PLANO DE ENSINO: GOVERNANÇA E SEGURANÇA DA INFORMAÇÃO

CARGA HORÁRIA: 66h Teórica: 33h Prática: 33h

EMENTA

Explora os temas de governança em tecnologia com ênfase nas melhores práticas de compliance em segurança da informação adotadas pelo mercado, abordando responsabilidades, métodos, projetos, justificativas, riscos e ferramentas de proteção à informação em ambiente informático.

COMPETÊNCIAS

II. TRABALHAR EM EQUIPE

III. ATINGIR OBJETIVOS

IV. ADAPTAR-SE À MUDANÇA

VI. COMUNICAR-SE ORALMENTE E POR ESCRITO

XII - ADMINISTRAÇÃO E GERENCIAMENTO - Gerenciar recursos, tempo e processos visando a tomada de decisão e a otimização dos resultados.

XIV - VISÃO ESTRATÉGICA - Planejar ações a curto, médio e longo prazo para atingir metas, antecipando tendências e novas oportunidades.

XV - PROJETO DE REDES DE COMPUTADORES - Projetar redes de computadores de acordo com a norma técnica regulamentadora. (CST em Redes de Computadores)

XVI - IMPLEMENTAÇÃO DE REDES DE COMPUTADORES - Implementar projetos lógicos e físicos de redes de computadores. (CST em Redes de Computadores)

XVIII - SEGURANÇA DE REDES DE COMPUTADORES - Projetar, implementar e configurar soluções de segurança em redes. (CST em Redes de Computadores)

XVI - GESTÃO DE REDES DE COMPUTADORES - Gerir redes de computadores e datacenter garantindo o seu funcionamento, controlando o acesso dos usuários e otimizando seus recursos. (CST em Sistemas de Telecomunicações)

OBJETIVOS DE APRENDIZAGEM

Analisar a importância da Segurança da Informação para às organizações e que, quando elevada ao patamar estratégico, pode proporcionar maior vantagem competitiva para a empresa.

Identificar aspectos que envolvem a segurança de redes, e de dispositivos móveis, em diversos ambientes, e implementar medidas que contribuam para a manutenção de um ambiente seguro.

Aplicar seus conhecimentos de forma independente e inovadora, acompanhando a evolução do setor e contribuindo na busca de soluções para diferentes tecnologias de redes de computadores.

Analisar e calcular os riscos relacionados às tecnologias, processos e pessoas.

Planejar um ambiente seguro de forma a permitir a empresa, um controle melhor de suas informações.

CRONOGRAMA DE AULA	
Unidade 1 1. Governança: Gestão da Segurança da Informação 2. A importância da Segurança da Informação para as organizações 3. Norma de segurança 4. Aplicação dos princípios básicos de segurança da informação em empresas, de	**Objetivos de Aprendizagem** ✓ Apontar a importância da Segurança da Informação para às organizações ✓ Identificar os princípios teóricos relacionados à Segurança da Informação nas atividades das empresas ✓ Comparar as estratégias de segurança da informação utilizadas por algumas empresas ✓ Aplicar os princípios básicos de segurança da informação em empresas, de acordo com o mercado em que atua

acordo com o mercado em que atua	✓ Identificar os princípios teóricos relacionados à Segurança da Informação nas atividades das empresas ✓ Comparar as estratégias de segurança da informação utilizadas por algumas empresas ✓ Aplicar os princípios básicos de segurança da informação como uma proposta para uma empresa fictícia. ✓ Apontar a importância de um Sistema de Gestão de Segurança da Informação para às organizações ✓ Identificar as empresas certificadas em Gestão de Segurança da Informação ✓ Descrever os benefícios para uma organização em ter um Sistema de Gestão de Segurança da Informação certificado. ✓ Identificar as normas e padrões de segurança da informação ✓ Descrever os benefícios para uma organização em utilizar normas e padrões nacionais e internacionais ✓ Identificar as normas e padrões de segurança da informação ✓ Descrever os benefícios para uma organização em utilizar normas e padrões nacionais e internacionais
	Estratégias de Ensino
	Utilização de material referencial em diferentes formatos: vídeos, textos de referência conceitual, atividades de pesquisa, estudos de caso, infografias interativas, entre outros. Sequência sugerida: ✓ Explorar a seção "**Inspire-se**" que contextualiza o tema da unidade e traz informações de tendências e inovações na respectiva área de conhecimento, aplicação prática ou estudos de caso, depoimentos ou entrevistas com profissionais qualificados do mercado de trabalho. ✓ Conhecer e entender os conceitos básicos da unidade apresentados na seção **"Explore"**. Neste material são apresentados os aspectos teóricos, exemplos práticos e conteúdos complementares que ampliam o conhecimento sobre as temáticas da unidade. Explorar os vídeos e infografias interativas.
	Atividade
	Atividade não pontuada disponível na seção "**Pratique e Compartilhe**". ✓ Estudos de caso, resoluções, proposta de pesquisa ou produção criativa que integram atividades práticas aos conceitos teóricos básicos da unidade. ✓ As respostas e resultados da atividade proposta devem ser postados no fórum disponível na sessão **"Compartilhe"**. ✓ Após a postagem será disponibilizado feedback com modelo de resposta).
	Avaliação Formativa
	Realizar a "Atividade Avaliativa" que constitui o recurso de avaliação pontuada da unidade. A pontuação desta atividade fará parte da nota final na N1 (ver item "Avaliação" deste plano").
Unidade 2 1. Política de Segurança da Informação e desafios para a adoção nas organizações 2. Estrutura de uma Política de Segurança da Informação 3. Estratégias de Implementação de Políticas de Segurança da Informação e a Importância de Conscientizar os Colaboradores	**Objetivos de Aprendizagem**
	✓ Reconhecer os conceitos relacionados com uma Política de Segurança da Informação, os benefícios e desafios da adoção pelas empresas. ✓ Analisar os desafios da adoção de uma Política de Segurança da Informação nas empresas. ✓ Descrever a estrutura de uma Política de Segurança da Informação. ✓ Identificar estratégias de conscientização em segurança da informação praticadas pelo mercado. ✓ Projetar estratégias de conscientização em segurança da informação.

4. Frameworks envolvidos na Gestão de Riscos	✓ Apontar a importância de medir a efetividade das estratégias de conscientização de diferentes níveis hierárquicos. ✓ Identificar os frameworks envolvidos com a Gestão de Riscos ✓ Descrever as fases da Gestão de Riscos ✓ Reconhecer os conceitos envolvidos com a Gestão de Riscos ✓ Projetar estratégias de segurança da informação para os principais riscos envolvidos com o ambiente de Tecnologia da empresa ✓ Descrever os principais ataques relacionados às Aplicações Web e Mobile ✓ Apontar os principais sites de divulgação de ataques/vulnerabilidade de aplicações (OWASP) ✓ Projetar estratégias de segurança da informação para os principais riscos envolvidos com ataques em aplicações Web e Mobile ✓ Descrever a influência do fator humano no alcance de um ambiente seguro ✓ Projetar estratégias de segurança da informação para os principais riscos envolvidos com pessoas: Engenharia social ✓ Projetar estratégias de segurança da informação para os principais riscos envolvidos malwares
	Estratégias de Ensino
	Utilização de material referencial em diferentes formatos: vídeos, textos de referência conceitual, atividades de pesquisa, estudos de caso, infografias interativas, entre outros. Sequência sugerida: ✓ Explorar a seção "**Inspire-se**" que contextualiza o tema da unidade e traz informações de tendências e inovações na respectiva área de conhecimento, aplicação prática ou estudos de caso, depoimentos ou entrevistas com profissionais qualificados do mercado de trabalho. ✓ Conhecer e entender os conceitos básicos da unidade apresentados na seção **"Explore"**. Neste material são apresentados os aspectos teóricos, exemplos práticos e conteúdos complementares que ampliam o conhecimento sobre as temáticas da unidade. Explorar os vídeos e infografias interativas.
	Atividade
	Atividade não pontuada disponível na seção "**Pratique e Compartilhe**". ✓ Estudos de caso, resoluções, proposta de pesquisa ou produção criativa que integram atividades práticas aos conceitos teóricos básicos da unidade. ✓ As respostas e resultados da atividade proposta devem ser postados no fórum disponível na sessão **"Compartilhe"**. ✓ Após a postagem será disponibilizado feedback com modelo de resposta.
	Avaliação Formativa
	Realizar a "Atividade Avaliativa" que constitui o recurso de avaliação pontuada da unidade. A pontuação desta atividade fará parte da nota final na N1 (ver item "Avaliação" deste plano").
Unidade 3 1.Gestão da Continuidade do Negócio 2. Plano de Continuidade de Negócios: estrutura 3. Plano de Continuidade de Negócios: desenvolvimento 4. Auditoria de Sistemas	**Objetivos de Aprendizagem**
	✓ Identificar os frameworks envolvidos com a Gestão da Continuidade de Negócios ✓ Descrever as fases da Gestão da Continuidade de Negócios ✓ Reconhecer os conceitos envolvidos com a Gestão da Continuidade de Negócios

	✓ Projetar estratégias de Continuidade de Negócios para a continuidade operacional mesmo em situações adversas ✓ Analisar conhecimentos relativos à continuidade de negócios. ✓ Descrever as fases da Gestão da Continuidade de Negócios. ✓ Reconhecer os conceitos envolvidos com a Gestão da Continuidade de Negócios. ✓ Projetar estratégias de Continuidade de Negócios para a continuidade operacional mesmo em situações adversas.
	Estratégias de Ensino
	Utilização de material referencial em diferentes formatos: vídeos, textos de referência conceitual, atividades de pesquisa, estudos de caso, infografias interativas, entre outros. Sequência sugerida: ✓ Explorar a seção "**Inspire-se**" que contextualiza o tema da unidade e traz informações de tendências e inovações na respectiva área de conhecimento, aplicação prática ou estudos de caso, depoimentos ou entrevistas com profissionais qualificados do mercado de trabalho. ✓ Conhecer e entender os conceitos básicos da unidade apresentados na seção **"Explore"**. Neste material são apresentados os aspectos teóricos, exemplos práticos e conteúdos complementares que ampliam o conhecimento sobre as temáticas da unidade. Explorar os vídeos e infografias interativas.
	Atividade
	Atividade não pontuada disponível na seção "**Pratique e Compartilhe**". ✓ Estudos de caso, resoluções, proposta de pesquisa ou produção criativa que integram atividades práticas aos conceitos teóricos básicos da unidade. ✓ As respostas e resultados da atividade proposta devem ser postados no fórum disponível na sessão **"Compartilhe"**. ✓ Após a postagem será disponibilizado feedback com modelo de resposta.
	Avaliação Formativa
	Realizar a **"Atividade Avaliativa"** que constitui o recurso de avaliação pontuada da unidade. A pontuação desta atividade fará parte da nota final na N1 (ver item **"Avaliação"** deste plano")
Unidade 4 1. Compliance 2. Melhores práticas de compliance em TI 3. Auditoria Interna x Compliance 4. Perícia Forense Digital	**Objetivos de Aprendizagem**
	• Analisar conhecimentos relativos à Auditoria de Sistemas. • Reconhecer os conceitos envolvidos com Auditoria de Sistemas. • Elaborar estratégias para a realização de auditoria no ambiente de tecnologia. • Descrever as funcionalidades de auditoria dos sistemas operacionais. • Analisar os conhecimentos relativos à Perícia Forense. • Descrever os conceitos e melhores práticas de Compliance. • Aplicar as melhores práticas para a Gestão de Compliance. • Avaliar as práticas de Compliance.
	Estratégias de Ensino
	Utilização de material referencial em diferentes formatos: vídeos, textos de referência conceitual, atividades de pesquisa, estudos de caso, infografias interativas, entre outros. Sequência sugerida:

	✓ Explorar a seção "**Inspire-se**" que contextualiza o tema da unidade e traz informações de tendências e inovações na respectiva área de conhecimento, aplicação prática ou estudos de caso, depoimentos ou entrevistas com profissionais qualificados do mercado de trabalho. ✓ Conhecer e entender os conceitos básicos da unidade apresentados na seção **"Explore"**. Neste material são apresentados os aspectos teóricos, exemplos práticos e conteúdos complementares que ampliam o conhecimento sobre as temáticas da unidade. Explorar os vídeos e infografias interativas.
	Atividade
	Atividade não pontuada disponível na seção "**Pratique e Compartilhe**". ✓ Estudos de caso, resoluções, proposta de pesquisa ou produção criativa que integram atividades práticas aos conceitos teóricos básicos da unidade. ✓ As respostas e resultados da atividade proposta devem ser postados no fórum disponível na sessão **"Compartilhe"**. ✓ Após a postagem será disponibilizado feedback com modelo de resposta.
	Avaliação Formativa
	Realizar a **"Atividade Avaliativa"** que constitui o recurso de avaliação pontuada da unidade. A pontuação desta atividade fará parte da nota final na N1 (ver item **"Avaliação"** deste plano").
Prova Presencial	Avaliação em formato de prova presencial constituída de atividades múltipla escolha contemplando as quatro unidades da disciplina (ver item **"Avaliação"** deste plano").

AVALIAÇÃO

A Nota Final (NF) da disciplina considera os seguintes elementos e valores:

NOTA N1				NOTA N2
UNIDADE 1	UNIDADE 2	UNIDADE 3	UNIDADE 4	PROVA PRESENCIAL A5
Atividade Avaliativa A1 Avaliação Individual com nota de 0 a 10	Atividade Avaliativa A2 Avaliação Individual com nota de 0 a 10	Atividade Avaliativa A3 Avaliação Individual com nota de 0 a 10	Atividade Avaliativa A4 Avaliação Individual com nota de 0 a 10	Contendo Questões Objetivas e/ou Dissertativas, individual.

Média Final (MF) é calculada com a seguinte média ponderada das duas notas, N1 e N2 e pesos, respectivamente, de 40% e 60%, resultante da seguinte equação:

$$MF = (N1*0,4) + (N2*0,6)$$

Para aprovação, a Nota Final da disciplina deverá ser igual ou superior a 6,0 (seis), além da necessária frequência mínima de 75%, que corresponde a realização de, no mínimo, três das quatro Atividades Avaliativas da N1

O estudante que não atingir a média final 6,0 (seis), poderá realizar uma Prova Substitutiva (A6), cuja nota substituirá a nota da N2 (A5) obtida, caso seja maior.

BIBLIOGRAFIA BÁSICA

BEAL, Adriana. Segurança da informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações. Atlas, 2008. [Minha Biblioteca]
https://integrada.minhabiblioteca.com.br/#/books/9788522472109/
Galvão, Michele Da Costa. Fundamentos de Segurança da Informação. Pearson, 2015. [Minha Biblioteca]

http://anhembi.bv3.digitalpages.com.br/users/publications/9788543009452/pages/-12
IMONIANA, Joshua Onome. Auditoria de Sistemas de Informação, 3ª edição. Atlas, 03/2016. [Minha Biblioteca].
https://integrada.minhabiblioteca.com.br/#/books/9788597005745/cfi/6/2!/4/2/2@0:0

BIBLIOGRAFIA COMPLEMENTAR

CANONGIA, Claudia; MANDARINO JUNIOR, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação. Parcerias Estratégicas, v. 14, n. 29, p. 21-46, 2010. http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/view/349
DA SILVA ETGES, Ana Paula Beck; DE SOUZA, Joana Siqueira. Estudo de campo sobre Gestão de Riscos Corporativos em empresas participantes de um Parque Científico e Tecnológico. International Journal of Knowledge Engineering and Management (IJKEM), v. 4, n. 8, p. 23-42, 2015. http://stat.cbsm.incubadora.ufsc.br/index.php/IJKEM/article/view/3286
JÚNIOR, Armando Kolbe. Sistemas de Segurança da Informação na era do conhecimento. InterSaberes, 2017. [Minha Biblioteca] http://anhembi.bv3.digitalpages.com.br/users/publications/9788559723038/pages/-2
MOREIRA, Nilton Stringasci. A segurança da informação na pequena e média empresa: Um instrumento alavancador de vantagem competitiva. FaSCi-Tech, v. 1, n. 6, 2016. http://www.fatecsaocaetano.edu.br/fascitech/index.php/fascitech/article/view/61/60
STALLINGS, William. Criptografia e segurança de redes: princípios e práticas. Pearson Prentice Hall, 2008. http://anhembi.bv3.digitalpages.com.br/users/publications/9788576051190/pages/_5