UNIVERSIDADE FEDERAL DO CEARÁ

UNIVERSIDADE FEDERAL DO CEARÁ
PRÓ-REITORIA DE GRADUAÇÃO
COORDENADORIA DE PROJETOS E ACOMPANHAMENTO CURRICULAR
DIVISÃO DE DESENVOLVIMENTO CURRICULAR

FORMULÁRIO PARA CRIAÇÃO E/OU REGULAMENTAÇÃO DE DISCIPLINA

(X) **Regulamentação** (se a disciplina está prevista no Projeto Pedagógico)

( ) **Criação/Regulamentação** (se a disciplina não está prevista no Projeto Pedagógico)

1. Unidade Acadêmica que oferta a Disciplina (Faculdade, Centro, Instituto, *Campus*)**:**
Campus Quixadá

2. Departamento que oferta a Disciplina (quando for o caso)**:**
--

3. Curso(s) de Graduação que oferta(m) a disciplina

Código do Curso	Nome do Curso	Grau do Curso[1]	Currículo (Ano/ Semestre)	Caráter da Disciplina[2]	Semestre de Oferta[3]	Habilitação[4]
402	Engenharia de Software	Bacharelado	2010.1	Optativa	5º	--
404	Ciência da Computação	Bacharelado	2013.1	Optativa	7º	--

4. Nome da Disciplina:
Segurança

5. Código da Disciplina (preenchido pela PROGRAD)**:**
QXD0069

6. Pré-Requisitos	Não (X)	Sim ( )	
		Código	Nome da Disciplina/Atividade
		QXD0021 (404)	Redes de Computadores

7. Correquisitos	Não (X)	Sim ( )	
		Código	Nome da Disciplina/Atividade

8. Equivalências		Sim ( )

[1] **Preencher com *Bacharelado, Licenciatura* ou *Tecnólogo*.**
[2] **Preencher com *Obrigatória, Optativa* ou *Eletiva*.**
[3] **Preencher quando obrigatória.**
[4] **Quando eletiva, preencher com a habilitação ou ênfase a que se vincula a disciplina.**

	Não (X)	Código	Nome da Disciplina/Atividade

9. Turno da Disciplina (é possível marcar mais de um item)**:**
(X) Matutino (X) Vespertino ( ) Noturno

10. Regime da Disciplina:
(X) Semestral ( ) Anual ( ) Modular

11. Justificativa para a criação/regulamentação desta disciplina – Máximo de 500 caracteres
(mostrar a importância da área / do conteúdo para a formação do aluno, a pertinência da disciplina na integralização curricular e outros aspectos):
A disciplina de Segurança visa capacitar o profissional a lidar com as mais diversas tecnologias de segurança da informação, habilitando-o a reconhecer riscos e ameaças ao ciclo de vida dos ativos de informação e a aplicar tais tecnologias para exercer o controle sobre o ciclo e a sua auditoria.

12. Objetivo(s) da Disciplina:
Objetivo Geral:
O aluno, ao final do semestre, deverá ser capaz de reconhecer o valor da informação para as organizações, suas principais ameaças e vulnerabilidades e as normas que formalizam as formas de proteção.

Objetivos específicos
- Reconhecer o valor intrínseco das informações para as organizações e para os indivíduos;
- Reconhecer e relacionar os principais riscos envolvidos no ambiente de informações;
- Descrever e explicar ferramentas e procedimentos com relação à segurança da informação - nos aspectos de segurança lógica, física e ambiental;
- Reconhecer e relacionar os principais pontos de controle de auditoria da tecnologia da informação no que se refere à auditoria do desenvolvimento e manutenção de sistemas, administração de dados, administração de banco de dados, administração de redes de computadores;
- Reconhecer e evitar vulnerabilidades na confecção de software.

13. Ementa:
Ameaças. Segurança como atributo qualitativo de projeto de software. Autenticação. Autorização. Integridade. Confidencialidade. Criptografia (chaves simétricas e assimétricas). Infraestrutura de chaves públicas brasileiras (ICP-Brasil). Certificados digitais. Assinaturas digitais. Desenvolvimento de software seguro. Noções de auditoria de sistemas. Norma NBR 27002.

14. Descrição da Carga Horária

Número de Semanas:	Número de Créditos:	Carga Horária Total:	Carga Horária Teórica:	Carga Horária Prática:
16	4	64	32	32

15. Bibliografia Básica (sugere-se a inclusão de, pelo menos, 03 títulos)**:**

IMONIANA, Joshua Onome. Auditoria de sistemas de informação. 2. ed. São Paulo: Atlas, 2008. 207 p. ISBN 9788522450022 (broch.).

STALLINGS, William. Criptografia e segurança de redes: princípios e práticas. 4. ed. São Paulo: Pearson/ Prentice Hall, 2008. 492 p. ISBN 9788576051190 (broch.).

BEAL, Adriana. Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo, SP: Atlas, 2008. 175 p. ISBN 9788522440856 (broch.).

16. Bibliografia Complementar (sugere-se a inclusão de, pelo menos, 05 títulos – de acordo com instrumento de avaliação de Curso de Graduação, INEP/maio-2012 ou legislação posterior)**:**

DASWANI, Neil; KERN, Christoph; KESAVAN, Anita. Foundations of security: what every programmer needs to know . Berkeley, Ca: Apress, 2007. 290 p. (The Expert's voice in security) ISBN 9781590597842 (broch.).

KUROSE, James F.; ROSS, Keith W. Redes de computadores e a Internet: uma abordagem top-down. 5. ed. São Paulo: Pearson Addison Wesley, 2010. xxii, 614 p. ISBN 9788588639973 (broch.).

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. Segurança de redes em ambientes cooperativos. São Paulo: Novatec, c2007. ISBN 9788575221365 (broch.).

STATO FILHO, André. Linux: controle de redes. Florianópolis: Visual Books, 2009. 352 p. ISBN 9788575022443 (broch.).

ULBRICH, Henrique Cesar; DELLA VALLE, James. Universidade H4CK3R: desvende todos os segredos do submundo dos hackers . 6. ed. São Paulo: Digerati Books, 2009. 348p. (Série Universidade) ISBN 9788578730529 (broch).

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001- Tecnologia da informação - técnicas de segurança - sistemas de gestão de segurança da informação - requisitos. Rio de Janeiro, RJ, 2006. 34 p. [recurso eletrônico]

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002- Tecnologia da informação - técnicas de segurança - código de prática para a gestão da segurança da informação. Rio de Janeiro, RJ, 2005. 120 p. ISBN 9788507006480. [recurso eletrônico]

17. Aprovação do Colegiado do Departamento (quando for o caso)	
Data de Aprovação:	_____ Chefe(a) do Departamento **Assinatura e Carimbo**

18. Aprovação do(s) Colegiado(s) de Curso(s)		
Código do Curso:	**Data de Aprovação:**	_____ Coordenador(a) do Curso **Assinatura e Carimbo**
Código do Curso:	**Data de Aprovação:**	_____ Coordenador(a) do Curso **Assinatura e Carimbo**

19. Aprovação do Conselho da Unidade Acadêmica	
Data de Aprovação:	_____ Diretor(a) da Unidade Acadêmica **Assinatura e Carimbo**

20. Aprovação do Conselho de Ensino, Pesquisa e Extensão (Câmara de Graduação)	
Data de Aprovação:	_____ Presidente(a) da Câmara de Graduação **Assinatura e Carimbo**

Orientações para tramitação do processo:
Deve ser aberto e encaminhado processo à Pró-Reitoria de Graduação / Câmara de Graduação, contendo: 1) Ofício(s) informando a data de aprovação da criação e/ou regulamentação da(s) disciplina(s) pela Coordenação do Curso, pelo(s) Departamento(s) envolvido(s) – se for o caso – e pela Direção da Unidade Acadêmica; 2) Formulário para Criação e/ou Regulamentação de Disciplina integralmente preenchido, com assinaturas, datas e carimbos solicitados.

ANEXO - Descrição do Conteúdo e Carga Horária

Descrição do Conteúdo e Carga Horária					
Unidades e Assuntos das Aulas			**Nº de Horas Teóricas**	**Nº de Horas Práticas**	**Nº de Horas EaD (quando for o caso):**
1. Introdução à Segurança			2		
2. Princípios de Segurança em Rede e Tipos de Ataques			2		
3. Criptografia Simétrica e Assimétrica; distribuição de chaves			4	2	
4. Autenticação, Assinatura Digital e Hash			2	2	
5. Firewall e Proxy				2	
6. Ameaças e Vulnerabilidades			2	6	
7. Segurança da Informação			4	2	
8. ISO/IEC 17799:2005 – Boas Práticas, ISO/IEC 27001:2006 – Requisitos de Certificação e ISO/IEC 27002:2005 – Gerenciamento de Segurança			8		
9. Política de Segurança da Informação			4		
10. Análise de Risco e Plano de Contingência			2	6	
11. Auditoria de Sistemas			2	4	
12. Bugs de Código				4	
13. Boas Práticas de Codificação				4	
Número de Semanas:	**Número de Créditos:**	**Carga Horária Total:**	**Carga Horária Teórica:**	**Carga Horária Prática:**	**Carga Horária EaD:**
16	4	64	32	32	