



EMENTA DE CURSO

1. **Nome do curso: Introdução à Segurança da Informação Corporativa**
2. **Objetivo Geral:** Estimular os profissionais para gestão de segurança de informação em seus órgãos, minimizando impactos diretos no cotidiano das organizações e estimulando a implantação e políticas e/ou controles.
3. **Carga Horária:** 20 horas/aula.
4. **Conteúdo Programático:**
 1. **Introdução aos conceitos da Segurança da Informação**
 - 1.1. Considerações iniciais
 - 1.2. Conceitos fundamentais
 - 1.3. Princípios Auxiliares
 - 1.4. Segurança nas organizações - visão de negócio
 - 1.5. Ciclo de Segurança da Informação
 - 1.6. Conceitos de Ameaças e Vulnerabilidade
 - 1.7. Ataques e Contramedidas
 - 1.8. Crimes cibernéticos
 - 1.9. Tecnologias e suas vulnerabilidades
 - 1.10. Tecnologias para a segurança da informação
 - 1.11. Padrões, metodologias e práticas de segurança da informação
 2. **Princípios de governança de segurança da informação**
 - 2.1. Conceitos de governança aplicada à segurança da informação
 - 2.2. Regras de segurança e Responsabilidades
 - 2.3. Estratégia de segurança da informação
 - 2.4. Frameworks para governança de segurança da informação
 3. **Gerenciamento de Risco**
 - 3.1. Conceitos de risco
 - 3.2. Análise de risco
 - 3.3. Padrões e normas
 - 3.4. Plano de Gerenciamento de Risco
 - 3.5. Plano de Continuidade de negócios
 4. **Desenvolvimento e Implantação de Política de segurança da Informação**
 - 4.1. Contexto jurídico e regulamentar
 - 4.2. Normas, procedimentos e diretrizes
 - 4.3. Metodologia de desenvolvimento e implantação
 - 4.4. Políticas de Segurança existentes no Estado



5. Tratamento de Ameaças

- 5.1. Conceito de Incidente
- 5.2. Processo de modelagem para o tratamento de ameaças
- 5.3. Tecnologias e processos de mitigação
- 5.4. Equipe de Resposta e Tratamento de Incidentes

6. Compliance

- 6.1. Modelo GRC
- 6.2. Legislações e marcos regulatório
- 6.3. Marco Civil da Internet
- 6.4. LGPD - Lei Geral de Proteção de Dados

4. Metodologia:

Metodologia de Ensino:

As aulas serão baseadas em exposições dialogadas com práticas e dinâmicas nos conceitos do curso. O curso será realizado com uso da ferramenta Microsoft Teams, uma plataforma unificada de comunicação e colaboração que combina bate-papo, videoconferências, armazenamento de arquivos. O tutor e alunos estarão no mesmo horário na plataforma. O aluno terá acesso à apostila, slides e exercícios através da plataforma.

Metodologia de Avaliação de Aprendizagem:

Ao término do curso, os alunos serão avaliados na própria ferramenta Microsoft Teams por meio de prova online com 10 (dez) questões, sendo 01 (um) ponto por questão, cuja nota mínima para aprovação do curso é 7,0 (sete) pontos. A primeira prova estará disponível no 1º dia útil imediatamente posterior ao fim do curso. A segunda prova (opcional e de recuperação de nota) estará disponível no 2º dia útil imediatamente posterior ao fim do curso. A frequência será feita no horário da aula ao vivo por meio de recursos da ferramenta Microsoft Teams, o aluno precisa ter 80% de frequência.

5. Bibliografia:

ABNT. Segurança da informação. Norma ISO/IEC 27000.



ALEXANDER, Philip., Information security. A manager's guide to thwarting data thieves and hackers., Praeger Security International, 2008, ISBN-13: 978-0-313-34558-6

ALVES, Gustavo Alberto. Segurança da Informação: uma visão inovadora da gestão. Rio de Janeiro: Ciência Moderna Ltda, 2006

ANDRESS, Jason., Foundations of information security, A Straightforward Introduction., No Starch Press, San Francisco, 2019, ISBN-13: 978-1-7185-0004-4

ANDRESS, Jason; LEARY, Mark., Building a Practical Information Security Program., Syngress Media, Inc., 2017, ISBN: 978-0-12-802042-5

BACIK, Sandy., Building an Effective Information Security Policy Architecture., CRC Press, 2008, ISBN 978-1-4200-5905-2

BEAVER, Kevin; DAVIS, Peter T., Hacking Wireless Networks For Dummies., Wiley Publishing, Inc, 2005, ISBN-13: 978-0-7645-9730-5

BENIAS, Nikolaos; LEVENTOPOULOS, Sozon A., Cyber warfare: a beyond the basics approach., Nova Science Publishers, Inc., Capítulo 4, 2019, ISBN: 978-1-53614-385-0

BIDGOLI, Hossein., Handbook of information security Volume 1, Key Concepts, Infrastructure, Standards, and Protocols, John Wiley & Sons, Inc., 2006, ISBN-13: 978-0-471-64830-7

BIDGOLI, Hossein., Handbook of information security Volume 2, Information Warfare; Social, Legal, and International Issues; and Security Foundations, John Wiley & Sons, Inc., 2006, ISBN-13: 978-0-471-64831-4

BIDGOLI, Hossein., Handbook of information security Volume 3, Threats, Vulnerabilities, Prevention, Detection, and Management, John Wiley & Sons, Inc., 2006, ISBN-13: 978-0-471-64832-1

BIDWELL, Teri., Hack proofing your identity in the information age, Protect Your Family on the Internet!, Syngress Publishing, Inc., 2002, ISBN: 1-931836-51-5

BLOCH, Matthieu; BARROS, João., Physical-Layer Security From Information Theory to Security Engineering., Cambridge University Press, 2011, ISBN 978-0-521-51650-1

BURGESS, Christopher; POWER, Richard., Secrets Stolen, Fortunes Lost: Preventing Intellectual Property Theft and Economic Espionage in the 21st Century, Syngress Publishing, Inc., 2008, ISBN-13: 978-1-59749-255-3

CALASHAIN, Tara., Google Hacks, 100 Industrial-Strength Tips & Tools., O'REILLY, 2002

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL – Cert.br. Cartilha de Segurança para internet. Disponível em:<<http://cartilha.cert.br/glossario>>

COLE, Dr. Eric; RING, Sandra., Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft., Springer Nature, Switzerland, 2016, ISBN: 1-59749-048-2

DYNAMICS, SPI., SQL Injection Are Your Web Applications Vulnerable?, Artigo da SPI Dynamics, Inc, 2002.

FERREIRA, Fernando N. F. Segurança da Informação. Rio de Janeiro: Ciência Moderna. 2003.



FINK, Steven., Sticky fingers : managing the global risk of economic espionage., Dearborn Trade, a Kaplan Professional Company, 2002, ISBN 0-7931-4827-8

FORESTI, Sara; LOPEZ, Javier., Information Security Theory and Practice., Springer Nature, Switzerland, 2016, ISBN 978-3-319-45931-8

GORDON, Adam (ISC)2 Official (ISC)2 Guide to the CISSP CBK, Fourth Edition. 2015

GRAVES, Kimberly., CEH Official Certified Ethical Hacker, Review Guide., Wiley Publishing, Inc., Indianapolis, Indiana, 2007, ISBN-13: 978-0-7821-4437-6

GREENBERG, Michael R., Explaining risk analysis: Protecting health and the environment., 1ª Edição. Routledge, 2017, ISBN: 978-1-315-64757-9.

GREENBERG, Michael R., Explaining Risk Analysis - Protecting health and the environment., Routledge, 2017, ISBN: 978-1-315-64757-9

GREGORY, Peter H., Enterprise Information Security, Information security for non-technical decision makers., Pearson Education Limited, 2003, ISBN 0-273-66157-4

GUPTA, Jatinder N.D.; SHARMA, Sushil K., Handbook of Research on Information Security and Assurance, IGI Global, 2009, ISBN 978-1-59904-856-7

GUPTA, Manish; SHARMAN, Raj., Social and Human Elements of Information Security: Emerging Trends and Countermeasures, IGI Global, 2009, ISBN 978-1-60566-037-0

HENDERSON, Lance., TOR and the Dark Art of Anonymity, How to Be Invisible From NSA Spying., Lance Henderson, 2015.

HERZOG, Pete; TRUETT, Check; BARCELÓ, Marta; TRUETT, Kim, Hacker Highschool, Security Awareness fir Teens., www.isecom.org, 2000-2004

HORTON, Mike; MUGGE, Clinton., Hacknotes - Network Security Portable Reference, McGraw-Hill/Osborne, 2003, ISBN 0-07-222783-4

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. Infraestrutura de Chaves Públicas Brasileira. Disponível em:< <http://www.iti.gov.br/index.php/icp-brasil/o-que-e>>.

LONG, Johnny; PINZON, Scott; WILES, Jack., No Tech Hacking: A guide to social engineering, dumpster diving, and shoulder surfing., Syngress Publishing, Inc., 2008, ISBN-13: 978-1-59749-215-7

LUDWIG, Mark., The Little Black Book of Computer Viruses., Eletronic Edition, American Eagle Publications, Inc., 1996, ISBN 0-929408-02-0

McCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George., Hacking exposed: network security, secrets and solutions, third edition, Osborne/McGraw-Hill, 2001, ISBN 0-07-219381-6

MITNICK, Kevin D.; SIMON, William L., The art of intrusion, The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers, Wiley Publishing, Inc., Indianapolis, Indiana. 2005, ISBN 0-7645-6959-7

MITNICK, Kevin d.; SIMON, William L., The art of deception, Controlling the Human Element of Security., Ed. Banned, 2001, ISBN-13 978-0764542800

NASHERI, Hedieh., Economic Espionage and Industrial Spying., Cambridge University Press, 2005, ISBN-13 978-0-511-08074-6



O'DEA, Michael., HackNotes: Windows Security Portable Reference, McGraw-Hill/Osborne, 2003, ISBN 0-07-222785-0

O'HANLEY, Richard; TILLER, James S., Information Security Management Handbook; Sixth Edition; Volume 7., CRC PRESS - Auerbach Publication Taylor & Francis Group, 2014, ISBN-13: 978-1-4665-6752-8

OGAWA, Kazuto; YOSHIOKA, Katsunari, Advances in Information and Computer Security, 11th International Workshop on Security, IWSEC 2016., Springer Nature, Switzerland, 2016, ISBN 978-3-319-44524-3.

PELTIER, Thomas R., Information Security Fundamentals. Second Edition., CRC Press, 2014.

PELTIER, Thomas R., Information Security Policies and Procedures, A Practitioner's Reference, Second Edition, CRC PRESS - Auerbach Publication Taylor & Francis Group, 2004, ISBN-13: ISBN 0-203-48873-3

PELTIER, Thomas R., Information Security Risk Analysis, Third Edition, CRC PRESS - Auerbach Publication Taylor & Francis Group, 2010, ISBN-13: ISBN 978-1-4398-3956-0

PIOTROWSKI, Michal., Dangerous Google – Searching for Secrets., Artigo publicado na Hacking magazine, edição 4/2005

POULSEN, Kevin L., Hack Proofing Your Network: Internet Tradecraft., Syngress Media, Inc., 2000, ISBN: 1-928994-15-6

PRASAD, Ramjee; ROHOKALE, Vandana., Cyber Security: The Lifeline of Information and Communication Technology., Springer Nature, Switzerland, 2020, ISBN 978-3-030-31703-4

RHODES-OUSLEY, Mark., Information Security, The Complete Reference., McGraw-Hill Companies. 2013, Segunda Edição, ISBN: 978-0-07-178436-8

ROGERS, Russ., Hacking a Terror Network - The silent threat of covert channels, Syngress Publishing, Inc., 2005, ISBN: 1-928994-98-9

SCAMBRAY, Joel; SHEMA, Mike., Hacking exposed web applications., McGraw-Hill, 2002, ISBN 0-07-222438-X

SCOTTO, Procolo., Darknet Master, TOR and Deep Web Secrets., e-book, 2020.

SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva. Rio de Janeiro: Campus.2003.

Syngress., Hack Proofing Your Network: Internet Tradecraft., Syngress Media, Inc., 2000, ISBN: 1-928994-15-6

SYSTEMS, Internet Security, Ethical Hacking, Student Guide., Internet Security Systems, Inc., 2000

TIPTON, Harold F.; KRAUSE, Micki., Information Security Management Handbook. Sixth Edition., CRC PRESS - Auerbach Publication Taylor & Francis Group, 2007, ISBN-13: 978-0-8493-7495-1

WHITMAN, Michael E.; MATTORD, Herbert J., Management of Information Security, Fourth Edition, Cengage Learning, 2014, ISBN-13: 978-1-285-06229-7