**Identificação do curso**

Título do curso: Tecnologia em Defesa Cibernética

Eixo tecnológico: Informação e Comunicação

Segmento: Tecnologia da Informação

Carga horária: 2.000 horas

Código DN: 2998

CBO da ocupação:

CBO sinônimos: 2123-20 – Analista em segurança da informação.

2123-20 – Tecnólogo em segurança da informação.

2124-10 – Analista de redes e de comunicação de dados.

Família: 2123 – Administradores de tecnologia da informação

**Perfil profissional de conclusão**

O tecnólogo em defesa cibernética é o profissional responsável por monitorar os ataques cibernéticos, testar e manter redes de computadores, sistemas computacionais de informação e dispositivos conectados em redes ou *off-line* contra perda de dados. Sua formação confere habilidades para avaliação e emissão de pareceres técnicos, propiciando a implantação de soluções de tecnologia da informação.

Ele atuará em empresas públicas e privadas, de pequeno, médio e grande porte, nas áreas de elaboração, implantação e gerenciamento de políticas e mecanismos técnicos de segurança cibernética. O egresso também estará apto a atuar no ramo de assessoria e consultoria na área de informática.

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

O tecnólogo em defesa cibernética 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 defesa cibernética:

1. Coordenar projetos de sistemas computacionais de informação para a proteção de ameaças e invasões cibernéticas.
2. Implantar soluções computacionais a partir do conhecimento acerca dos processos de negócios.
3. Estabelecer estudos de viabilidade técnica e econômica, laudos, perícias e pareceres técnicos, propiciando a implantação de soluções de tecnologia da informação.
4. Investigar e monitorar ataques cibernéticos.
5. Planejar, projetar e configurar ferramentas e mecanismos de segurança.
6. Manter as políticas de segurança tanto das corporações quanto das diversas ferramentas que as implementam.

**Detalhamento das competências**

1. **Coordenar projetos de sistemas computacionais de informação para a proteção de ameaças e invasões cibernéticas**

**Descritivo:** espera-se que os alunos sejam capazes de conceber a aplicação de metodologias adequadas de gestão de projetos em tecnologia da informação, considerando variáveis econômicas, tecnológicas, organizacionais, ambientais e sociais, contribuindo para assegurar a viabilidade, a proteção e a segurança dos sistemas de TIC, a sustentabilidade e a qualidade dos produtos desenvolvidos e/ou dos serviços oferecidos.

**Abarca unidades curriculares que abordam:** gestão de projetos; gestão de produtos e serviços; ameaças e invasões cibernéticas.

1. **Implantar soluções computacionais a partir do conhecimento acerca dos processos de negócios**

**Descritivo:** espera-se que os alunos sejam capazes de identificar necessidades de defesa e segurança nos processos de negócios e da cadeia de valor dos empreendimentos no campo dos sistemas computacionais de informação, considerando os cenários prováveis e as soluções viáveis sob o ponto de vista econômico, tecnológico, organizacional, ambiental e social.

**Abarca unidades curriculares que abordam:** a gestão da continuidade dos negócios; normas técnicas relacionadas à defesa e à segurança da informação; empreendedorismo e inovação;

1. **Estabelecer estudos de viabilidade técnica e econômica, laudos, perícias e pareceres técnicos, propiciando a implantação de soluções de tecnologia da informação**

**Descritivo:** espera-se que os alunos sejam capazes de identificar, monitorar e mitigar as ameaças relacionadas à computação forense aplicada em diferentes contextos e investigações, bem como compreender as implicações legais e éticas da computação forense em contextos investigativos.

**Abarca unidades curriculares que abordam:** conceitos e técnicas de computação forense aplicadas a investigações; legislações e normas técnicas nacionais e internacionais aplicadas à defesa e segurança da informação.

1. **Investigar e monitorar ataques cibernéticos**

**Descritivo:** espera-se que os alunos sejam capazes de planejar e estabelecer procedimentos e protocolos contra invasão de redes e guerra eletrônica, visando a defesa e a segurança dos ambientes corporativos.

**Abarca unidades curriculares que abordam:** os protocolos e ferramentas de defesa e segurança da informação; mecanismos de redução de vulnerabilidades e ataques a sistemas cibernéticos; proteção de dispositivos de redes.

1. **Planejar, projetar e configurar ferramentas e mecanismos de segurança**

**Descritivo:** espera-se que os alunos sejam capazes de identificar ameaças, necessidades de defesa e segurança e aplicar os mecanismos adequados para redução de invasões cibernéticas.

**Abarca unidades curriculares que abordam:** protocolos e ferramentas de monitoramento e detecção de falhas; ameaças de segurança cibernética em *sites* e ambientes conectados; normas técnicas de defesa e segurança da informação.

1. **Manter as políticas de segurança tanto das corporações quanto das diversas ferramentas que as implementam**

**Descritivo:** espera-se que os alunos sejam capazes de preservar as políticas de segurança nas corporações e nas ferramentas que as implementam para a proteção de um ambiente de TI corporativo.

**Abarca unidades curriculares que abordam:** normas técnicas de defesa e segurança da informação.

**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 para o tecnólogo em defesa cibernética, à luz das competências que compõem o Curso Técnico de Redes de Computadores do segmento de Informação e Comunicação, tinham amplitude e complexidade diferentes.

No entanto, para permitir a possibilidade de convergência e contribuir com 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 Redes de Computadores que estão relacionadas com as competências do Curso Superior de Tecnologia em Defesa Cibernética 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 de estudos 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 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 e o tecnólogo, 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 Defesa Cibernética, 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 Defesa Cibernética** | **Descrição da competência CST** | **Unidade curricular do técnico** | **Recomendações para o aproveitamento** |
| Coordenar projetos de sistemas computacionais de informação para a proteção de ameaças e invasões cibernéticas. | Espera-se que os alunos sejam capazes de conceber a aplicação de metodologias adequadas de gestão de projetos em tecnologia da informação, considerando variáveis econômicas, tecnológicas, organizacionais, ambientais e sociais, contribuindo para assegurar a viabilidade, a proteção e a segurança dos sistemas de TIC, a sustentabilidade e a qualidade dos produtos desenvolvidos e/ou dos serviços oferecidos. | 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 que promovam a segurança dos sistemas de TI. |
| Implantar soluções computacionais a partir do conhecimento acerca dos processos de negócios | Espera-se que os alunos sejam capazes de identificar necessidades de defesa e segurança nos processos de negócios e na cadeia de valor dos empreendimentos no campo dos sistemas computacionais de informação, considerando os cenários prováveis e as soluções viáveis sob o ponto de vista econômico, tecnológico, organizacional, ambiental e social. | 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 continuidade de negócios. |
| Estabelecer estudos de viabilidade técnica e econômica, laudos, perícias e pareceres técnicos, propiciando a implantação de soluções de tecnologia da informação. | Espera-se que os alunos sejam capazes de identificar, monitorar e mitigar as ameaças relacionadas à computação forense aplicada em diferentes contextos e investigações, bem como compreender as implicações legais e éticas da computação forense em contextos investigativos. | - | **Não há convergência** – inexiste UC relativa ao conteúdo abordado nesta competência. |
| Investigar e monitorar ataques cibernéticos. | Espera-se que os alunos sejam capazes de planejar e estabelecer procedimentos e protocolos contra invasão de redes e guerra eletrônica, visando a defesa e a segurança dos ambientes corporativos. | UC 5, UC 11, UC 12, UC 13, UC 14 | **Há convergência integral**, pois as unidades trabalham conceitos de políticas de segurança semelhantes aos abordados nesta competência, sendo capazes de identificar e elaborar politicas de infraestrutura de TI seguras |
| Planejar, projetar e configurar ferramentas e mecanismos de segurança. | Espera-se que os alunos sejam capazes de identificar ameaças, necessidades de defesa e segurança e aplicar os mecanismos adequados para a redução de invasões cibernéticas. | UC 11, UC 13, UC 14 | **Convergência parcial** – as UCs indicadas ao lado mobilizam elementos introdutórios de ataques básicos, criptografias e suas tecnologias, temas que são abordados também no CST, porém em um nível de profundidade mais avançado. Além disso, as UCs do técnico não levam em consideração conhecimentos específicos de monitoramento de redes seguras, mitigação de ameaças e ou teste de intrusão de ataques, pois têm menos abrangência neste quesito de segurança. |
| Manter as políticas de segurança tanto das corporações quanto das diversas ferramentas que as implementam. | Espera-se que os alunos sejam capazes de preservar as políticas de segurança nas corporações e nas ferramentas que as implementam para a proteção de um ambiente de TI corporativo. | - | **Não há convergência** – inexiste UC relativa ao conteúdo abordado nesta competência. |