**Identificação do curso**

**Título do curso:** Tecnologia em Segurança da Informação

**Eixo tecnológico:** Informação e Comunicação

**Segmento:** Tecnologia da Informação

**Carga horária:** 2.000 horas

**Código DN:** 3002

**CBO da ocupação:** 2123-20 – Tecnólogo em segurança da informação

**CBO sinônimos:** 2123-20 – Administrador em segurança da informação

2123-20 – Analista em segurança da informação

2123-20 – Especialista em segurança da informação

**Família:** 2123 – Administradores de tecnologia da informação

**Perfil profissional de conclusão**

O tecnólogo em segurança da informação é o profissional responsável pela análise, proposição e implementação de soluções que visem a manutenção da confidencialidade, integridade e disponibilidade da tecnologia da informação. Realiza análise de risco, auditoria, perícia, emite laudo e parecer técnico quanto à segurança da informação.

O egresso do curso poderá atuar em organizações e empresas de diversos segmentos e portes que utilizem a tecnologia da informação como ferramenta de suporte nos processos operacionais e na tomada de decisão, tais como: indústria, comércio e serviços, organizações não-governamentais, órgãos públicos, institutos e centros de pesquisa e instituições de ensino.

Trabalha e interage em equipes multidisciplinares em projetos locais e/ou globais, articulando-se com as mais diversas áreas das organizações.

O tecnólogo em segurança da informação formado pelo Senac tem como Marcas Formativas: domínio técnico-científico, visão crítica, colaboração e comunicação, criatividade e atitude empreendedora, autonomia digital e atitude sustentável. Essas Marcas reforçam o compromisso da Instituição com a formação integral do ser humano, considerando aspectos relacionados ao mundo do trabalho, ao exercício da cidadania e às questões específicas de cada região. Tal perspectiva propicia o comprometimento do profissional com a qualidade do trabalho, com o desenvolvimento de uma visão ampla e consciente sobre sua atuação profissional e sua capacidade de transformação da sociedade.

Nesse sentido, as Marcas Formativas equivalem às competências gerais que compõem este perfil profissional.

A seguir, as competências específicas que compõem o perfil do tecnólogo em segurança da informação:

1. Identificar, diagnosticar e avaliar vulnerabilidades de sistemas de informação nas organizações.
2. Desenvolver, implementar e acompanhar a política de segurança da informação (PSI).
3. Desenhar e implantar soluções de segurança da informação.
4. Emitir laudos e pareceres técnicos quanto à segurança da informação.
5. Coordenar projetos e equipes multidisciplinares de produção de sistemas computacionais de informação.
6. Realizar auditorias e análises de riscos em sistemas de informação.
7. Projetar e gerenciar redes de computadores seguras.
8. Planejar soluções computacionais e executar procedimentos para processos de negócios.
9. Propor atualização tecnológica quanto a equipamentos e ferramentas de segurança da informação utilizadas nas organizações.

**Detalhamento das competências**

1. **Identificar, diagnosticar e avaliar vulnerabilidades de sistemas de informação nas organizações.**

**Descritivo:** espera-se que os alunos sejam capazes de realizar estudos em ambientes informatizados com o intuito de identificar as possíveis vulnerabilidades, avaliar suas consequências e, a partir disso, materializar o diagnóstico por meio de relatórios técnicos.

**Abarca unidades curriculares que abordam:** processos deanálise de vulnerabilidade em sistemas de informação e princípios de segurança cibernética.

1. **Desenvolver, implementar e acompanhar a política de segurança da informação (PSI)**

**Descritivo:** espera-se que os alunos sejam capazes de atuar no desenvolvimento da política de segurança da informação (PSI) de uma organização, levando em consideração as práticas, as normas, os procedimentos e os costumes existentes, contribuindo para sua implementação e promovendo revisões periódicas no documento.

**Abarca unidades curriculares que abordam:** as boas práticasda gestão da segurança da informação (ISO 27001/27002), conhecimentos relacionados ao direito digital e ao planejamento estratégico das organizações.

1. **Desenhar e implantar soluções de segurança da informação**

**Descritivo:** espera-se que os alunos sejam capazes de identificar necessidades em ambientes computacionais quanto a aspectos da segurança da informação, desenhando arquiteturas e implementando estruturas que mitiguem os problemas encontrados.

**Abarca unidades curriculares que abordam:** conteúdos relacionados ainfraestrutura de *hardware*, segurança em redes de computadores, protocolos de redes, ferramentas e equipamentos utilizados em estruturas de segurança da informação.

1. **Emitir laudos e pareceres técnicos quanto à segurança da informação**

**Descritivo:** espera-se que os alunos sejam capazes de realizar estudos em situações específicas na área de segurança da informação (incidentes, acessos maliciosos, investigações), emitindo laudos e pareceres técnicos solicitados.

**Abarca unidades curriculares que abordam:** princípios da área deperícia eforense computacional**,** conhecimentos de direito digital,sistemas operacionais, criptografia e segurança cibernética.

1. **Coordenar projetos e equipes multidisciplinares de produção de sistemas computacionais de informação.**

**Descritivo:** espera-se que os alunos sejam capazes de liderar equipes multidisciplinares em projetos associados às áreas da TI voltados à produção de sistemas de informação, sempre observando as boas práticas vigentes no mercado de trabalho.

**Abarca unidades curriculares que abordam:** as práticas de gestão de projetos e conteúdos que abordem o exercício da liderança, o gerenciamento de conflito e a ética profissional.

1. **Realizar auditorias e análises de riscos em sistemas de informação**

**Descritivo:** espera-se que os alunos sejam capazes de auditar sistemas de informação e fazer a análise de riscos correspondente, utilizando ferramentas adequadas e atendendo a eventuais legislações vigentes associadas ao contexto.

**Abarca unidades curriculares que abordam:** conteúdos sobre*softwares*, ferramentas e procedimentos para auditorias, gestão de riscos em sistemas de informação e segurança de dados.

1. **Projetar e gerenciar redes de computadores seguras**

**Descritivo:** espera-se que os alunos sejam capazes de desenhar e gerenciar soluções de tecnologia por meio de estruturas físicas (equipamentos e dispositivos) e/ou lógicas (ferramentas, *softwares*) que controlem as vulnerabilidades e tragam mais segurança às redes de computadores de uma organização.

**Abarca unidades curriculares que abordam:** o contexto de projetos e segurança em redes de computadores e sistemas operacionais, além de infraestruturas de TI.

1. **Planejar soluções computacionais e executar procedimentos para processos de negócios**

**Descritivo:** espera-se que os alunos sejam capazes de propor e executar soluções computacionais por meio de procedimentos que visam a continuidade dos sistemas de missão crítica da organização, considerando a prática dos processos de negócios existentes.

**Abarca unidades curriculares que abordam:** planejamento estratégico nas organizações e gestão do conhecimento e de projetos.

1. **Propor atualização tecnológica quanto a equipamentos e ferramentas de segurança da informação utilizadas nas organizações**

**Descritivo:** espera-se que os alunos sejam capazes de analisar o parque tecnológico de uma organização que envolva a área de segurança da informação e propor possíveis atualizações quanto ao uso de ferramentas e equipamentos que melhorem o controle e monitoramento dos ambientes computacionais.

**Abarca unidades curriculares que abordam:** infraestruturas de TI, bem como os tipos de equipamentos e soluções utilizadas em arquiteturas que envolvem a segurança da informação (redes, *hardware*, ferramentas, protocolos).

**Orientações de convergência com o Curso Técnico em Redes de Computadores**

**Contexto**

Durante o desenvolvimento do perfil profissional de conclusão do Curso Superior de Tecnologia (CST), observou-se que as competências propostas neste perfil do tecnólogo em segurança da informação, à luz das competências que compõem o Curso Técnico em Redes de Computadores do segmento de Informação e Comunicação, tinham amplitude e complexidade diferentes.

No entanto, para permitir a possibilidade de convergência e contribuir para o itinerário formativo do aluno Senac, explicitamos as competências do técnico contidas nas competências específicas do perfil profissional de conclusão do tecnólogo para apoiar a construção, no âmbito da organização curricular proposta por cada DR ofertante, das unidades curriculares no nível superior. O quadro elaborado indica as competências do PCN de habilitação técnica do Curso de Informática que estão relacionadas com as competências do Curso Superior de Tecnologia em Segurança da Informação e de que forma indicamos essas correlações.

Cada DR irá analisar o perfil alinhado do CST (competências, indicações de aproveitamento de estudos e temáticas afins) e definir sua organização curricular e seus critérios para aproveitamento conforme processos próprios da instituição e à luz da legislação vigente.

**ANÁLISE DE CONVERGÊNCIA**

Tendo como referência o curso de Habilitação Técnica em Redes de Computadores, fizemos uma primeira aproximação de convergência com base nos conhecimentos e nas habilidades utilizando a ferramenta Excel.

Após análise preliminar, aprofundamos a identificação da convergência considerando também os indicadores. Na sequência, fizemos recomendações para o aproveitamento das competências do técnico apontando em que medida elas podem ser aproveitadas no tecnólogo, tendo em vista o nível de complexidade na mobilização dos saberes e o contexto da ação profissional.

Em síntese, apesar de termos verificado a possibilidade de convergência entre o Técnico em Redes de Computadores e o Curso Superior de Tecnologia em Segurança da Informação, esse cenário não viabiliza, necessariamente, um efetivo aproveitamento. Neste caso, observamos que as competências do técnico assumem caráter mais operacional, enquanto as do tecnólogo estão mais relacionadas às dimensões de planejamento e gestão.

O quadro a seguir apresenta as competências específicas do perfil profissional de conclusão do CST em Segurança da Informação, suas respectivas descrições, as UCs do Curso Técnico em Redes de Computadores analisadas e as recomendações para o aproveitamento das mesmas.

|  |  |  |  |
| --- | --- | --- | --- |
| **Competências específicas do Tecnólogo em Segurança da Informação** | **Descrição da competência CST** | **Unidade curricular analisada** | **Recomendações para o aproveitamento** |
| Identificar, diagnosticar e avaliar vulnerabilidades de sistemas de informação nas organizações. | Espera-se que os alunos sejam capazes de realizar estudos em ambientes informatizados com o intuito de identificar as possíveis vulnerabilidades, avaliar suas consequências e, a partir disso, materializar o diagnóstico por meio de relatórios técnicos. | UC 12, UC 13 | **Não há convergência** – apesar da existência de conteúdo relativo aos processos básicos, como segurança de rede sem fio e criptografia de dados, que perpassam as UCs 12 e 13 do Técnico em Rede de Computadores e a competência em questão, o técnico não aprofunda os conteúdos de proteção de redes, como monitoramento de redes, sistemas de gerenciamento de protocolos, sistema *firewall* e análise de vulnerabilidade. Portanto, não há viabilidade de convergência entre UCs do Técnico e a competência do Tecnólogo. |
| Desenvolver, implementar e acompanhar a política de segurança da informação (PSI). | Espera-se que os alunos sejam capazes de atuar no desenvolvimento da política de segurança da informação (PSI) de uma organização, levando em consideração as práticas, as normas, os procedimentos e os costumes existentes, contribuindo para sua implementação e realizando revisões periódicas no documento. | UC 15 | **Não há convergência –** a UC em questão desenvolve a política de projetos, mas não o conteúdo de PSI, em que as violações de segurança de rede podem interromper o comércio eletrônico. Essas violações, quando não abordadas de forma adequada, podem resultar em perda de receita para as empresas, roubo de propriedade intelectual, ações judiciais e até ameaçar a segurança pública. |
| Desenhar e implantar soluções de segurança da informação. | Espera-se que os alunos sejam capazes de identificar necessidades em ambientes computacionais quanto a aspectos da segurança da informação, desenhando arquiteturas e implementando estruturas que mitiguem os problemas encontrados. | UC 3, UC 11, UC 13, UC 14 | **Convergência parcial** – as UCs indicadas mobilizam elementos introdutórios de ataques básicos, criptografias, seguranças de *endpoints* e IPS e suas tecnologias, temas que são abordados também no CST, porém em um nível de profundidade mais avançado. No entanto, não leva em consideração conhecimentos especificos de criação de redes seguras, mitigação de ameaças e ou listas de controle de acessos, pois apresentam abrangência menor neste quesito de segurança. |
| Emitir laudos e pareceres técnicos quanto à segurança da informação. | Espera-se que os alunos sejam capazes de realizar estudos em situações específicas na área de segurança da informação (incidentes, acessos maliciosos, investigações), emitindo laudos e pareceres técnicos solicitados. | - | **Não há convergência –** inexiste UC relativa ao conteúdo abordado nesta competência. |
| Coordenar projetos e equipes multidisciplinares de produção de sistemas computacionais de informação. | Espera-se que os alunos sejam capazes de liderar equipes multidisciplinares em projetos associados às áreas da tecnologia da informação voltados à produção de sistemas de informação, sempre observando as boas práticas vigentes no mercado de trabalho. | UC 15 | **Não há convergência** – apesar da correlação de temáticas entre a UC do Técnico e a competência do Tecnólogo, como gerenciamento de projetos e utilização de metodologias ágeis, as UCs do técnico não aprofundam em modelos e *frameworks* de governança de TI. |
| Realizar auditorias e análises de riscos em sistemas de informação. | Espera-se que os alunos sejam capazes de auditar sistemas de informação e fazer a análise de riscos correspondente, utilizando ferramentas adequadas e atendendo a eventuais legislações vigentes associadas ao contexto. | - | **Não há convergência –** inexiste UC relativa ao conteudo abordado nesta competência. |
| Projetar e gerenciar redes de computadores seguras. | Espera-se que os alunos sejam capazes de desenhar e gerenciar soluções de tecnologia por meio de estruturas físicas (equipamentos e dispositivos) e/ou lógicas (ferramentas, *softwares*) que controlem as vulnerabilidades e tragam mais segurança às redes de computadores de uma organização. | UC 9, UC 11, UC 14, UC 15 | **Convergência integral** – pois as unidades trabalham conceitos de políticas de segurança semelhantes aos abordados nesta competência, sendo capazes de identificar e elaborar políticas de infraestrutura de TI seguras |
| Planejar soluções computacionais e executar procedimentos para processos de negócios. | Espera-se que os alunos sejam capazes de propor e executar soluções computacionais por meio de procedimentos que visam a continuidade dos sistemas de missão crítica da organização, considerando a prática dos processos de negócios existentes. | UC 15 | **Não há convergência –** apesar da existência de conteúdo relativo aos processos básicos de gestão, como a criação de métricas de acordo com as regras de negócio da organização que perpassam a UC 15 do técnico em Rede de Computadores e a competência em questão, o técnico não aprofunda o planejamento estratégico da gestão e a continuidade de negócios. |
| Propor atualização tecnológica quanto a equipamentos e ferramentas de segurança da Informação utilizadas nas organizações. | Espera-se que os alunos sejam capazes de analisar o parque tecnológico de uma organização que envolva a área de segurança da informação e propor possíveis atualizações quanto ao uso de ferramentas e equipamentos que melhorem o controle e o monitoramento dos ambientes computacionais. | UC 3 | **Convergência parcial** – há correlação temática em metodologias de desenvolvimento de *software*, uso de ferramentas, monitoramento e configuração de redes. No entanto, a UC em questão promove a implementação de servidores para redes locais, ao passo que o Tecnólogo explora o mesmo contexto por meio de servidores em nuvem aliados a aplicações específicas de segurança da informação. |