



Serviço Nacional de Aprendizagem Industrial
Departamento Regional de São Paulo

Faculdade SENAI de Tecnologia
de Santos

PROJETO DO CURSO DE PÓS-GRADUAÇÃO
LATO SENSU

SEGURANÇA EM REDES CIBERNÉTICAS

Eixo Tecnológico: Tecnologia da Informação

SANTOS – 2020

Sumário

1. TÍTULO: SEGURANÇA EM REDES CIBERNÉTICAS.....	2
2. JUSTIFICATIVA.....	2
3. HISTÓRICO DA INSTITUIÇÃO	4
4. OBJETIVOS.....	7
5. PÚBLICO-ALVO	8
6. CONCEPÇÃO DO PROGRAMA	8
7. COORDENAÇÃO DO PROGRAMA.....	9
8. CARGA HORÁRIA	9
9. PERÍODO E PERIODICIDADE	10
10. CONTEÚDO PROGRAMÁTICO.....	11
11. CORPO DOCENTE	19
12. METODOLOGIA	20
13. ATIVIDADES COMPLEMENTARES.....	20
14. RECURSOS.....	21
15. CRITÉRIO DE SELEÇÃO.....	28
16. SISTEMAS DE AVALIAÇÃO	28
17. CONTROLE DE FREQUÊNCIA	29
18. MONOGRAFIA	29
19. CERTIFICAÇÃO	30
20. INDICADORES DE DESEMPENHO	30

1. TÍTULO: SEGURANÇA EM REDES CIBERNÉTICAS

O curso de pós-graduação *lato sensu* Segurança em Redes Cibernéticas está inserido na área de conhecimento tecnológico Tecnologia da Informação e será oferecido de forma presencial.

2. JUSTIFICATIVA

A segurança de redes industriais tem sido evidenciada como uma das prementes necessidades da chamada indústria 4.0, muito em função da característica de integração na qual esta nova revolução industrial se apoia. Neste sentido, a sociedade da informação e do conhecimento, juntamente com a globalização, tem gerado novas demandas relacionadas à preservação de dados, bloqueio de invasões e desenvolvimento de técnicas de impedimento de ataques maliciosos nas referidas redes e nos dispositivos de campo que dela fazem parte.

A área de dispositivos de segurança em redes industriais é populada por fabricantes de equipamentos diversos, que cumprem papéis específicos na cadeia de automação constituída por roteadores, gateways, firewalls e outros equipamentos que estão evoluindo constantemente com a disseminação de novas tecnologias e técnicas para proteção de dados industriais.

2.1 Necessidades reais e potenciais de profissionais requeridos pelo mercado

A demanda de especialistas na área de cibersegurança, com expertise no meio industrial e com uma visão atualizada das tecnologias disponíveis no mercado com relação à segurança das redes industriais tem sido evidenciada nos principais estudos e relatórios emitidos por instituições nacionais e internacionais como, por exemplo, no último relatório *“The Future of Jobs Report”* elaborado em 2018 pelo Fórum Econômico Mundial.

O curso de Pós-Graduação Lato Sensu de Segurança em Redes Cibernéticas foi elaborado com foco no atendimento às demandas evidenciadas nestes estudos, tendo como cerne a capacitação e a pesquisa para o desenvolvimento de técnicas de proteção de equipamentos industriais, e seus respectivos softwares de supervisão/controlado que, conectados à nuvem, atendem à automação avançada de fábricas cada vez mais integradas, viabilizando a convergência da indústria nacional aos patamares tecnológicos inerentes à 4ª revolução industrial.

Considerando a vocação, experiência e recursos na área da instrumentação e automação industrial, a Faculdade SENAI de Tecnologia de Santos decidiu implantar o curso de Pós-

Graduação Lato Sensu de Segurança em Redes Cibernéticas, que vem complementar a formação profissional dos cursos de graduação oferecidos por esta e outras instituições de ensino da região.

Esta iniciativa beneficiará a comunidade local propiciando maior especialização ao profissional, que estará preparado para atender às demandas do mercado e gerenciar sua própria carreira. Além disso, fortalecerá a educação profissional do país, intensificando a geração e o uso efetivo do conhecimento e garantindo capital humano para as indústrias otimizarem seus recursos técnicos e tecnológicos.

O programa foi concebido para suprir o mercado com especialistas com a capacidade de desenvolver técnicas e políticas para proteção em redes industriais, capacitando-os a conceber e implementar tecnologias para proteção de redes e dispositivos, efetuar testes de penetração nas redes industriais, elaborar relatórios de segurança e efetuar gerenciamento de contingência em sistemas cibernéticos, além de outros aspectos relacionados à área de cibersegurança industrial.

A vinculação entre teoria e prática, aspecto fundamental na metodologia adotada no curso, é praticada por meio de aulas expositivas existentes com o objetivo de fundamentar as atividades em laboratórios realizadas com equipamentos industriais e didáticos adquiridos com recursos próprios da instituição e por meio de parcerias com empresas da área de automação e tecnologia da informação.

3. HISTÓRICO DA INSTITUIÇÃO

A Escola SENAI "Antônio Souza Noschese" foi inaugurada em 1957, graças a uma grande mobilização desencadeada pelo jornal "A Tribuna" de Santos. Este veículo de comunicação acreditava que era necessária a formação de mão de obra específica visando responder às demandas das atividades industriais e portuária, principalmente depois da inauguração da Refinaria Presidente Bernardes em Cubatão. Com esse pensamento, tornava-se indispensável a instalação de uma unidade do SENAI na Baixada Santista para consolidar a criação de um complexo industrial na região. Com localização privilegiada e estrutura física e ambiental agradável, a Escola vem, ao longo dos anos, atendendo às necessidades da indústria e da comunidade em relação à formação e preparação de mão de obra e à prestação de serviços.

Pioneira na área de Instrumentação Industrial, a Escola SENAI de Santos procura corresponder às necessidades das organizações industriais em todo o território nacional, além de prestar serviços a clientes de outros países, como já ocorreu com alunos provenientes da Bolívia, Angola e Guatemala.

A área de atuação da escola compreende os municípios de Santos e São Vicente. Além destes, a Escola atende os municípios do Litoral Sul de São Paulo e do Vale do Ribeira, abrangendo vinte cidades, onde vivem aproximadamente 1.500.000 habitantes.

A configuração econômica da região se dá em razão do setor da construção civil, do porto de Santos (que abrange as cidades de Santos, Guarujá e Cubatão), das indústrias de base localizadas principalmente em Cubatão, do turismo e do setor primário (agricultura e extrativismo), predominante no Litoral Sul e Vale do Ribeira.

A Escola completou 60 anos em 2017, promovendo grandes mudanças nas atividades de Educação Profissional, em sintonia com a modernização da área portuária e do advento das oportunidades do segmento de petróleo e gás da Bacia de Santos. Respondendo às novas necessidades da comunidade da Baixada Santista, no segundo semestre de 2012, foi implantado o Curso Técnico em Portos, cujo objetivo é preparar trabalhadores de acordo com o perfil requerido pelo mercado. Mesmo com a implantação desse curso, a Escola não se descuida em oferecer produtos de conteúdos tecnológicos sempre atualizados (Formação Inicial e Continuada).

Alinhada com a Missão da Instituição, a Escola preocupa-se em atender às organizações industriais, portuárias e àquelas vinculadas ao setor de petróleo e gás, além de desenvolver cursos *in company* de acordo com as necessidades específicas de seus clientes. A Unidade,

acompanhando o dinamismo e o desenvolvimento econômico dos municípios da região em que atua qualifica profissionais para as diferentes áreas tecnológicas, tais como: Automobilística, Mecânica, Eletroeletrônica, Informática, Instrumentação e Vestuário. A partir dessa visão, a Unidade passou a oferecer, no ano de 2013, o Curso Superior em Tecnologia de Instrumentação Industrial.

Contando com uma forte e moderna base tecnológica instalada e recursos humanos de elevada competência, a Escola SENAI “Antônio Souza Noschese” passou a abrigar, a partir de 2013, a Faculdade SENAI de Tecnologia de Santos, na cidade de Santos-SP, por decisão do Conselho Regional do SENAI-SP, como unidade vinculada à Faculdade SENAI de Tecnologia Mecatrônica, nos termos do § 3o , do art. 20, da Lei nº 12.513, de 26/10/2011, DOU-27/10/2011, alterada pela Lei nº 12.816, de 05/06/2013, DOU-06/06/2013.

A unidade vinculada denominada Faculdade SENAI de Tecnologia de Santos, está localizada na cidade de Santos, Estado de São Paulo, a área de atuação compreende os municípios de Santos e São Vicente, além de municípios do Litoral Sul do Estado de São Paulo e do Vale do Ribeira, abrangendo 22 municípios, que fazem parte da Região Metropolitana da Baixada Santista.

A Região Metropolitana da Baixada Santista foi criada mediante Lei Complementar Estadual 815, em 30 de julho de 1996, tornando-se a primeira região metropolitana brasileira sem status de capital estadual.

Estende-se sobre municípios pertencentes tanto à Mesorregião de Santos (sobrepota à Microrregião de Santos) quanto à Mesorregião do Litoral Sul Paulista (mais precisamente, à Microrregião de Itanhaém). Todos os municípios da Região Metropolitana integram o litoral de São Paulo.

A região abrange 2 419,930 quilômetros quadrados (corresponde a menos de 1% da superfície do estado de São Paulo). É a 15ª região metropolitana mais populosa do Brasil, com uma população de cerca de 1,7 milhão de moradores fixos, e faz parte do Complexo Metropolitano Expandido, uma megalópole que compreende 12% da população brasileira, ou cerca de 30 milhões de habitantes. Nos períodos de férias, acolhe igual número de pessoas, que se instalam na quase totalidade em seus municípios.

A região caracteriza-se pela grande diversidade de funções presentes nos municípios que a compõem. Além de contar com o parque industrial de Cubatão e o Complexo Portuário de

Santos, ela desempenha outras funções em nível estadual, como as atividades industrial e de turismo, e outras de abrangência regional, como as relativas aos comércios atacadista e varejista, ao atendimento à saúde, educação, transporte e sistema financeiro. Têm presença marcante ainda na região as atividades de suporte ao comércio de exportação, originadas pela proximidade do complexo portuário.

Com aproximadamente 13 km de cais, quase 500 mil m² de armazéns, o Porto de Santos, maior e mais importante complexo portuário da América do Sul, movimenta anualmente 76 milhões de toneladas, entre carga geral, líquidos e sólidos a granel e mais de 40% do movimento nacional de contêineres, ou seja, de cada cinco contêineres embarcados ou desembarcados na costa brasileira, dois passam pelo Porto de Santos. Para o Estado de São Paulo, a presença do Porto representa enorme avanço econômico, permitindo o direcionamento de grande parcela de suas atividades industriais e agrícolas para o suprimento de mercados internacionais.

As atividades industriais, localizadas predominantemente em Cubatão, importante polo siderúrgico em escala regional, assim como as portuárias em Santos e as ligadas ao comércio, serviços e atividades de turismo e veraneio têm reflexos diretos na economia da região e respondem pela geração de um Produto Interno Bruto de R\$ 52,3 bilhões (Seade/2011), o que representa 3,88% do PIB do estado de São Paulo.

O turismo também tem grande participação no PIB da região, quesito que inclui todas as cidades da Região Metropolitana, tendo para vários atrativos naturais e culturais. Com a Camada pré-sal situada na Bacia de Santos o PIB da região tende a aumentar gradativamente de forma robusta.

O parque da Baixada Santista ficará localizado entre os bairros do Valongo e Vila Mathias e será voltado às áreas de petróleo, gás natural, porto, tecnologia da informação, meio ambiente e logística. As empresas que já manifestaram interesse em fazer parte do empreendimento são a Petrobrás, a Usiminas e iniciativas especializadas em TI.

O crescimento exacerbado em Santos, Cubatão e Guarujá, aliado a outras atividades geradoras de emprego nos setores de comércio e serviços, provocou um movimento altamente pendular em direção a outros municípios, com melhores condições de habitabilidade e espaço disponível.

Os municípios de São Vicente e Praia Grande e o distrito de Vicente de Carvalho, no Guarujá, adquiriram características de cidades-dormitório, apresentando intensa conurbação

entre si, só prejudicada pela presença de restrições de ordem física, que os impedem, aqui e ali, de apresentar uma mancha urbana contínua. Apesar da sua função portuária, importante para um crescente intercâmbio em face do processo de globalização, e de constituir sede do expressivo polo siderúrgico e da indústria de turismo, a RMBS apresenta problemas comuns aos grandes aglomerados urbanos, como os relacionados com a questão ambiental, carência de infraestrutura, saneamento ambiental, transporte e habitação.

No âmbito da Educação Profissional, a Unidade oferece duas categorias de programas: os gratuitos e os ressarcidos. Pertencem à primeira categoria, os Cursos de Aprendizagem Industrial (CAI), os Cursos Técnicos (CT), o Programa Comunitário de Formação Profissional (PCFP), em parceria com entidades públicas e associativas. E à categoria dos programas ressarcidos, os Cursos de Formação Inicial e Continuada e os Treinamentos Personalizados para as empresas.

Nos Cursos de Formação Inicial e Continuada, a Unidade atende as áreas de Vestuário, Eletroeletrônica, Informática, Instrumentação, Mecânica Automobilística, Mecânica Industrial, entre outras.

Como mencionado anteriormente, a Escola se mantém atenta ao futuro desenvolvimento técnico e tecnológico que a região deverá alcançar diante dos desafios relacionados à exploração do petróleo proveniente do “pré sal” e ao crescimento e melhoria da produtividade portuária. Assim, a Unidade vem analisando sistematicamente os cenários em que atua. Nesse sentido, investimentos em novos equipamentos devem ocorrer em um ambiente amplo e moderno. Diante disso, a Instituição entendeu que a estrutura física da Unidade não mais comportaria a grande demanda por formação profissional que os anos vindouros trariam.

4. OBJETIVOS

Oferecer aos especialistas da área de automação industrial subsídios para o estabelecimento de Políticas de Segurança da Informação, com vistas a viabilizar a segurança organizacional e gerenciamento das operações, e da comunicação, minimizando vulnerabilidades ao lançar mão de sistemas de segurança lógica, classificação e controle dos ativos de informação, controles de acesso visando a segurança física, ambiental e de pessoas mantendo a integridade dos dados, sistemas e equipamentos.

5. PÚBLICO-ALVO

O curso de pós-graduação lato sensu Segurança em Redes Cibernéticas é aberto a candidatos diplomados em cursos nas áreas de automação, mecânica, elétrica, eletrônica, tecnologia da informação, mecatrônica e correlatas.

6. CONCEPÇÃO DO PROGRAMA

O mercado de automação industrial é segmentado por fabricantes de equipamentos que trabalham em diversas redes e que cumprem papéis específicos na cadeia de automação constituída por atuadores, equipamentos de processamento de sinais e sensores diversos para monitoração e controle de processos automáticos.

Na concepção da topologia de interconexão destes equipamentos existem diversas peculiaridades, as quais precisam ser conhecidas do especialistas da área de cibersegurança que auxiliará na integração destes equipamentos com vistas à implementação de um sistema automatizado. Este trabalho envolverá aspectos de compatibilidade de sistemas, máquinas e dispositivos e a proteção da rede que os interliga.

Considerando estes aspectos, o programa foi concebido para suprir o mercado com especialistas aptos ao desenvolvimento de técnicas e políticas para proteção em redes industriais, concepção e implementação de tecnologias para proteção de redes e dispositivos, realização de testes de penetração em redes industriais, elaboração de relatórios de segurança e gerenciamento de contingência em sistemas cibernéticos.

A vinculação entre teoria e prática, aspecto fundamental na metodologia adotada no curso, é praticada através de aulas expositivas, bem como pelo desenvolvimento de atividades em laboratórios com softwares de proteção e equipamentos industriais e didáticos adquiridos com recursos próprios da instituição e por meio de parcerias com empresas da área de segurança cibernética.

A inovação surge num ambiente impregnado do que se tem como estado da arte em tecnologia de automação industrial e segurança de redes. As soluções propostas pelos fabricantes que atuam no mercado servem como base inspiradora para a proposição de inovações em sistemas de automação. A Faculdade SENAI de Tecnologia de Santos, por meio de seus recursos tecnológicos, máquinas e equipamentos, bem como de seu qualificado corpo docente, constitui-se num ambiente propício à inovação e desenvolvimento do potencial de seus alunos.

7. COORDENAÇÃO DO PROGRAMA.

A coordenação do programa está sob a responsabilidade do Prof. Fabrício Ramos da Fonseca, Mestre em Engenharia Elétrica e Doutor em Ciências, contratado no regime de 40 horas pela CLT. Com experiência e contato com empresas do ramo, atua há mais de 20 anos em docência e coordenação de cursos técnicos e tecnológicos. Atualmente é coordenador do curso superior de Tecnologia em Automação Industrial da Faculdade SENAI de Tecnologia de Santos.

8. CARGA HORÁRIA

A carga horária é distribuída entre as disciplinas que compõe o curso onde se desenvolvem atividades de forma a atender a concepção do programa. Na grade curricular temos elencadas disciplinas onde se desenvolvem atividades individuais, em grupo, dentro e fora da sala de aula notadamente no desenvolvimento do trabalho de conclusão do curso. As 360 horas do curso são distribuídas de forma a atender todas estas atividades em sala de aula e nos laboratórios.

A metodologia empregada busca um balanço entre as exposições teóricas dialogadas e atividades práticas em sala de aula desenvolvidas individualmente e em pequenos grupos, considerando-se ainda como fundamental o tempo utilizado fora de sala de aula para consolidar os conhecimentos e conceitos por meio de pesquisas bibliográficas, desenvolvimento de listas de exercícios e elaboração da monografia. A tabela 3 a seguir, mostra a sugestão de distribuição média nas disciplinas das diversas atividades desenvolvidas.

Tabela 3 – Sugestão de distribuição média da carga horária por atividade:

TIPO DE ATIVIDADE	CARGA HORÁRIA DA UNIDADE CURRICULAR (C)
Atividades práticas em grupo	10% de C
Atividades práticas individuais	10% de C
Exposição teórica dialogada	20% de C
Atividades em salas de aula e laboratórios	45% C
Pesquisas, listas de exercício, feiras tecnológicas, visitas técnicas e trabalho de conclusão do curso, fora de sala de aula.	15% C (recomendado ao aluno)

9. PERÍODO E PERIODICIDADE

As disciplinas do curso de pós-graduação – *lato sensu* da Faculdade de Tecnologia SENAI de Santos serão oferecidos aos sábados ou em duas noites durante a semana, seguindo os horários abaixo:

- Sábados – das 9h15 às 12h30 e das 13h30 as 16h45;
- Ocasionalmente, dias de semana – das 18h45 às 22h00.

A oferta das disciplinas ocorrerá em sintonia com a grade curricular proposta e com a disponibilidade de laboratórios, sendo que a preocupação fundamental será atender os alunos no sentido de prover todas as condições para que as 360 horas do curso possam ser cumpridas em três semestres letivos.

10. CONTEÚDO PROGRAMÁTICO

As disciplinas que compõem o curso, com respectivas cargas horárias estão colocadas na tabela 4, a seguir:

Tabela 4 - Organização Curricular

Semestre	Disciplina(s)/módulo(s)	Carga horária (horas)
1º	Fundamentos de Cyber Security	30
	Redes de Computadores - Protocolos e Dispositivos	30
	Segurança de Redes e Dispositivos	30
	Metodologia Científica	30
2º	Controladores Industriais	30
	Sistemas de Segurança Lógica	30
	Redes Industriais - Dispositivos e Protocolos	30
	Testes de Penetração em Redes e <i>Ethical Hacking</i>	30
3º	Internet Industrial	30
	Gestão de Segurança	30
	Arquitetura de Sistemas Seguros	30
	Gestão de Projetos	30
Total		360

EMENTAS E BIBLIOGRAFIA PARA AS DISCIPLINAS

METODOLOGIA CIENTÍFICA

A disciplina/módulo oferecerá aos alunos elementos que contribuam para a compreensão dos fundamentos científicos: sua natureza, métodos, leis e teorias, bem como, o uso do método científico na construção do conhecimento, na solução de problemas, no estabelecimento de modelos e no levantamento de hipóteses.

Este módulo tem por finalidade fornecer conceitos e ferramentas da metodologia científica em pesquisa e elaboração de monografia e textos acadêmicos voltados para projetos, incluindo:

- Pesquisa científica;
- Pesquisa bibliográfica;
- Monografias;
- Apresentação de trabalhos.

Bibliografia:

1. ANDRADE, Maria Margarida de. Como preparar trabalhos para cursos de pós-graduação: noções práticas. 6ª ed. São Paulo: Atlas, 2004.
2. BASTOS, Lilia da Rocha et al. Manual para elaboração de projetos e relatórios de pesquisa, teses, dissertações e monografias. 6ª ed. Rio de Janeiro: LTC, 2011.
3. MATTAR NETO, João Augusto. Metodologia científica na era da informática. 2ª ed. São Paulo: Saraiva, 2005.
4. APOLINÁRIO, Fábio. Metodologia da Ciência: Filosofia e prática da pesquisa. 2ª ed. São Paulo: Cengage Learning, 2012.
5. SANTOS, João Almeida. Metodologia Científica. 2ª ed. São Paulo: Cengage Learning, 2012

REDES DE COMPUTADORES - PROTOCOLOS E DISPOSITIVOS

Desenvolver nos alunos a capacidade de identificar os principais dispositivos e protocolos de uma rede de comunicação, conhecer as principais tecnologias envolvidas e ser capaz de criar e analisar, por meio de simulações, infraestrutura de redes de comunicação.

Bibliografia:

1. BUNGART, J. W. Redes de Computadores: Fundamentos e Protocolos. 1. ed. São Paulo: SENAI-SP Editora, 2017. v. 1. 200p.

2. COMER, Douglas. Interligação de Redes com TCP/IP - Volume 1. 6ª Edição. Rio de Janeiro: Campus. 2015. 520p.
3. TANEMBAUM, Andrew S., WETHERALL, David. Redes de computadores. 5ª ed. São Paulo: Person, 2011. 600 p.

FUNDAMENTOS DE CYBER SECURITY

Apresentar os conceitos primordiais de segurança da informação tais como confidencialidade, integridade e disponibilidade.

Aplicação dos princípios de sistemas de controle de acesso, como implementar, gerenciar e proteger esses sistemas, incluindo arquiteturas de confiabilidade de redes internas, gerenciamento de identidade, ciclo de vida de gerenciamento de identidade e várias estruturas de controle de acesso.

Bibliografia:

1. GORDON, Adam; MURPHY, George. SSCP (ISC) 2 Systems Security Certified Practitioner Official Study Guide and SSCP CBK Kit. 2ª Edição. Nova Jersey: Sybex. 2016. 1504p.
2. MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. Hackers Expostos. 7ª Edição. São Paulo: Bookman. 2017. 738p
3. SUEHRING, Steve. Linux Firewalls - Enhancing Security With Nftables And Beyond. 4ª Edição. Boston: Addison Wesley, 2015. 432p
4. RUFINO, Nelson Murilo de O. Segurança em Redes Sem Fio. 4ª Edição. São Paulo: Novatec, 2014.
5. CHAPMAN, Chris. Network Performance and Security: Testing and Analyzing Using Open Source and Low-Cost Tools. 1ª Edição. Syngress. 2016. 380p.

SEGURANÇA DE REDES E DISPOSITIVOS

Capacitar os alunos a identificar e analisar vulnerabilidades de redes e do protocolo TCP/IP. Especificar e configurar mecanismos de defesa, para a segmentação de rede e criação de controle de listas de acesso em redes cabeadas, sem fio e em nuvem.

Bibliografia:

1. GORDON, Adam; MURPHY, George. SSCP (ISC) 2 Systems Security Certified Practitioner Official Study Guide and SSCP CBK Kit. 2ª Edição. Nova Jersey: Sybex. 2016. 1504p.
2. MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. Hackers Expostos. 7ª Edição. São Paulo: Bookman. 2017. 738p

3. SUEHRING, Steve. Linux Firewalls - Enhancing Security With Nftables And Beyond. 4ª Edição. Boston: Addison Wesley, 2015. 432p
4. RUFINO, Nelson Murilo de O. Segurança em Redes Sem Fio. 4ª Edição. São Paulo: Novatec, 2014.
5. CHAPMAN, Chris. Network Performance and Security: Testing and Analyzing Using Open Source and Low-Cost Tools. 1ª Edição. Syngress. 2016. 380p.

CONTROLADORES INDUSTRIAIS

Capacitar o aluno em competências técnicas relativas à elaboração e testes de programas em controladores lógicos programáveis para integrá-los a sistemas automatizados industriais, com vistas a compor o cenário de equipamentos a serem preservados de invasões.

Bibliografia:

1. LUGLI, Alexandre Baratella e SANTOS, Max Mauro Dias. Redes industriais para automação industrial: AS-I, Profibus e Profinet. São Paulo : Érica, 2010.
2. SOUSA, Lindeberg Barros de. Redes de Computadores - Guia Total. 1ª. São Paulo : Érica, 2009.
3. FONSECA, Fabrício Ramos da. LOBUE, Fábio. COELHO, Marcelo Saraiva. Sistemas Digitais de Controle Industrial. São Paulo. Editora SENAI, 2016. 113p.2. GEORGINI, Marcelo. Automação aplicada; descrição e implementação de sistemas sequenciais com PLCs. 9. ed. Imp. São Paulo: Érica, 2010. 236 p. il.
4. SILVEIRA, Paulo Rogerio da; SANTOS, Winderson E. dos. Automação e controle discreto. d. São Paulo: Erica, 2002. 229 p.
5. FONSECA, Marcos de Oliveira; SEIXAS FILHO, Constantino; BOTTURA FILHO, João Aristides. Aplicando a Norma IEC 61131 na Automação de Processos. 1ª ed. São Paulo: ISA, 2009.

SISTEMAS DE SEGURANÇA LÓGICA

Capacitar o aluno para planejar a segurança lógica de redes de comunicação. Configurar e testar dispositivos e sistemas de proteção de redes. Também visa apresentar os fundamentos e as tecnologias relacionados à segurança ciber-física para proteção dos dados e dos sistemas Industriais, incluindo:

- Classificação e análise de riscos, modelo de ameaças;
- Técnicas de ciber-ataques e medidas de defesa;

- Firewalls comerciais e industriais, proxy;
- Criptografia, privacidade, autenticidade e certificado digital;
- Protocolos de segurança na Internet: IPSec e TLS.

Bibliografia:

1. GORDON, Adam; MURPHY, George. SSCP (ISC) 2 Systems Security Certified Practitioner Official Study Guide and SSCP CBK Kit. 2ª Edição. Nova Jersey: Sybex. 2016. 1504p.
2. MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. Hackers Expostos. 7ª Edição. São Paulo: Bookman. 2017. 738p
3. SUEHRING, Steve. Linux Firewalls - Enhancing Security With Nftables And Beyond. 4ª Edição. Boston: Addison Wesley, 2015. 432p.
4. KRUTZ, Ronald L. Industrial automation and control system security principles: protecting the critical infrastructure. 2. ed. ISA: 2017.
5. TEUMIM, David J. Industrial network security. 2. ed. ISA: 2010.

REDES INDUSTRIAIS - DISPOSITIVOS E PROTOCOLOS

Capacitar o aluno para atuar com redes industriais, realizando comunicação entre dispositivos e processos, utilizando ferramentas de software diversificadas, seguindo normas técnicas, de saúde, segurança e de meio ambiente. Fornecer conceitos sobre redes industriais e protocolos. O aluno irá desenvolver a capacidade de comunicar sistemas de automação via rede industrial, integrar sistemas de automação com sistema robótico via rede, criar comunicação entre sistemas de automação e robô, criar comunicação com sistemas remotos e dispositivos. Além disto, objetiva-se capacitar o aluno no desenvolvimento de sistemas de automação utilizando tecnologias de redes por meios guiados utilizando-se das tecnologias e padrões ISA SP100; Wireless HART (WiHART), segurança de redes Industriais wireless; instalação das redes wireless; configuração dos pontos de acesso; problemas de transmissão de sinais, arquitetura e suas aplicações no ambiente industrial.

Bibliografia:

1. LUGLI, Alexandre Baratella; SANTOS, Max Mauro Dias. Redes Industriais Para Automação Industrial. AS-I, Profibus e Profinet. São Paulo: Érica Saraiva, 2010. 176 p.
2. MAHNKE, Wolfgang; LEITNER, Stefan-Helmut. OPC Unified Architecture. USA: Springer, 2009. 351p.
3. PIGAN, Raimond; METTER, Mark. Automating with PROFINET: Industrial Communication Based on Industrial Ethernet. USA: Wiley, 2008. 462p.
4. DARGIE, W. W., POELLABAUER, C. Fundamentals of wireless sensor networks: Theory and Practice. Wiley, 2010.

5. RUFINO, Nelson Murilo de O. Segurança em redes sem fio. 4. ed. São Paulo: Novatec, 2014.
6. HANES, David, et al. IoT Fundamentals: networking technologies, protocols, and use cases for the internet of things. 1. ed.: Cisco Press, 2017.
7. LUGLI, A. B. e SANTOS M. M. D., Redes Sem Fio Para Automação Industrial, São Paulo, Editora Érica, 2013.

TESTES DE PENETRAÇÃO EM REDES E ETHICAL HACKING

Capacitar o aluno para atuar na defesa de redes de comunicação, realizando testes de penetração controlados, de forma ética, para levantar vulnerabilidades nas redes que administram a segurança. Planejar e configurar ambientes para testes de penetração. Executar os testes, analisar e documentar os resultados.

Fornecer conceitos de *ethical hacking*, planejamento do ambiente de execução de testes de penetração. Execução dos testes de penetração com o uso de ferramentas de varredura, exploração de vulnerabilidades e ataques de força bruta. Analisar os resultados obtidos nos testes e preparar a documentação final com os resultados.

Bibliografia:

1. GORDON, Adam; MURPHY, George. SSCP (ISC) 2 Systems Security Certified Practitioner Official Study Guide and SSCP CBK Kit. 2ª Edição. Nova Jersey: Sybex. 2016. 1504p.
2. GREGG, Michael Douglas. The Network Security Test Lab: A Step-by-Step Guide. 1ª Edição. Nova Jersey: Wiley. 2015. 480p.
3. WEIDMAN, Georgia. Testes de Invasão: Uma Inovação Prática ao Hacking. 1ª Edição. São Paulo: Novatec, 2014. 576p.
4. BARRETO, Alesandro Gonçalves. BRASIL, Beatriz Silveira. Manual de Investigação Cibernética à Luz do Marco Civil da Internet. BRASPORT Editora. Rio de Janeiro. 2016.
5. BARRETO, Alesandro Gonçalves; WENDT, Emerson. CASELLI, Guilherme. Investigação Digital em Fontes Abertas. BRASPORT Editora. Rio de Janeiro. 2017.

INTERNET INDUSTRIAL

Fornecer subsídios para atuação na Internet Industrial, fornecendo uma visão atualizada das tecnologias disponíveis no mercado da IoT, seguindo normas técnicas, de saúde, segurança e de meio ambiente. Capacitar o aluno no processo de integração de Internet Industrial com Dispositivos Industriais. O aluno irá desenvolver a capacidade de comunicar equipamentos para monitorar, coletar, trocar e analisar dados de uma planta para gestão do processo, utilizando os conceitos de internet das coisas. Este módulo tem por finalidade, também,

apresentar aos alunos as principais tecnologias de redes e de protocolos voltados para sistemas IoT, bem como fornecer fundamentos para balizar a escolha de tecnologias atualmente empregadas no mercado:

Redes para IoT: Sigfox, LoRaWan, Zigbee, Bluetooth, Z-Wave, 6LoWPAN, ISA100, WiFi, Thread, NFC, LTE-M, LPWAN, 5G, NB-IoT, RPMA, entre outras;

Protocolos para redes IoT: mDNS, UPnP, Physical Web, NanoIP, CCN, TSMP, Ingenu, MtConnect, OPC-UA, ESP, dentre outros.

Bibliografia:

1. GREENGARD, Samuel. The Internet of Things. USA: MIT PRESS, 2015. 232p.
2. HANES, David; SALGUEIRO, Gonzalo; GROSSETETE, Patrick, BARTON, Rob. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things. USA: Cisco Press, 2017. 576p.
3. OLIVEIRA, Sérgio de. Internet das Coisas com ESP8266, Arduino e Raspberry Pi. São Paulo: 2017. 240p.
4. ALBUQUERQUE, Pedro U. B e ALEXANDRIA, Auzuir R. de. Redes industriais: aplicações em sistemas digitais de controle distribuído: protocolos industriais e aplicações SCADA. 3. ed. rev. e ampl. São Paulo : Ensino Profissional, 2009.
5. DARGIE, W. W., POELLABAUER, C. Fundamentals of wireless sensor networks: Theory and Practice. Wiley, 2010.
6. LUGLI, A. B. e SANTOS M. M. D., Redes Sem Fio Para Automação Industrial, São Paulo, Editora Érica, 2013.

GESTÃO DE SEGURANÇA

Capacitar o aluno para analisar as melhores práticas a serem incorporadas pelas organizações modernas para assegurar o monitoramento contínuo dos dados e a integridade das informações corporativa. Criação de processos voltados ao monitoramento contínuo da integridade das informações, visando à prevenção de ataques e ao furto dos dados, assegurando em casos emergenciais o pronto restabelecimento dos sistemas e o acesso seguro às informações.

Bibliografia:

1. GORDON, Adam; MURPHY, George. SSCP (ISC)2 Systems Security Certified Practitioner Official Study Guide and SSCP CBK Kit. 2ª Edição. Nova Jersey: Sybex. 2016. 1504p.
2. SÊMOLA, Marcos, Gestão da Segurança da Informação: uma visão executiva. São Paulo: Campus Elsevier. 2012. 184 p.

3. SILVA, Manoel Sérgio; Governança de Segurança da Informação - Como Criar Oportunidades Para o Seu Negócio. 1ª Edição. São Paulo: Brasport, 2014. 168p.
4. ALEVATE, William; Gestão da Continuidade de Negócios. 1ª Edição, São Paulo: Campus Elsevier. 2013. 160 p.
5. MAHNKE, Wolfgang; LEITNER, Stefan-Helmut. OPC Unified Architecture. USA: Springer, 2009. 351p.

ARQUITETURA DE SISTEMAS SEGUROS

O objetivo desta componente é o de desenvolver conhecimentos acerca da arquitetura e infraestrutura de sistemas necessários para que se possa realizar a análise e a especificação de controles de segurança orientados a sistemas seguros. Estes aspectos são trabalhados no contexto do desenvolvimento de sistemas de automação utilizando diferentes tecnologias e considerando: os componentes de um sistema distribuído, aspectos de segurança destes sistemas e processos de desenvolvimento seguro. São abordados assuntos como: Top 10 OWASP, testes de segurança em aplicações web, *cloud computing*, *Big Data*, *Analytics*. e armazenamento seguro.

Bibliografia:

1. KIZZA, Joseph Migga. Computer network security and cyber ethics. 2nd ed. Jefferson: McFarland & Company, c2006;
2. RAY, John. Maximum Linux security: a hackers guide to protecting your Linux server and workstation. 2nd ed. Indianapolis: SAMS, 200;
3. KUROSE, James F.; ROSS, Keith W. "Redes de Computadores e a Internet: Uma nova abordagem", Editora Pearson;
4. STALLINGS, William. Criptografia e segurança de redes: princípios e práticas. São Paulo: Pearson Education do Brasil, 2010;
5. MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. Hackers expostos/ segredos e soluções para a segurança das redes. São Paulo: Makron Books, 2000;
6. TANENBAUM, Andrew S.; WETHERALL, D. Computer networks. 5th ed. Boston, MA; Columbus, OH: Prentice Hall, 2011.

GESTÃO DE PROJETOS

Capacitar os alunos em ferramentas de gestão de projetos, análise na tomada de decisão e controle, para atuar na área industrial e de serviços, aplicando o controle e tomada de decisão em projetos, para implementar PMOs (Project Management Office).

Bibliografia:

1. GIDO, Jack; CLEMENTS, James P. Gestão de projetos. Tradução Vértice Translate. São Paulo: Cengage Learning, 2010. 451 p.
2. HILLIER, F. S; LIEBERMAN, G. J. Introduction to Operations Research. 7ª ed. McGraw Hill, 2002.
3. TAHA, H. A. Operations Research: an introduction. 7th Edition. Prentice Hall, 2002.
4. MOLINARI, Leonardo. Gestão de Projetos - Teoria, Técnicas e Práticas. 1ª Ed. São Paulo. Érica. 2010. 240p.
5. PAHL, Gerhard et al. Projeto na Engenharia. 6ª Ed. São Paulo: Edgard Blücher, 2005. 432p.
6. Project Management Institute. Um guia do conhecimento em gerenciamento de projetos (Guia PMBOK). 6. ed. EUA: Project Management Institute, Inc., 2018. 756 p.

11. CORPO DOCENTE

O corpo docente envolvido no curso é composto pelos seguintes professores:

- Alexandre Stucchi (dedicação integral)
 - Mestre em Engenharia Mecânica;
 - MBA em Auditoria de Sistemas de Segurança;
 - Graduação: Engenharia Eletrônica.
- Roberto Blanco Lorenzo (dedicação integral)
 - Mestre em Engenharia Mecânica;
 - Especialização em Engenharia da Manutenção;
 - Graduação: Ciências da Computação.
- Alessandro Marreiro (dedicação parcial)
 - Mestre em Engenharia Mecânica;
 - Graduação: Tecnologia de Processamento de Dados.
- Samanta Roveri (dedicação integral)
 - MBA Executivo em Negócios;
 - Graduação em Logística.
- Fábio Cardoso (dedicação integral)
 - Especialização em Automação Industrial e Sistemas Embarcados- SENAI;
 - Graduação: Engenharia Elétrica.

12. METODOLOGIA

A metodologia empregada tem como diretriz básica a vinculação entre teoria e prática, os aspectos teóricos que serão abordados terão como ponto de partida situações reais que sirvam de base para aplicação do conceito teórico a ser estudado.

A concepção metodológica do curso prioriza, portanto, a teorização, onde os “cases” subsidiam os tópicos teóricos, situando-lhes e os justificando a sua aplicação na proteção cibernética de sistemas automatizados. A exposição desta experiência adquirida por docentes, que além da visão acadêmica, possuem a vivência na área de segurança de redes, se caracteriza como uma metodologia que propõe referenciais balizadores para inovações e proposição de novas soluções no âmbito da tecnologia de integração dos equipamentos e sistemas automatizados.

Dessa forma a instituição implementa em suas ações a formação por competências, reduzindo o espaço entre teoria e prática, entre instituição de ensino e empresa.

13. ATIVIDADES COMPLEMENTARES

As atividades complementares ocorrem vinculadas a eventos relacionados à área tecnológica da automação industrial e segurança de redes, como: FIEE - Feira Internacional da Indústria Elétrica, ISA Expo, eventos de fabricantes da área de segurança de rede como a CISCO, Amazon, Fortnet e Checkpoint. São promovidas também palestras de profissionais e fabricantes de equipamentos para área de segurança cibernética e automação na Semana Tecnológica da Faculdade que é um evento anual na Faculdade de Tecnologia SENAI de Santos.

14. RECURSOS

O curso contará com a infraestrutura física exposta na Tabela 5.

Tabela 5 – Infraestrutura

Dependências	Quantidade	m²
Sala de Manutenção	01	45 m ²
Almoxarifado	01	70 m ²
Sala de Atendimento a Empresas	01	40 m ²
Sala de Direção	01	25 m ²
Sala de Coordenação dos Cursos	01	28 m ²
Sala de Coordenação de Estágios	01	10 m ²
Sala de Orientação Educacional	01	20 m ²
Sala de Preparação de aulas	01	80 m ²
Sala de Professores	01	40 m ²
Salas de Aulas para o curso	02	120 m ²
Sanitários	08	250 m ²
Área de Lazer / Convivência	01	800 m ²
Secretaria	01	65 m ²
Auditório	01	250 m ²
Biblioteca com Sala de Leitura/Estudos	01	220 m ²
Laboratórios:		
Laboratório de Instrumentação 1	01	69 m ²
Laboratório de Instrumentação 2	01	75 m ²
Laboratório de Instalações de Instrumentação	01	89 m ²
Laboratório de Controle de Processos	01	75 m ²
Laboratório de CLP	01	80 m ²
Laboratório de Automação e Redes Industriais	01	60 m ²
Laboratório de Sistemas Digitais de Controle	01	60 m ²
Laboratório de Projetos de Instrumentação	01	60 m ²
Laboratório Planta Piloto	01	90 m ²

Os recursos audiovisuais são apresentados na Tabela 6.

Tabela 6 - Recursos Audiovisuais

Item	Quantidade
Projetores Multimídia	26
Máquinas fotográficas digitais	02

Equipamentos:

A instituição conta com diversos equipamentos distribuídos entre os laboratórios e salas relacionadas à administração. Nos diversos laboratórios encontramos os seguintes equipamentos segundo a tabela 3:

Tabela 7- Equipamentos por laboratórios

Laboratório de Instrumentação 1		Área 80m ²
Equipamentos instalados		
Qtde	Especificações	
01	Microcomputador	
10	Bancadas para instrumentação	
04	Configuradores de instrumentos HART/FIELDBUS 475/EMERSON	
04	Conjunto didático para estudo de medidores de nível	
04	Conjunto didático para estudo de medidores de pressão e temperatura	
04	Calibradores de pressão PC-507/PRESYS	
04	Calibradores de pressão 718 Ex30G FLUKE	
04	Calibradores multifunção ISOCAL MCS-8/PRESYS	
04	Calibradores de processos multifunção 725/FLUKE	
04	Calibradores de malha 715/FLUKE	
04	Calibradores de temperatura TC502/PRESYS	
05	Banho térmico tipo bloco seco T25N/PRESYS	
08	Multímetros digitais	
08	Manômetros padrão 0 a 30 psi	
08	Transmissores de pressão LD301/SMAR	
06	Transmissores de temperatura TT301/SMAR	
08	Transmissores de temperatura YTA/YOKOGAWA	
08	Válvulas Reguladoras de Pressão	

Laboratório de Instrumentação 2		Área 80m²
<i>Equipamentos instalados</i>		
Qtde	Especificações	
01	Microcomputador	
04	Configuradores de instrumentos HART/FIELDBUS 475/EMERSON	
08	Bancadas para instrumentação com conjunto para medição de vazão e teste de válvulas	
04	Calibradores de pressão PC-507/PRESYS	
04	Calibradores de pressão 718 Ex30G FLUKE	
04	Calibradores multifunção ISOCAL MCS-8/PRESYS	
04	Calibradores de malha 715/FLUKE	
08	Calibradores de temperatura TC507/PRESYS	
5	Válvulas de controle HITER	
4	Válvulas de controle SPIRAX SARCO	
8	Multímetros digitais	
8	Manômetros padrão 0 a 200 kPa	
4	Transmissores Multivariável /EMERSON	
10	Transmissores de pressão /PROVIDER CONTROLS	
8	Válvulas reguladora de pressão	
4	Transmissor de temperatura Rosemount	
4	Termômetro Infravermelho Raytech	
4	Kit Turbina	

Laboratório de Controle de Processos		Área 80m²
<i>Equipamentos instalados</i>		
Qtde	Especificações	
09	Microcomputadores	
08	Bancadas para instrumentação	
03	Plantas didáticas para controle de processos PLINT	
07	Conjunto didático para estudo de controle de processos DEGEM SYSTEM	
08	Calibradores multifunção ISOCAL MCS-08	
04	Multímetros digitais	
08	Transmissor de Pressão Provider Controls	
04	Controlador Digital CD-600 SMAR	
04	Registrador Honeywell	
<i>Softwares Instalados</i>		
Sistema Operacional Windows XP, Indusoft Web Studio		

Laboratório de Automação/Redes Industriais		Área 60m²
<i>Equipamentos instalados</i>		
Qtde	Especificações	
09	Microcomputadores	
08	Bancadas para instrumentação	
08	CLP's SIEMENS com comunicação PROFIBUS	
04	Conjunto manipulador eletropneumático de 3 eixos	
04	Conjunto didático para controle de pressão	
04	Conjunto didático para estudo e interligação de inversor de frequência	
04	Multímetros digitais	
<i>Softwares Instalados</i>		
Sistema Operacional Windows XP, Simatic Step/7		

Laboratório de Sistemas Digitais para Controle		Área 60m²
<i>Equipamentos instalados</i>		
Qtde	Especificações	
09	Microcomputadores	
08	Bancadas para eletroeletrônica	
04	Conjunto didático para estudo de medidores de pressão e temperatura - FIELDBUS	
04	Multímetros digitais	
08	Controladores digitais CD600/SMAR	
04	Registradores digitais sem papel YOKOGAWA	
04	Configuradores de Instrumentos HART/FIELDBUS 475 / EMERSON	
08	Maletas CLP Atos com Kit Wireless	
<i>Softwares Instalados</i>		
Sistema Operacional Windows XP, Software de supervisão Indusoft Web Studio, System 302 (configurador Rede Fieldbus Foundation), configurador do controlador digital – conf600plus, configurador do CLP-A1 soft		

Laboratório de Instalação de Instrumentação		Área 60m²
<i>Equipamentos instalados</i>		
Qtde	Especificações	
01	Microcomputador	
04	Bancadas para instrumentação analítica	
04	Analisadores de pH	
04	Analisadores de 3 gases ABB	
04	Analisadores de oxigênio dissolvido	
04	Misturador de gás	
04	Condutivímetro	
02	Turbidímetro	
01	Analisador de Poluentes Atmosféricos	

Laboratório de Projetos de Instrumentação		Área 60m²
Equipamentos instalados		
Qtde	Especificações	
09	Microcomputadores	
08	Bancadas para informática	
01	Impressora jato de tinta formato A3	
04	CLP's Rockwell Automation com comunicação Ethernet e Devicenet	
04	Interface Homem Máquina com comunicação Devicenet	
01	Impressora Laser Samsung	
01	Plotter jato de tinta	
08	Multímetro digital	
Softwares Instalados		
Sistema Operacional Windows XP, Rockwell RSLogix 5000, Rockwell RSNetwork, Indusoft Web Studio		

Laboratório Planta Piloto de Processo		Área 100m²
Equipamentos instalados		
Qtde	Especificações	
10	Microcomputadores	
01	Planta Piloto de Processo com armário de controle com CLP, tanques e tubulações em aço inox, aquecedor de água a gás natural, torre de resfriamento, instrumentação padrão Profibus, instrumentação wireless e analisador de gás	
Softwares Instalados		
Sistema Operacional Windows XP, LogicDesigner-YOKOGAWA, FastTools-YOKOGAWA, PRM-YOKOGAWA, Indusoft Web Studio		

Laboratório de Infraestrutura de Redes (202)		Área: m²
Softwares Instalados		
Equipamentos instalados		
Qtde	Especificações	
2	Rack 36U aberto (com patch panels, organizadores de cabos metálicos - DIO fibra óptica)	
1	Rack fechado 36U (servidor vOIP)	
3	Rack Fechado 24U	
2	Switches 2960 CISCO Catalyst	
6	Roteadores CISCO série 2000	
2	Máquinas de fusão fibra óptica	
2	Certificadores de cabos metálicos/ fibra óptica / Coaxial / Fluke	

2	Qualificadores de cabos metálicos/ fibra óptica / Coaxial - Ideal
8	Testadores de cabo Ideal
4	Microscópios para inspeção de núcleo fibra óptica
8	Telefones Cisco - VOIp
16	Amplifier Probe
16	Alicate cute fibra óptica
16	Alicate crimpagem
16	Decapador cabo metálico
2	bigfoot decapador cabo telefônico
16	alicate stripper fibra óptica
16	alicate idg - fibra óptica

Laboratório de Informática (203)		Área: m²
<i>Softwares Instalados</i>		
Sistema Operacional Windows 7, Microsoft Office 2013 , M. Visio 2010, SQL Server 2008, Visual Studio 2008 e Adobe Premium.		
<i>Equipamentos instalados</i>		
Qtde	Especificações	
18	Microcomputadores	

Laboratório de Informática (211)		Área: m²
<i>Softwares Instalados</i>		
Sistema Operacional Windows 7, Autocad 2015, Office 2013, SQL Server 2008, Visual Studio 2010, Packet Tracer, Virtual Box.		
<i>Equipamentos instalados</i>		
Qtde	Especificações	
17	Microcomputadores	
1	Impressora jato de tinta formato A3	

Em cumprimento à Portaria MEC nº 1.679, de 2 de dezembro de 1999, a instituição adaptou as condições de acesso para portadores de deficiência física nos ambientes coletivos, da seguinte maneira:

- Reserva de vaga especial em frente ao prédio da Faculdade(1);
- Adequação do espaço físico das portas de acesso;
- Telefone público instalado em altura acessível aos usuários de cadeiras de rodas (1)
- Elevador (1)
- Banheiros com barras de apoio nas paredes (1)
- Lavabos e bebedouros em altura acessível aos usuários de cadeiras de rodas.

15. CRITÉRIO DE SELEÇÃO

O processo seletivo ocorrerá especificamente ou de forma combinada por meio dos seguintes instrumentos tomando por base a quantidade de candidatos por vaga:

- I – avaliação do atendimento aos pré-requisitos exigidos.
- II – análise de currículo.
- III – entrevista.
- IV – prova escrita de conhecimento.
- V – redação.
- VI – outros.

16. SISTEMAS DE AVALIAÇÃO

A avaliação e o controle de frequência são computados por módulo. Serão considerados aprovados no módulo os alunos que tiverem obtido aproveitamento correspondente a 50% (cinquenta por cento) em uma escala de 0 a 100 de notas, e, pelo menos, 75% (setenta e cinco por cento) de frequência. Os critérios de avaliação de cada módulo serão determinados pelo respectivo professor responsável e deverão constar dos programas distribuídos no início de cada módulo.

Os critérios de avaliação da monografia serão determinados pelo professor orientador responsável e devem obedecer ao que está colocado parágrafo anterior no que se refere ao mínimo para aprovação.

A cada módulo concluído será levantado o índice de satisfação dos alunos com o curso em relação a: cumprimento dos objetivos e horários, docência, coordenação, infraestrutura e atendimento administrativo. Será utilizado um instrumento de coleta da satisfação do participante que se constitui num formulário com dez itens de avaliação conforme a Tabela 8.

Tabela 8 - Itens do formulário de avaliação

1	Os conteúdos ministrados estão coerentes com os objetivos do curso
2	Cumprimento dos objetivos propostos para o curso
3	Cumprimento do horário das aulas pelo docente
4	Objetividade e clareza do docente ao atender as dúvidas e expor o conteúdo
5	Habilidade de relacionamento interpessoal do docente com os alunos
6	Atuação e postura da coordenação na solução de problemas referentes ao curso
7	Atendimento na recepção / secretaria da escola
8	Qualidade de livros e textos, quanto a adequação da informação
9	Atendimento na biblioteca
10	Limpeza , conservação e adequação das salas de aula e/ou laboratórios

17. CONTROLE DE FREQUÊNCIA

A frequência mínima exigida em cada módulo é de 75%.O controle de frequência é feito pelo docente em cada aula ministrada com base no relatório específico de cada módulo onde consta a relação de alunos participantes.

18. MONOGRAFIA

O trabalho de conclusão do curso será elaborado pelos alunos em forma de uma monografia. Os critérios de avaliação da monografia serão determinados pelo professor orientador responsável e devem obedecer ao requisito de aproveitamento correspondente a 50% (cinquenta por cento) na escala de 0 a 100 de notas para obter a certificação.

19. CERTIFICAÇÃO

Os certificados de conclusão de cursos serão registrados na Faculdade de Tecnologia SENAI de Santos, em livro próprio, destinado especificamente a esse fim e terão validade nacional conforme dispõe o § 3º, do artigo 8, da Resolução CNE/CES n.º 1, de 6 de abril de 2018, do Conselho Nacional de Educação.

20. INDICADORES DE DESEMPENHO

Os indicadores de desempenho para o curso de pós-graduação *lato sensu* Segurança em Redes Cibernéticas terão como parâmetros os critérios apresentados na Tabela 9. Estes critérios estabelecem os indicadores e as respectivas metas a serem atingidas.

Tabela 9 - Indicadores de desempenho e metas

INDICADOR DE DESEMPENHO	METAS
1. Número de alunos formados (a cada três semestres)	18 alunos / 18 meses
2. Aproveitamento médio no curso (0 a 100)	70
3. Frequência Média (%)	90%
4. Taxa de evasão por módulo (% de alunos desistentes / alunos ingressantes)	10%
5. Números de Monografias aprovadas por período	18 /18 meses
6. Taxa de satisfação dos alunos com o curso (%)	85%

HISTÓRICO DAS ALTERAÇÕES

Data	Versão	Descrições das alterações
12-12-2020	1.0	Projeto elaborado pela equipe técnica da Faculdade SENAI de Tecnologia de Santos.
03/03/2010	2.0	Substituição da disciplina Gerenciamento de Contingências e Recuperação de Desastres pela disciplina Arquitetura de Sistemas Seguros. Fabrício Fonseca CFP 2.01.