



CONSELHO ESTADUAL DE EDUCAÇÃO

PRAÇA DA REPÚBLICA, 53 – CENTRO/SP - CEP: 01045-903
FONE: 2075-4500

PROCESSO	CEESP-PRC-2024/00046
INTERESSADO	Centro Estadual de Educação Tecnológica Paula Souza / FATEC Araraquara
ASSUNTO	Renovação do Reconhecimento do Curso Superior de Tecnologia em Segurança da Informação
RELATOR	Cons. Roque Theophilo Júnior
PARECER	Nº 17/2026 CES "D" Aprovado em 28/01/2026 Comunicado ao Pleno em 04/02/2026

CONSELHO PLENO

1. RELATÓRIO

1.1 HISTÓRICO

Cuida-se de pedido de Renovação do Reconhecimento do Curso Superior de Tecnologia em Segurança da Informação, mantido pelo Centro Estadual de Educação Tecnológica Paula Souza / FATEC Araraquara, inaugurado por pedido institucional através do Ofício 051/2024 - GDS, enviado para a SCA/CEE em 11/03/2024, realizada dentro do prazo estipulado pelo Art. 47 da Deliberação CEE 171/2019, ou seja, nove meses antes do término da validade do reconhecimento do curso.

Em 03/04/2024, a Portaria CEE-GP 108 designou os Professores Ecivaldo de Souza Matos e José Avelino Placca para elaborar o Relatório circunstanciado sobre o Curso com visita *in loco* foi realizada pelos Especialistas no dia 23/04/2024, e o Relatório circunstanciado de fls. 140 a 151.

Os autos foram baixados em diligência para esclarecimentos e complementação de informações sobre a metodologia aplicada nas atividades de extensão e o Ofício CES 103/2024 destaca a adequação dos cursos das FATECs à Deliberação CEE 216/2023, a qual estabelece a curricularização da extensão. Em razão disso, os processos em trâmite foram sobrestados até a implementação da adequação. Em 11/11/2024, a FATEC encaminhou o PPC atualizado, incluindo a curricularização da extensão acompanhado do Ofício 436/2024-CEETEPS-CESU-GAP. Finalmente em 05/02/2025, os autos foram encaminhados à CES para manifestação dos Especialistas, em razão das divergências entre o Relatório Síntese e o Relatório da Comissão que apresentaram suas considerações a fls.

A Assessoria Técnica informou o Processo que passa a integrar o presente.

É o relatório.

1.2 APRECIÇÃO

Com base na norma em epígrafe e nos dados do Relatório Síntese, segue o relato.

1.2.1 Dados Gerais

Histórico Institucional e Dados do Curso

Recredenciamento	Parecer CEE 123/2019, Portaria CEE-GP 191/2019, DOE 04/05/2019, por 7 anos
Diretor-Superintendente	Clóvis de Souza Dias mandato: de 21/11/2024 a 20/11/2028
Reconhecimento	Parecer CEE 292/2021 e Portaria CEE-GP 447/2021, publicada no DOE em 11/12/2021 - pelo prazo de três anos, com 40 vagas semestrais.
Horários de Funcionamento:	Noturno: das 19h00 às 22h30 horas de segunda-feira a sexta-feira, sábado das 08h00 às 13h00
Duração da hora/aula:	50 minutos
Carga horária total do Curso:	2800 horas, sendo 2880 aulas = 2400 horas + 240 de Estágio Supervisionado e 160 horas de Trabalho de Graduação.
Número de vagas oferecidas por período:	Noturno: 40 vagas, por semestre
Tempo para integralização:	Mínimo: 6 semestres Máximo: 10 semestres
Forma de Acesso:	O ingresso se dá pela classificação em Processo Seletivo Vestibular, que é realizado em uma única fase, com provas dos componentes do núcleo comum do Ensino Médio ou equivalente, em forma de testes objetivos e uma redação ou processo classificatório mediante análise de rendimento escolar no Ensino Médio. Processo para preenchimento de vagas remanescentes por discentes formados na Instituição ou



CEESP/PC/202600032

	transferência de discentes de outra Fatec ou Instituição de Ensino Superior (processo seletivo composto de duas fases: processo seletivo classificatório por meio de Edital, com número de vagas, seguido pela análise da compatibilidade curricular).
Responsável pelo PPC	Gilmar Cação Ribeiro Mestre em Ciência da Computação, Univ. Federal de São Carlos, UFSCAR Graduado em Ciência da Computação, USP. http://lattes.cnpq.br/5879887635797188

1.2.2 Caracterização da Infraestrutura Física da Instituição reservada para o Curso

Instalação	Quantidade	Capacidade	Observações
Salas de aula	6	40	9 salas com <i>datashow</i>
Laboratórios de Informática	5	125	1 laboratório com 40 computadores, 1 laboratório com 25 computadores, 2 laboratórios com 20 computadores cada e um laboratório com 20 notebooks
Apoio	1	230	Auditório
	1	88	Biblioteca
	1	40	Sala de Estudos
	3	3	Sala de Estudos individual
	2	4	Sala de Coordenação
	1	40	Sala Maker
	1	4	Sala de RJI
	1	12	Sala de Professores
	1	12	Sala de Reuniões
	1	4	Secretaria Acadêmica
Outros (listar)	1	1	Sala da Direção
	1	4	Secretaria Administrativa
	1	32	Cantina
	1	8	Cozinha
	1	-	Almoxarifado

1.2.3 Biblioteca

Tipo de acesso ao acervo	(X) Livre () Através de funcionário
É específica para o Curso	() Sim (X) Não () Específica da área
Total de livros para o Curso	Impressos: Títulos: 79 Volumes: 647
Indicar endereço do sítio na WEB que contém detalhes do acervo	http://biblio.cps.sp.gov.br/

1.2.4 Corpo Docente

A relação dos docentes com respectivas disciplinas encontra-se encartado aos autos e atende ao disposto na Deliberação CEE 145/2016.

1.2.4.1 Classificação dos Docentes por Titulação

Titulação	Quantidade	Percentual
Especialista	3	15
Mestre	8	40
Doutor	9	45
Total	20	100%

1.2.5 Corpo Técnico disponível para o Curso

Tipo	Quantidade
Diretor	1
Coordenador do Curso	1
Diretoria de Serviço Acadêmico	1
Diretoria de Serviço Administrativo	1
Auxiliar administrativo	4
Bibliotecária	1
Estagiário	2

1.2.6 Demanda do Curso nos últimos Processos Seletivos - Vestibular, desde o último Reconhecimento (últimos 5 anos)

Semestre	Vagas Noturno	Candidatos Noturno	Relação candidato/vaga Noturno
2023/2	40	183	4,58
2023/1	40	252	6,30
2022/2	40	168	4,20
2022/1	40	262	6,55
2021/2	40	235	5,88
2021/1	40	256	6,40
2020/2	40	297	7,43
2020/1	40	156	3,90
2019/2	40	146	3,65
2019/1	40	166	4,15



1.2.7 Demonstrativo de Alunos Matriculados e Formados no Curso, desde o último Reconhecimento por semestre

Semestre	Matriculados		
	Ingressantes	Demais séries	Total
	Noturno	Noturno	Noturno
2023/2	40	166	206
2023/1	40	161	201
2022/2	40	151	191
2022/1	40	143	183
2021/2	40	146	186
2021/1	40	133	173
2020/2	40	105	145
2020/1	40	88	128
2019/2	40	70	110
2019/1	40	44	84
Semestre	Egressos		
	Noturno		
2023/1	26		
2022/2	10		
2022/1	20		
2021/2	11		

1.2.8 Matriz Curricular

A matriz e estrutura curricular, encartada nos autos e devidamente conferida pelo relator signatário, que fazem parte da estrutura do Curso Superior de Tecnologia em Segurança da Informação, classificado no Eixo Tecnológico em Informação e Comunicação, propõe uma carga horária total de 2.400 horas, destinada aos componentes curriculares (2880 aulas de 50 minutos), acrescida de 160 horas de Trabalho de Graduação e de 240 horas de Estágio, perfazendo um total de 2800 horas, contemplando, assim, o disposto na legislação e às diretrizes internas do Centro Paula Souza. A composição curricular do Curso acha-se regulamentada na Resolução CNE/CP 01/2021. O Curso Superior de Tecnologia em Segurança da Informação está contemplado no Catálogo Nacional de Cursos Superiores de Tecnologia (CNCST), aprovado pela Portaria MEC 514/2024, sob o Eixo Tecnológico de Informação e Comunicação, estando estabelecida a carga horária mínima de 2.000 horas para o Curso. Não há conceito ENADE registrado no sistema e-MEC para o Curso em tela.

Total de aulas do curso .				1440	1440	-	-	264	2880
Total de horas do curso				1200	1200	-	-	220	2400
Distribuição da carga horária dos componentes complementares									
Componente Complementar			Total de horas		Obrigatoriedade				
Trabalho de Graduação			160 horas		Obrigatório a partir do 5º Semestre				
Estágio Curricular Supervisionado			240 horas (72 h Extensão)		Obrigatório a partir do 4º Semestre				
Demonstrativo da Carga Horária									
			horas/aula 50 min		horas/relógio 60 min				
Disciplinas			2.880		2.400				
Estágio			-		240				
Trabalho de Graduação			-		160				
Total					2.800				

1.2.9 Projetos das Atividades de Extensão

As atividades de extensão são desenvolvidas nos componentes: Tecnologia da Informação nas Organizações; Princípios da Segurança da Informação; Diagnóstico e Soluções de Problemas em TI; Análise e Gestão de Riscos em Segurança da Informação; Governança de Tecnologia da Informação; Fator Humano em Segurança da Informação; Políticas de Segurança da Informação; Matemática Discreta; Probabilidade e Estatística; Estágio Curricular Supervisionado; Direito e Ética Profissional na Sociedade da Informação; Gestão da Segurança da Informação e Inglês VI. A seguir, transcrevemos as informações correspondentes.

Fls. 265 a 267

Título	Educação Digital para Todos: Capacitação em Tecnologia por meio da Inclusão Digital
Temática	Inclusão digital é o processo de democratizar o acesso às tecnologias da informação, de modo a permitir que todos tenham acesso a elas, independentemente de sua situação econômica, idade, localização ou habilidades. São muitos os benefícios da tecnologia, a praticidade na área de compras, acesso a informações, desbravando novas áreas de interesse. A inclusão digital busca eliminar barreiras que impedem as pessoas de participar plenamente na sociedade digital. A inclusão digital pode trazer diversos benefícios, como: Melhora da qualidade de vida, Oportunidades para melhores empregos, Capacitação profissional, Participação cidadã, Estímulo à inovação e ao desenvolvimento econômico. Elaboração de projetos para resolver problemas reais das comunidades regionais, estreitando e fortalecendo laços com a comunidade.



Descrição	O projeto de extensão curricular " Educação Digital para Todos: Capacitação em Tecnologia por meio da Inclusão Digital " é uma iniciativa que será desenvolvida pelos alunos em conjunto com seus professores orientadores visando promover a inclusão digital e capacitar a comunidade em temas fundamentais de Tecnologia da Informação (TI). O projeto busca democratizar o acesso ao conhecimento digital e fortalecer a segurança no uso de tecnologias, integrando atividades de Workshops e Palestras, Cursos Online e Presenciais, e Criação de Materiais Didáticos.
Objetivos	• Fomentar a inclusão digital por meio da capacitação da comunidade em conceitos de tecnologia da informação de acordo com os objetivos dos componentes curriculares envolvidos. • Desenvolver habilidades digitais essenciais para o uso consciente e seguro das ferramentas digitais. • Promover a integração entre os alunos e a comunidade, proporcionando um espaço de troca de conhecimentos e experiências.
Carga horária	60 aulas/50 horas
Público-alvo	Estudantes, sociedade e micro e pequenas empresas da região.
Ações/Etapas de execução	Workshops e Palestras • Identificar os temas de necessidade da comunidade. • Organizar o calendário de eventos e divulgar na comunidade.
	• Avaliar o impacto dos workshops por meio de feedback dos participantes Cursos Online e/ou Presenciais • Definir o público-alvo e o nível de conhecimento prévio dos participantes. • Criar ou adaptar materiais didáticos adequados ao nível de desconhecimento da comunidade. • Selecionar uma plataforma para cursos online ou local adequado para cursos presenciais. • Promover os cursos e gerenciar inscrições. Criação de Materiais didáticos • Selecionar os tópicos a serem abordados, garantindo que estejam alinhados aos objetivos de aprendizado identificados. • Escolher o formato do material (e.g., apostilas, vídeos, apresentações, exercícios práticos).
Entregas	O projeto entregará serviços à comunidade, promovendo conhecimentos que visam a inclusão digital. Curso: planejamento do curso, incluindo módulos, temas abordados, objetivos de aprendizado, e cronograma. Materiais de Aula: Apostilas, slides, vídeos, e recursos complementares para cada módulo do curso. Manuais e Apostilas: Documentos detalhados que cobrem os temas do curso de forma estruturada, com explicações teóricas e exemplos práticos. Certificados de Participação: Certificados digitais ou impressos para os participantes que assistiram aos workshops e palestras. Relatórios de Avaliação: Relatórios que incluem feedback dos participantes, análise de impacto, e sugestões de melhorias para futuras edições
Instrumentos e procedimentos de avaliação	A avaliação se dará por meio de: • Condução dos trabalhos pelos estudantes • Comprovação da apresentação do material às comunidades, ou, em eventos da instituição abertos à comunidade • Os resultados serão medidos em relação ao alcance das ações através de quantidades de pessoas e empresas que tiveram contato com o projeto.
Componente(s) curricular(es) envolvidos	• Tecnologia da Informação nas Organizações • Princípios da Segurança da Informação • Diagnóstico e Soluções de Problemas em TI
Formas de evidência	• Divulgação dos Trabalhos • Fotos das ações e apresentações • Material produzido dos temas relacionados • Listas de divulgação dos encontros na unidade • Relatório final

Fls. 268 a 270

Título	Segurança Digital para Micro e Pequenas Empresas: Conscientização, políticas e gestão
Temática	Capacitação de micro e pequenas empresas para prevenir golpes digitais e ataques de engenharia social, promover melhores práticas de Segurança da Informação, e implementar políticas de segurança cibernética eficazes.
Descrição	O projeto "Segurança Digital para Micro e Pequenas Empresas: Conscientização, políticas e gestão" visa capacitar micro e pequenas empresas da região para protegerem suas operações contra ameaças cibernéticas. Dado o aumento dos ataques digitais e da importância da segurança da informação para a continuidade dos negócios, o projeto irá abordar a prevenção de golpes digitais, técnicas de engenharia social, e a implementação de políticas de segurança eficazes. A iniciativa inclui uma série de atividades educacionais e práticas, como workshops, treinamentos, e desenvolvimento de materiais específicos para ajudar os colaboradores e stakeholders a adotar padrões e práticas reconhecidas na proteção de recursos de TI, garantindo que a segurança cibernética suporte as estratégias e objetivos empresariais.
Objetivos	Aumentar o nível de conhecimento dos gestores e colaboradores das micro e pequenas empresas sobre prevenção de golpes digitais e ataques de engenharia social. Divulgar melhores práticas de Segurança da Informação que possam ser aplicadas nas operações cotidianas das empresas. Desenvolver e implementar políticas de segurança da informação que sejam práticas, eficazes e adaptáveis ao contexto das micro e pequenas empresas. Promover a conscientização sobre segurança cibernética entre colaboradores e stakeholders, preparando-os para agir de forma proativa em relação às ameaças digitais. Capacitar as empresas a utilizarem padrões e práticas reconhecidas para garantir que seus recursos de TI suportem suas estratégias e objetivos organizacionais.
Carga horária	94 aulas/78,3 horas
Público-alvo	Micro e pequenas empresas da região
Ações/Etapas de execução	Diagnóstico Inicial e Levantamento de Necessidades: Realizar uma pesquisa com micro e pequenas empresas da região para identificar o nível atual de conhecimento sobre segurança cibernética, práticas de prevenção de golpes digitais, e políticas de segurança existentes. Levantar necessidades específicas e desafios enfrentados pelas empresas em relação à segurança da informação.
	• Workshops e Treinamentos: • Workshops sobre Prevenção de Golpes Digitais e Engenharia Social:



	- Realizar workshops práticos e interativos sobre como identificar e prevenir golpes digitais e técnicas de engenharia social. - Simulações de situações reais para que os participantes aprendam a responder a tentativas de phishing, fraudes e outras ameaças digitais. Treinamentos em Boas Práticas de Segurança da Informação: - Sessões de treinamento sobre melhores práticas, como gestão de senhas, proteção de dados, autenticação multifator, e resposta a incidentes. - Capacitação para uso seguro de ferramentas e softwares comuns, como e-mail, navegadores e sistemas de gestão. Desenvolvimento de Políticas de Segurança da Informação: - Auxiliar as empresas a criar ou melhorar suas políticas de segurança da informação, adaptando-as às suas necessidades e realidade. - Sessões de consultoria personalizada para apoiar o desenvolvimento de políticas claras e aplicáveis, envolvendo todos os níveis da organização. Criação de Materiais Educativos e de Referência: - Desenvolvimento de guias práticos, checklists, infográficos e tutoriais para uso contínuo pelos colaboradores, facilitando a disseminação das melhores práticas. - Produção de vídeos explicativos e manuais para o treinamento de novos funcionários e reciclagem dos atuais. Acompanhamento e Avaliação: - Realizar visitas nas empresas participantes para avaliar a eficácia das políticas implementadas. - Coletar feedback dos participantes sobre aplicabilidade das medidas e o impacto percebido na segurança cibernética de suas empresas.
Entregas	Relatório de Diagnóstico Inicial: Documento com a análise das necessidades e desafios das micro e pequenas empresas em relação à segurança cibernética. Workshops e Treinamentos Realizados: Conjunto de materiais utilizados (slides, gravações, guias de estudo) e certificados de participação emitidos. Políticas de Segurança da Informação Desenvolvidas: Políticas personalizadas para cada empresa, incluindo diretrizes para prevenção de ataques cibernéticos.
	Materiais Educativos Criados: Apostilas, guias práticos, infográficos, vídeos tutoriais, checklists e FAQs. Relatórios de Acompanhamento e Avaliação: Relatórios detalhando os resultados das auditorias de segurança e feedbacks coletados.
Instrumentos e procedimentos de avaliação	A avaliação se dará por meio de: - Condução dos trabalhos pelos alunos e participantes. - Comprovação da apresentação do material e/ou eventos da instituição abertos às empresas. - Os resultados serão medidos em relação ao alcance das ações através de quantidades de pessoas e empresas que tiveram contato com o projeto.
Componente(s) curricular(es) envolvidos	- Análise e Gestão de Riscos em Segurança da Informação - Governança de Tecnologia da Informação - Fator Humano em Segurança da Informação - Políticas de Segurança da Informação
Formas de evidência	- Divulgação dos Trabalhos - Fotos das ações e apresentações - Material produzido dos temas relacionados - Listas de divulgação dos encontros - Relatório final

Fls. 271 a 272

Título	Matemática Sem Fronteiras: Projeto de Capacitação e Formação
Temática	Matemática básica e para preparação para vestibulares
Descrição	O projeto "Matemática Sem Fronteiras: Projeto de Capacitação e Formação" é uma iniciativa de extensão curricular que visa promover o aprendizado da matemática básica e avançada, inclusive a preparação da comunidade local para o vestibular da Fatec. O projeto busca proporcionar aulas de reforço, oficinas práticas, atividades interativas e/ou simuladas, com o objetivo de aumentar o conhecimento matemático da população, reduzir as desigualdades educacionais e facilitar o acesso ao ensino superior. O projeto poderá atender pessoas de diferentes faixas etárias e níveis de escolaridade.
Objetivos	- Promover a inclusão educacional, democratizando o acesso ao conhecimento matemático; - Elevar o nível de conhecimento em matemática de alunos da rede pública e da população; - Capacitar os participantes para resolver problemas típicos de provas de vestibular, principalmente com formato de conteúdo do vestibular da Fatec promovendo o acesso ao ensino superior; - Oferecer suporte contínuo por meio de materiais didáticos, aulas e mentorias.
Carga horária	30 aulas/25 horas
Público-alvo	Estudantes e a Comunidade Externa.
Ações/Etapas de execução	Planejamento e Organização: - Criação de um cronograma de aulas e atividades. - Elaboração de materiais didáticos (apostilas, vídeos, listas de exercícios, simulados entre outros). - Divulgação do projeto na comunidade por meio de redes sociais, parcerias com escolas e associações comerciais e comunitárias. Execução das Aulas e/ou Oficinas: - Realização de aulas presenciais ou online, abordando conteúdos de matemática básica e avançada. - Oficinas práticas focadas em resolução de problemas, técnicas de estudo e métodos de memorização. - Sessões de tutoria para apoiar os participantes com maiores dificuldades. - Aplicação de simulados mensais, simulando o formato e as questões do vestibular da Fatec. Acompanhamento e Avaliação: - Correção e feedback das atividades dos participantes para identificar pontos de melhoria e reforçar os conteúdos necessários. - Realização de grupos de estudo para promover a aprendizagem colaborativa. - Coleta de feedback dos participantes e da equipe sobre o projeto.



Entregas	• Apostilas e materiais didáticos. • Relatórios de desempenho baseados nos resultados das atividades. • Certificados de participação para todos os que completarem o curso. • Relatório final do projeto com avaliação dos resultados e sugestões para futuras edições.
Instrumentos e procedimentos de avaliação	A avaliação se dará por meio de: • Condução dos trabalhos pelos alunos e participantes. • Comprovação da apresentação do material e/ou eventos de instituição abertos à comunidade. • Os resultados serão medidos em relação ao alcance das ações através de quantidades de pessoas e organizações que tiveram contato com o projeto. • Questionários e entrevistas com os participantes para obter feedback sobre o conteúdo, a metodologia de ensino e o impacto do projeto.
Componente(s) curricular(es) envolvidos	• Matemática Discreta • Probabilidade e Estatística.
Formas de evidência	• Divulgação dos Trabalhos • Fotos das ações e apresentações • Material produzido dos temas relacionados • Listas de divulgação dos encontros • Relatório final

Fis. 273 a 275

Título	Prática Profissional em Segurança da Informação: Desenvolvimento de Atividade Estratégica no Ambiente de Estágio
Temática	Aplicação prática de conceitos de Segurança da Informação em ambiente empresarial
Descrição	O projeto "Prática Profissional em Segurança da Informação" visa proporcionar ao aluno do curso de Segurança da Informação uma oportunidade de desenvolver alguma atividade prática e estratégica durante o seu estágio em uma empresa de qualquer segmento e não necessariamente o segmento de TI. Essa atividade deverá ser relacionada à segurança da informação, como estudos para capacitação da empresa neste âmbito, a proposição e, se possível, a implementação de uma política de segurança, o desenvolvimento de um plano de resposta a incidentes, a realização de uma auditoria de segurança, a aplicação de controles de proteção de dados, entre outras atividades que podem ser delineadas durante o estágio com a coordenação de estágios e/ou coordenação de cursos. O aluno deverá documentar todas as etapas do desenvolvimento dessa atividade e apresentar um relatório final detalhado, que será utilizado como parte da avaliação do seu estágio.
Objetivos	• Identificar uma necessidade ou problema relacionado à segurança da informação na empresa de estágio. • Desenvolver e executar uma atividade prática de segurança da informação no ambiente de estágio, aplicando conhecimentos teóricos adquiridos ao longo do curso. • Planejar e implementar uma solução que aborde a necessidade identificada. • Aplicar metodologias e ferramentas apropriadas de segurança da informação. • Avaliar o impacto da atividade desenvolvida sobre a segurança da informação da empresa. • Documentar o processo de desenvolvimento da atividade, incluindo desafios, soluções, resultados e aprendizados.
Carga horária	72 aulas
Público-alvo	Empresas
Ações/Etapas de execução	Identificação da necessidade • Análise inicial do ambiente de TI da empresa de estágio para identificar vulnerabilidades, riscos ou oportunidades de melhoria na segurança da informação mediante a realização de uma capacitação sobre um determinado aspecto envolvido no curso. • Reuniões com o supervisor de estágio e a equipe de TI para definir a atividade de segurança a ser proposta durante o estágio. Planejamento da atividade: • Definição dos objetivos específicos da atividade, recursos necessários e cronograma de execução. • Elaboração de um plano de ação detalhado, incluindo a metodologia a ser utilizada, etapas de execução e critérios de avaliação.
Entregas	Implementação da atividade: • Execução do plano de ação, aplicando as ferramentas e metodologias de segurança da informação apropriadas. • Monitoramento contínuo dos resultados e ajustes conforme necessário para garantir a eficácia da atividade desenvolvida. Avaliação e publicação dos resultados: • Análise dos resultados obtidos com a atividade, utilizando métricas de segurança, relatórios de monitoramento e feedback da equipe. • Identificação de melhorias e recomendações para fortalecer ainda mais a segurança da informação na empresa. • Preparação de um relatório final detalhado, descrevendo todas as etapas da atividade, metodologias utilizadas, resultados alcançados, desafios enfrentados e aprendizados. • Apresentação do relatório para o supervisor de estágio e para a coordenação de estágio / curso.
Instrumentos e procedimentos de avaliação	Avaliação do Supervisor de Estágio: • Feedback do supervisor sobre a participação do aluno, comprometimento, habilidades técnicas e resultados obtidos com a atividade desenvolvida. Avaliação do Relatório Final: • Análise do relatório final pelo coordenador do estágio, considerando clareza, detalhamento, profundidade da análise e conformidade com as melhores práticas de segurança da informação.



	Auto avaliação do Aluno: Reflexão escrita do aluno sobre sua experiência, desafios enfrentados, habilidades desenvolvidas e impacto percebido da atividade na segurança da informação da empresa.
Componente(s) curricular(es) envolvidos	Estágio Curricular Supervisionado
Formas de evidência	- Anuência do supervisor de estágio - Relatório final - Comprovantes das atividades

Fis. 276 a 278

Título	Gestão Ética de Segurança da Informação
Temática	Gestão de Segurança da Informação, Ética Profissional e Ordenamento Jurídico na Tecnologia da Informação
Descrição	O projeto "Gestão Ética de Segurança da Informação" tem como propósito capacitar micro e pequenas empresas, além da comunidade local, na criação e implementação de planos de gestão de Segurança da Informação. Seu principal objetivo é fomentar uma compreensão dos princípios éticos, bem como identificar e interpretar os conceitos-chave e normas do ordenamento jurídico aplicáveis ao setor de TI, com destaque para as leis referentes à segurança da informação. A iniciativa poderá contar com o desenvolvimento de cenários e a formulação de estratégias para mitigar riscos e enfrentar as consequências jurídicas e éticas das ações realizadas dentro do contexto ou por meio de recursos de TI. Além disso, alguns artefatos gerados e entregues, como, por exemplo, manuais, poderão ser traduzidos para a língua inglesa para aumentar o impacto do projeto, que poderá ser prospectado em níveis internacionais.
Objetivos	- Capacitar as micro e pequenas empresas e a comunidade na construção, entendimento e implementação de um plano gerencial de Segurança da Informação, fundamentado em práticas éticas em conformidade com as legislações vigentes, fornecendo conhecimento sobre os princípios de segurança da informação, incluindo confidencialidade, integridade e disponibilidade. - Identificar e interpretar as principais leis e regulamentos aplicáveis à segurança da informação no Brasil, como, por exemplo, a LGPD (Lei Geral de Proteção de Dados) e o Marco Civil da Internet. - Promover o entendimento das implicações éticas e jurídicas dos atos realizados no âmbito ou através de recursos de TI. - Elaborar modelos de planos gerenciais de segurança da informação, adequados a diferentes cenários e necessidades das empresas ou membros da comunidade participantes. - Tradução de alguns materiais didáticos produzidos para o idioma inglês para aumentar a abrangência do projeto.
Carga horária	80 aulas/66,6 horas
Público-alvo	Micro e pequenas empresas da região e a comunidade.
Ações/Etapas de execução	Capacitação Inicial e Workshops - Criação de materiais didáticos, incluindo apostilas, slides, vídeos explicativos e estudos de caso. - Divulgação do projeto para a comunidade e micro e pequenas empresas através de redes sociais, parcerias com associações comerciais e visitas diretas. - Realização de workshops presenciais ou online sobre os fundamentos de segurança da informação, sessões de capacitação sobre ética profissional, leis de proteção de dados e outras legislações relevantes, como, por exemplo, a LGPD e o Marco Civil da Internet.
	- Discussão de estudos de caso e análise de situações reais envolvendo infrações à segurança da informação e suas consequências jurídicas, como ataques cibernéticos, vazamento de dados e interrupções de serviço. - Orientação e suporte para a criação de planos gerenciais de segurança da informação personalizados, adaptados às necessidades e características específicas de cada empresa participante. Tradução para língua inglesa - Traduzir parte dos materiais gerados para o inglês, facilitando a prospecção em mercados internacionais. Avaliação e Ajuste - Revisão dos planos gerenciais desenvolvidos, garantindo conformidade com as melhores práticas e com os requisitos legais. - Coleta de feedback dos participantes sobre o impacto do projeto e as melhorias percebidas.
Entregas	- Modelos de planos gerenciais de segurança da informação, ajustados para diferentes cenários. - Materiais didáticos (apostilas, guias práticos, estudos de caso). - Materiais didáticos traduzidos para a língua inglesa. - Relatórios de simulações de incidentes e avaliações de eficácia dos planos. - Certificados de participação para os participantes que completarem o programa. - Relatório final do projeto com análise de resultados, feedback dos participantes e recomendações para continuidade.
Instrumentos e procedimentos de avaliação	A avaliação se dará por meio de: - Condução dos trabalhos pelos alunos e participantes. - Comprovação da apresentação do material e/ou eventos da instituição. - Os resultados serão medidos em relação ao alcance das ações através de quantidades de pessoas e organizações que tiveram contato com o projeto. - Questionários e entrevistas com os participantes para obter feedback sobre o conteúdo, a metodologia de ensino e o impacto do projeto.
Componente(s) curricular(es) envolvidos	- Direito e Ética Profissional na Sociedade da Informação - Gestão da Segurança da Informação - Inglês VI
Formas de evidência	- Divulgação dos Trabalhos - Fotos das ações e apresentações - Material produzido dos temas relacionados - Listas de divulgação dos encontros - Relatório final



1.2.10 Da Comissão de Especialistas

A Comissão de Especialistas analisou os documentos constantes dos autos e realizou visita *in loco* elaborando Relatório Circunstanciado, de fls. manifestando-se favoravelmente ao reconhecimento do Curso em comento.

Todavia em seu relatório, destacam que *"Da relação de livros disponíveis para o curso, notou-se que o acervo físico apresenta deficiências, devido à falta de atualização"*, observação que acolha plenamente.

1.2.13 Considerações Finais

Acolho e recebo elementos positivos e negativos evidenciados no Relatório dos Especialistas e isto posto, e pelo que mais remanesce nos presentes, conheço do pedido e voto no sentido de deferir o pedido de Renovação do Reconhecimento do Curso Superior de Tecnologia em Segurança da Informação mantido pelo Centro Estadual de Educação Tecnológica Paula Souza / FATEC Araraquara pelo prazo de 5 (cinco) anos, nos termos da Deliberação CEE 171/2019.

2. CONCLUSÃO

2.1 Aprova-se, com fundamento na Deliberação CEE 171/2019, o pedido de Renovação do Reconhecimento do Curso Superior de Tecnologia em Segurança da Informação, oferecido pela FATEC Araraquara, do Centro Estadual de Educação Tecnológica Paula Souza, pelo prazo de cinco anos.

2.2 A IES deverá atender integralmente as conclusões dos Especialistas com vista ao novo ciclo avaliatório.

2.3 A presente renovação do reconhecimento tornar-se-á efetiva por ato próprio deste Conselho, após homologação deste Parecer pela Secretaria de Estado da Educação.

São Paulo, 27 de janeiro de 2026.

a) Cons. Roque Theophilo Junior
Relator

3. DECISÃO DA CÂMARA

A CÂMARA DE EDUCAÇÃO SUPERIOR adota, como seu Parecer, o Voto do Relator.

Presentes os Conselheiros Anderson Ribeiro Correia, Cláudio Mansur Salomão, Décio Lencioni Machado, Eliana Martorano Amaral, Hubert Alquéres, Marcos Sidnei Bassi, Mário Vedovello Filho, Nina Beatriz Stocco Ranieri e Roque Theophilo Junior.

Reunião por videoconferência, 28 de janeiro de 2026.

a) Cons. Hubert Alquéres
Presidente da Câmara de Educação Superior

DELIBERAÇÃO PLENÁRIA

O CONSELHO ESTADUAL DE EDUCAÇÃO toma conhecimento, da decisão da Câmara de Educação Superior, nos termos do Voto do Relator.

Sala "Carlos Pasquale", em 04 de fevereiro de 2026.

Consª Maria Helena Guimarães de Castro
Presidente

Parecer CEE 17/2026	-	Publicado no DOESP em 05/02/2026	-	Seção I	-	Página 25
Res. Seduc de 09/02/2026	-	Publicada no DOESP em 13/02/2026	-	Seção I	-	Página 38
Portaria CEE-GP 40/2026	-	Publicada no DOESP em 18/02/2026	-	Seção I	-	Página 45

