF

Cursos: **Gestão de Tecnologia da Informação – GTI e Segurança da Informação - TSI**
Disciplina: **Gestão da Segurança da Informação**
Professor: Clenio Emidio
Semestre: 4º GTI e 3º TSI

EMENTA:
Segurança empresarial. Políticas de segurança da informação. Segurança lógica e física. Administrando a segurança da informação. Auditoria das políticas de segurança da informação. Projeto de segurança da informação nas instituições.
Norma ISO (International Organization for Standardization), ISO/IEC 27001:2013, sobre segurança da informação. Análise de riscos. Inventário de ativos de informação.

OBJETIVO GERAL:
Disciplina habilita a tomada de decisão do gestor de segurança da informação, bem como desenvolve competências para que atue em busca da melhoria da segurança da informação organizacional, reconhecendo vulnerabilidades e implantando remediações e controles preventivos.

OBJETIVOS ESPECÍFICOS:
Desenvolvimento de Projeto de Segurança da Informação (PSI) voltado para o atendimentodas normas de segurança da informação nas instituições

COMPETÊNCIAS E HABILIDADES:
Conhecer e aplicar boas práticas de governança de TI; Elaborar, aplicar
e gerenciar normas de segurança em TI;
Planejar, implantar, controlar e auditar processos de TI e de gestão de TI alinhados às estratégias da organização;
Atuar com ética, responsabilidade socioambiental e respeito aos direitos humanos, à diversidade humana e aos demais valores definidos pela organização e pela sociedade.

METODOLOGIA DE ENSINO/APRENDIZAGEM:
Exposição dialogada sobre os temas**,** Pesquisa vançada de assuntos referentes a segurança da informação, Desenvolvimento de resumos baseados nas normas ISO de segurança da informação, Leitura de artigos e publicações.

CONTEÚDO PROGRAMÁTICO:

1. Unidade I – Fundamentos de Segurança da Informação

1.1. Ciclo de vida da informação
1.2. Classificação da informação
1.3. Conceito e objetivos de segurança da informação
1.4. Conceitos básicos
1.5. Ativos e seus tipos
1.6. Ameaças e agentes ameaçadores
1.7. Vulnerabilidades
1.8. Proteções e seus tipos
1.9. Riscos
1.10. Impactos
1.11. Incidentes
1.12. Premissas e mitos da segurança da informação
1.13. Tríade da segurança da informação: confidencialidade, integridade e disponibilidade
1.14. Estratégias de proteção

1.15. Teoria do perímetro
1.16. Norma ISO/IEC 27001

2. Unidade II – Gestão de riscos
2.1. Termos e definições
2.2. Objetivos e benefícios
2.3. Equação do risco
2.4. Fases da implementação da gestão de riscos
2.5. Definição do escopo
2.6. Identificação de ameaças
2.7. Estimar probabilidade e impacto das ameaças
2.8. Identificação dos ativos de maior risco
2.9. Avaliar melhores proteções
2.10. Implementar proteções
2.11. Análise e avaliação dos riscos
2.12. Tratamento do risco
2.13. Aceitação do risco
2.14. Comunicação do risco
2.15. Monitoramento do risco
2.16. Gestão de riscos na ISO/IEC 27001

3. Unidade III – Políticas de segurança da informação (PSI)
3.1. Conceitos e definições
3.2. Estrutura e requisitos
3.3. Elaboração e implementação
3.4. Auditoria e manutenção
3.5. Políticas de segurança na ISO/IEC 27001

4. Unidade IV – Plano de continuidade de negócios (PCN)
4.1. Conceitos e definições
4.2. Gestão da continuidade de negócios
4.3. Tipos de planos
4.4. Planos de contingência
4.5. Plano de administração de crise
4.6. Plano de continuidade operacional
4.7. Plano de recuperação de desastres
4.8. Fases do PCN
4.9. Iniciação
4.10. Análise de impacto nos negócios
4.11. Identificação das estratégias de recuperação: cold-site, warm-site, sister-site, hot-sitee móbile-site
4.12. Projeto, desenvolvimento e implementação
4.13. Testes e simulações
4.14. Manutenção e atualização
4.15. Execução
4.1.6. PCN na ISO/IEC 27001

5. Unidade V - Segurança física e operacional
5.1. Conceitos e definições
5.2. Segurança física x segurança lógica
5.3. Mecanismos de proteção perimetral e de proteção interna
5.4. Teste de invasão física

5.5. Legislação e regulamentação

6. Unidade VI – Segurança lógica

6.1. Tipos de ataques lógicos
- Ataques de malwares: vírus, spywares, trojans e worms
- Ataques de negação de serviço
- Ataques para obtenção de informações
- Ataques de protocolo
- Ataques coordenados
- Ataques em nível de aplicação

6.2. Serviços de segurança lógica
- Autenticação
- Confidencialidade
- Integridade
- Não-repúdio
- Autorização
- Disponibilidade
- Auditoria

6.3. Mecanismos de proteção lógica
- Antivírus, anti-trojan e anti-spyware
- Firewall e DMZ
- Filtros de conteúdo (Proxies)
- Sistemas de detecção de intrusão
- Sistemas de prevenção de intrusão

7. Unidade VII – Segurança organizacional

7.1. Gestão de pessoas em segurança da informação
- Aspectos gerais da comunicação
- Papéis e responsabilidades
- Educação e conscientização
- Cuidados com o turnover, desligamentos e contratações

7.2. Papéis de segurança da informação
- Gestor de segurança da informação (CSO)
- Comitê de segurança
- Consultor de segurança
- Analista de segurança
- Auditor de sistemas de informação
- Equipe de respostas a incidentes

AVALIAÇÃO:
Detalhamento das atividades e provas avaliativas e respectivas notas, com base na Resolução do Conselho Superior nº 03/2019 da Faculdade descrita a seguir:

Art. 1º Regulamentar a forma de avaliação de desempenho escolar do estudante.

Art. 2º O desempenho escolar do estudante é realizado por disciplina, incidindo sobre a frequência e o aproveitamento.

§ 1º Independentemente dos demais resultados obtidos, somente é considerado aprovado o estudante que obtenha frequência de, no mínimo, 75% (setenta e cinco por cento) das aulas e demais atividades programadas na disciplina e média final acima de 6,0 (seis).

§ 2º A verificação e o registro da frequência são de responsabilidade do professor, e o respectivo controle, para efeito do parágrafo anterior, da Secretaria Acadêmica.

Art. 3º O aproveitamento escolar é avaliado por meio de acompanhamento contínuo doestudante e dos resultados por ele obtidos nas avaliações parciais, calculada na Média Parcial (MP) e na avaliação final, calculada na Média Final (MF) expressos em notas de 0(zero) a 10 (dez), apuradas até o primeiro decimal.

§ 1º A apuração do aproveitamento do estudante, de acordo com a natureza da disciplina, éproveniente de, no mínimo, 1 (uma) prova no semestre letivo e de atividades práticas avaliativas, para compor a Nota do Bimestre (NP).

§ 2º A Nota do 1º bimestre letivo pode ser composta por prova e/ou atividades/trabalhosque totalizem 10,0 pontos;

§ 3º A Nota do 2º bimestre letivo deve ser composta pela seguinte pontuação:

a) 2,0 (dois) Avaliação Integrada;
b) 1,0 (um) Participação na Jornada Interdisciplinar
c) 7,0 (sete) Prova e/ou Atividades Avaliativas.

§ 4º O estudante que obtiver Média Final (MF) igual ou superior a 6,0 (seis) será aprovadosem Prova Final (PF).

§ 5º A Média Final (MF) de cada disciplina será calculada aplicando-se média aritmética dasMédias Parciais (MP):

$$MF: \frac{MP\ 1º\ Bim. + MP\ 2º\ Bim.}{2} \geq 6,0\ (seis)$$

§ 6º O estudante que não atingir a Média Final de 6,0 (seis) nas Médias Parciais (MP) e obtiver Média Final (MF) igual ou superior a 2,0 (dois) e inferior a 6,0 (seis) na disciplina, será submetido a Prova Final (PF), abrangendo todo o conteúdo programático da disciplinano valor de 10,0 (dez).

§ 7º A Média Final (MF) de cada disciplina, com a realização da Prova Final (PF) serácalculada aplicando-se a seguinte média aritmética:

$$MF: \frac{MP\ (1º\ e\ 2º\ Bim) + PF}{2} \geq 6,0\ (seis)$$

§ 8º Ao professor compete elaborar um cronograma anexado ao Plano de Ensino da disciplina, amplamente divulgado aos estudantes, estabelecendo o dia de aplicação daprova regular e de 2ª Chamada, e período de realização das atividades avaliativas.

Parágrafo único - O professor que optar por não aplicar prova no 2º bimestre no períododefinido no Calendário Acadêmico, deverá utilizar obrigatoriamente o dia da aula para realizar atividade avaliativa para compor a Média Parcial (MP).

BIBLIOGRAFIA BÁSICA:

LIMA, Adriano. **Gestão da segurança e infraestrutura de tecnologia da informação**. São Paulo: Senac, 2018. (Série Universitária). *E-book.* Disponível em: https://bibliotecadigitalsenac.com.br/

OLIVEIRA, Roberto Carlos Queiroz. **Tópicos de segurança da informação.** São Paulo: SENAC, 2017. (Série Universitária). *E-book.* Disponível em: https://bibliotecadigitalsenac.com.br/

LYRA, Maurício Rocha, Segurança e Auditoria em Sistema de Informação; 1ª Edição; ano:2008; Editora: Ciência Moderna.

BIBLIOGRAFIA COMPLEMENTAR:

MANOTTI, Alessandro; Curso Prático - Auditoria de Sistemas; 1ª edição; ano: 2010; editora:Ciência Moderna

AGUILERA-FERNANDES, Edson. **Padrões, normas e políticas de segurança da informação**. São Paulo: Senac, 2017. (Série Universitária). *E-book.* Disponível em: https://bibliotecadigitalsenac.com.br/