São Paulo Skills SENAI

DESCRITIVO

#54 Segurança Cibernética

SENAI

A São Paulo Skills, por decisão do Comitê de Gestores e de acordo com as Regras da Competição, adotou os seguintes requisitos mínimos para a execução desta ocupação na São Paulo Skills.
O Descritivo Técnico consiste em:

Sumário

INTRODUÇÃO

1.1 NOME E DESCRIÇÃO DA OCUPAÇÃO

1.1.1 O nome dessa ocupação é:

Segurança Cibernética

1.1.2 Descrição das funções ou dos papeis dessa ocupação

Nos últimos anos, tem havido um enorme crescimento nas transações comerciais online, na Internet das Coisas (IoT) e na computação em nuvem. Ao mesmo tempo, a TI se tornou uma ferramenta política oficial e não oficial, bem como um meio para novos tipos de guerra. Muitos países agora fornecem serviços essenciais online, fazendo com que cidadãos sem acesso à TI possam ficar isolados e em desvantagem. Esta dependência coletiva e individual da TI cada

vez mais impõe uma obrigação significativa aos prestadores de serviços de TI de proteger seus sistemas e usuários contra violações intencionais ou acidentais da segurança de dados e de sistemas inteiros. Por esses motivos, a importância do Profissional de Segurança Cibernética não pode ser subestimada.

Um Profissional de Segurança Cibernética trabalha para proteger as redes de sistemas de computadores de uma organização, garantindo sua robustez e impedindo que hackers acessem e/ou roubem informações e dados confidenciais. Esta função normalmente envolve a configuração de firewalls, IPS/IDS, funções/serviços de servidor e soluções de segurança da Web para proteger informações confidenciais. Esses profissionais também monitoram e investigam violações de segurança. Eles podem realizar testes de intrusão simulando ataques a fim de encontrar vulnerabilidades em suas redes antes que essas possam ser exploradas com intenções maliciosas. Suas atividades forenses incluem a coleta, conservação, processamento, análise e apresentação de evidências informáticas para mitigar a vulnerabilidade das redes a atividades criminosas, fraudulentas e outras atividades hostis. Eles adotam uma série de táticas, técnicas e procedimentos, usando uma gama completa de ferramentas e processos investigativos.

Um Profissional de Segurança Cibernética geralmente também apoia os planos de recuperação de desastres das organizações, os quais descrevem os passos e procedimentos para restaurar o funcionamento adequado dos sistemas e redes de TI de uma organização após um desastre ou um ataque. Estes planos são de suma importância, financeiramente, para a reputação e para a continuidade dos serviços essenciais. Normalmente eles incluem medidas preventivas, como backup periódico e transferência de dados para um local externo.

Em um setor em rápida evolução, os Profissionais de Segurança Cibernética precisam estar sempre um passo à frente de possíveis hackers. Eles devem se manter atualizados com as técnicas de ataque mais recentes usadas para se infiltrar em sistemas informáticos, bem como com as novas tecnologias de segurança que podem ajudar as organizações a combater essas ameaças com sistemas e medidas robustos.

1.1.3 Número de Competidores por equipe

A ocupação de Segurança Cibernética é realizada em equipes, com dois competidores por equipe.

1.1.4 Limite de idade dos Competidores

Para a São Paulo Skills, os Competidores não poderão completar 24 anos em 2022

1.2 RELEVÂNCIA E USO DESTE DOCUMENTO

Este documento contém as informações sobre os requisitos exigidos para competir nesta ocupação, bem como os princípios, métodos e procedimentos de avaliação que regem a competição.

Todos os Avaliadores e Competidores deverão conhecer e compreender este Descritivo Técnico.

1.3 DOCUMENTOS RELACIONADOS

Considerando que este Descritivo Técnico contém apenas informações específicas da ocupação, deve ser utilizado juntamente com o Regulamento da Competição, Boletins Técnicos, Lista de Infraestrutura e Recursos Online, conforme indicados neste documento ou definidos pela Coordenação Geral da São Paulo Skills.

2. ESPECIFICAÇÃO DE PADRÕES DA SÃO PAULO SKILLS

2.1 OBSERVAÇÕES GERAIS SOBRE O REGULAMENTO E CÓDIGO DE ÉTICA DA SÃO PAULO SKILLS

O Regulamento e Código de Ética da São Paulos Skills especifica o conhecimento, a compreensão e as ocupações específicas que constituem as boas práticas internacionais no desempenho técnico e profissional. Deve refletir uma compreensão global compartilhada de quais funções ou dos papéis relacionados a este trabalho que representam para o meio industrial e corporativo (SharePoint>SãoPauloSkills).

A competição de ocupações visa a refletir as melhores práticas internacionais conforme descrito pelo Regulamento e Código de Ética da São Paulo Skills, e tanto quanto for possível. A Especificação de Padrões é, portanto, uma diretriz para a preparação e para o treinamento necessários para a competição de ocupações.

Na competição de ocupações, a avaliação do conhecimento e da compreensão ocorrerá através da avaliação de desempenho. Não haverá testes separados de conhecimento e compreensão.

A Especificação de Padrões é dividida em seções distintas com títulos e números de referência.

É atribuída uma porcentagem das notas totais a cada seção para indicar sua importância relativa dentro da Especificação de Padrões. A soma de todas as notas percentuais é 100.

O Esquema de Pontuação e o Projeto Teste avaliarão apenas as ocupações que são descritas na Especificação de Padrões. Eles refletirão a Especificação de Padrões de maneira mais abrangente possível dentro das restrições da Competição de cada Ocupação.

O Esquema de Pontuação e o Projeto Teste seguirão a designação de notas de acordo com a Especificação de Padrões, dentro das limitações possíveis de serem praticadas. Permite-se uma variação de cinco por cento, desde que essa variação não distorça o coeficiente atribuído pela Especificação de Padrões.

Esses padrões são especificados pela São Paulo Skills em conformidade com a World Skills Internacional, ou seja, a São Paulo Skills seguirá os padrões preestabelecidos para a competição na fase internacional.

2.2 ESPECIFICAÇÃO DE PADRÕES DA SÃO PAULO SKILLS

Seção		Importância relativa (%)
1	**Preparação e organização do trabalho**	**5**

	O Competidor deve conhecer e compreender: • A legislação, as obrigações, os regulamentos e a documentação relativas à saúde e segurança • As situações em que o equipamento de proteção individual (EPI) deve ser utilizado, por exemplo, contra descarga eletrostática (ESD) • A importância da integridade e da segurança ao lidar com equipamentos e informações do usuário • A importância da eliminação segura de resíduos para reciclagem • As técnicas de planejamento, programação e priorização • A importância da precisão, conferência e atenção aos detalhes em todas as práticas de trabalho • A importância de práticas de trabalho metódicas	
	O Competidor deve ser capaz de: • Seguir normas, regras e regulamentos relativos à saúde e segurança • Manter um ambiente de trabalho seguro • Identificar e utilizar os Equipamentos de Proteção Individual apropriados contra descarga eletrostática (ESD) • Selecionar, usar, limpar, conservar e armazenar com segurança as ferramentas e equipamentos • Organizar a área de trabalho de modo a maximizar a eficiência e manter uma disciplina de arrumação regular • Trabalhar com eficiência e conferir o progresso e os resultados regularmente • Manter-se atualizado a respeito das licenças profissionais exigidas e mantê-las em dia • Conduzir métodos de pesquisa completos e eficientes para apoiar o crescimento do conhecimento • Tentar proativamente novos métodos, sistemas e abraçar a mudança	
2	**Comunicação e relacionamento interpessoal**	**10**
	O Competidor deve conhecer e compreender: • A importância de ouvir para garantir uma comunicação eficaz • Os papéis e exigências dos colegas e os métodos mais eficazes de comunicação • A importância de construir e manter relações de trabalho produtivas com colegas e superiores • As técnicas para o trabalho em equipe eficaz • As técnicas para resolver mal-entendidos e conflitos de demanda • O processo para controlar a tensão e a raiva para resolver situações difíceis • As exigências para a documentação completa das medidas tomadas nas investigações de segurança cibernética e suas descobertas	
	O Competidor deve ser capaz de: • Empregar habilidades superiores de escuta e questionamento para entender a fundo situações complexas • Assegurar comunicações verbais e escritas consistentemente eficazes com oscolegas • Reconhecer e adaptar-se às mudanças nas necessidades dos colegas • Contribuir proativamente para o desenvolvimento de uma equipe sólida e eficaz	

	• Compartilhar conhecimento e experiência com os colegas e desenvolver uma cultura de aprendizagem de apoio • Controlar a tensão e a raiva e transmitir confiança de que os problemas podem ser resolvidos • Documentar com precisão as medidas tomadas e as descobertas durante as investigações • Garantir o cumprimento estrito das políticas e procedimentos de segurança e operação em sistemas informáticos	
3	**Projeto e criação de sistemas seguros**	**10**
	O Competidor deve conhecer e compreender: • As normas, políticas, requisitos e procedimentos para o gerenciamento de riscos de TI • As ferramentas de avaliação de vulnerabilidade e defesa cibernética e seus recursos. • Sistemas Operacionais • Sistemas de rede • Conceitos de programação de computadores, incluindo linguagens, programação, testes, depuração e tipos de arquivo • Os princípios e métodos de segurança cibernética e privacidade aplicáveis ao desenvolvimento de software O Competidor deve ser capaz de: • Aplicar os princípios de segurança cibernética e privacidade às exigências da organização (referentes à confidencialidade, integridade, disponibilidade, autenticação, não repúdio) ao projetar e documentar os procedimentos de Teste e Avaliação do programa em geral. • Conduzir avaliações abrangentes independentes do gerenciamento, dos controles operacionais e técnicos de segurança, e das melhorias no controle adotados nos sistemas de tecnologia da informação (TI) ou herdados por eles para determinar a eficácia geral dos controles • Desenvolver e conduzir avaliações de sistemas para confirmar a conformidade com as especificações e requisitos • Proteger a interoperabilidade de sistemas ou elementos de sistemas que incorporam TI • Modificar aplicativos de computador, software ou programas utilitários especializados existentes • Analisar a segurança de aplicativos de computador, software ou programas utilitários especializados novos ou existentes, para proporcionar resultados acionáveis • Desenvolver e manter negócios, sistemas e processos de informação para apoiar as necessidades da missão empresarial • Desenvolver regras e requisitos de tecnologia da informação (TI) que descrevam arquiteturas iniciais e de destino • Garantir que os requisitos de segurança das partes interessadas necessários para proteger a missão e os processos da organização sejam adequadamente tratados em todos os aspectos da arquitetura corporativa, incluindo modelos de referência, arquiteturas de segmento e da solução, e os sistemas resultantes que dão suporte a essas missões e processos • Conduzir pesquisas em sistemas de software e de engenharia de software e sistemas para desenvolver novas capacidades, garantindo a integração total da segurança cibernética Conduzir pesquisas (incluindo testes de intrusão) para avaliar possíveis	

	vulnerabilidades nos sistemas do ciberespaço • Consultar as partes interessadas para avaliar os requisitos funcionais e traduzi-los em soluções técnicas • Planejar, preparar e executar testes nos sistemas • Analisar, avaliar e relatar os resultados em relação às especificações e requisitos • Projetar, desenvolver, testar e avaliar a segurança dos sistemas informáticosdurante todo o ciclo de vida de desenvolvimento dos sistemas	
4	**Operação e manutenção seguras dos sistemas**	**15**
	O Competidor deve conhecer e compreender: • Linguagens de consulta, como SQL (linguagem de consulta estruturada) e Sistemas de Banco de Dados • Protocolos de rede, como TCP/IP, Protocolo Dinâmico de Configuração de Host, Sistema de Nomes de Domínio (DNS), e serviços de diretório • Os conceitos e funções de firewall (por exemplo, ponto único de autenticação/auditoria/aplicação de política, varredura de mensagens em busca de conteúdo malicioso, anonimização de dados para conformidade com PCI e PII, verificação da proteção contra perda de dados, segurança SSL e processamento REST/JSON) • Os conceitos de arquitetura de segurança de rede, incluindo topologia, protocolos, componentes e princípios • As técnicas de *hardening* de sistemas operacionais, de rede e de Administração de Sistemas • As políticas de segurança do usuário de tecnologia da informação (TI) organizacional (por exemplo, criação de conta, regras de senha e controle de acesso) • Os princípios e métodos de segurança da tecnologia da informação (TI) • Os métodos de autenticação, autorização e controle de acesso • Os princípios de privacidade e vulnerabilidade da segurança cibernética	
	O Competidor deve ser capaz de: • Instalar, configurar, testar, operar, manter e gerenciar infraestruturas de rede • Gerenciar softwares que permitem o compartilhamento e a transmissão de todos os dados • Instalar, configurar, solucionar e manter as configurações do servidor (hardware e software) para garantir sua privacidade, integridade e disponibilidade • Gerenciar contas quanto ao controle de acesso, senhas, criação de contas e administração • Analisar os sistemas informáticos das organizações e atualizar as soluções informáticas para ajudá-las a operar de forma mais segura, eficiente e eficaz • Desenvolver métodos para monitorar e medir o risco, a conformidade e os esforços de garantia • Conduzir auditorias nos programas de tecnologia da informação (TI), na infraestrutura de rede para otimizá-la continuamente, na segurança cibernética e na assistência para solução de problemas	
5	**Proteção e defesa seguras de sistemas**	**15**

	O Competidor deve conhecer e compreender: ● Os métodos de implementação de sistemas de arquivos ● Como os arquivos do sistema (por exemplo, arquivos de log, arquivos de registro, arquivos de configuração) contém informações relevantes e onde encontrá-los ● Os conceitos de arquitetura de segurança de rede, incluindo topologia, protocolos, componentes e princípios (por exemplo, aplicação de defesa em profundidade) ● Os princípios, métodos e ferramentas de análise padrão do setor e aceitos pela organização para identificar vulnerabilidades ● Investigações de ameaças, notificações, ferramentas de investigação e leis/regulamentos ● As categorias de incidentes e metodologias de tratamento de respostas ● As ferramentas de avaliação de vulnerabilidade e defesa cibernética e seus recursos ● A implementação de contramedidas para os riscos de segurança identificados ● As abordagens de autenticação, autorização e acesso (por exemplo, controlede acesso baseado em função, controle de acesso obrigatório e controle de acesso opcional)	
	O Competidor deve ser capaz de: ● Utilizar as medidas defensivas e informações coletadas de uma série de fontes para identificar, analisar e relatar eventos que ocorrem ou poderão ocorrer dentro da rede visando proteger as informações, os sistemas informáticos e as redes contra ameaças ● Testar, implementar, manter, revisar e administrar a infraestrutura de hardware e software necessária para gerenciar com eficiência a rede e os recursos de informática ● Monitorar a rede para remediar ativamente as atividades não autorizadas ● Responder a crises ou situações urgentes dentro das próprias áreas de especialização para mitigar imediatas e potenciais ameaças ● Usar abordagens de mitigação, preparação e resposta e recuperação, conforme necessário, para evitar ao máximo a perda de vidas, danos à propriedade e violações da segurança da informação. ● Investigar e analisar todas as atividades de resposta pertinentes ● Conduzir avaliações das ameaças e vulnerabilidades ● Determinar desvios aceitáveis das configurações e das políticas locais ou da empresa ● Avaliar o nível de risco e desenvolver e/ou recomendar medidas de mitigação adequadas em situações operacionais e não operacionais Seguir os procedimentos documentados da organização para preparação eresposta a incidentes	
6	**Operações e Gerenciamento**	**20**

	O Competidor deve conhecer e compreender: ● Os agentes de ameaças cibernéticas e seus métodos ● Os métodos e técnicas empregadas para detectar várias atividades de exploração de vulnerabilidades ● Os recursos e repositórios de coleta de informações/inteligência cibernética ● As ameaças e vulnerabilidades cibernéticas ● As noções básicas de segurança de rede (por exemplo, criptografia, firewalls, autenticação, *honeypots*, proteção do perímetro) ● As fontes de disseminação de informações de vulnerabilidade (por exemplo, alertas, avisos, erratas e boletins) ● Quais arquivos do sistema (por exemplo, arquivos de log, arquivos de registro, arquivos de configuração) contém informações relevantes e onde encontrá-los ● A estrutura, a abordagem e a estratégia das ferramentas (por exemplo, *sniffers*, *keyloggers*) e técnicas (por exemplo, obter acesso por *backdoor*, coleta/*exfiltration* de dados, condução de análise de vulnerabilidade de outros sistemas na rede) de exploração de vulnerabilidades ● As táticas internas para antecipar e/ou emular capacidades e ações de ameaça ● As capacidades e ferramentas para operações cibernéticas internas e de parceiros externos ● Desenvolvimento de metas (ou seja, conceitos, papéis, responsabilidades, produtos etc.) ● Artefatos do sistema e casos de uso forense ● Explorações ou ameaças emergentes aplicáveis aos sistemas e softwares instalados ● A importância da preparação para a recuperação em casos de desastres naturais	
	O Competidor deve ser capaz de: ● Identificar e avaliar as capacidades e atividades de cibercriminosos ou serviços de inteligência estrangeiros ● Obter evidências para ajudar a iniciar ou apoiar investigações ou atividades de execução da lei e contra espionagem ● Analisar as informações coletadas para identificar vulnerabilidades e potencial de exploração ● Analisar informações sobre ameaças de várias fontes, disciplinas e agências em toda a comunidade de inteligência ● Sintetizar e colocar as informações de inteligência dentro de um contexto, e obter *insights* sobre as possíveis implicações ● Aplicar o conhecimento atualizado de uma ou mais regiões, países, entidades não estatais e/ou tecnologias ● Aplicar conhecimentos linguísticos, culturais e técnicos para apoiar a coleta de informações, análise e outras atividades de segurança cibernética ● Identificar, preservar e utilizar os artefatos do sistema para análise Executar com sucesso a recuperação de dados e sistemas em caso de perda	
7	**Coleta e análise de informações**	**10**

	O Competidor deve conhecer e compreender: • Identificar e avaliar as capacidades e atividades de cibercriminosos ou serviços de inteligência estrangeiros • Obter evidências para ajudar a iniciar ou apoiar investigações ou atividades de execução da lei e contra espionagem • Analisar as informações coletadas para identificar vulnerabilidades e potencial de exploração • Analisar informações sobre ameaças de várias fontes, disciplinas e agências emtoda a comunidade de inteligência • Sintetizar e colocar as informações de inteligência dentro de um contexto, e obter *insights* sobre as possíveis implicações • Aplicar o conhecimento atualizado de uma ou mais regiões, países, entidades não estatais e/ou tecnologias • Aplicar conhecimentos linguísticos, culturais e técnicos para apoiar a coleta de informações, análise e outras atividades de segurança cibernética • Identificar, preservar e utilizar os artefatos do sistema para análise • Executar com sucesso a recuperação de dados e sistemas em caso de perda	
	O Competidor deve ser capaz de: • Identificar e avaliar as capacidades e atividades de cibercriminosos ou serviços de inteligência estrangeiros • Obter evidências para ajudar a iniciar ou apoiar investigações ou atividades de execução da lei e contra espionagem • Analisar as informações coletadas para identificar vulnerabilidades e potencial de exploração • Analisar informações sobre ameaças de várias fontes, disciplinas e agências emtoda a comunidade de inteligência • Sintetizar e colocar as informações de inteligência dentro de um contexto, e obter *insights* sobre as possíveis implicações • Aplicar o conhecimento atualizado de uma ou mais regiões, países, entidades não estatais e/ou tecnologias • Aplicar conhecimentos linguísticos, culturais e técnicos para apoiar a coleta de informações, análise e outras atividades de segurança cibernética • Identificar, preservar e utilizar os artefatos do sistema para análise • Executar com sucesso a recuperação de dados e sistemas em caso de perda	
8	**Investigação e Computação Forense**	**15**
	O Competidor deve conhecer e compreender: • Investigações de ameaças, notificações, ferramentas de investigação e leis/regulamentos • Os conceitos e as metodologias para análise de *malwares* • Os processos para coleta, embalagem, transporte e armazenamento de provas eletrônicas, mantendo a cadeia de custódia • Os tipos e as formas de coleta de dados persistentes • Os conceitos e as práticas de tratamento de dados forenses digitais • Os tipos de dados forenses digitais e como reconhecê-los • As implicações forenses da estrutura e das operações do sistema operacional • Os impactos operacionais específicos dos lapsos de segurança cibernética	
	O Competidor deve ser capaz de: • Coletar, processar, preservar, analisar e apresentar provas digitais para auxiliar na mitigação da vulnerabilidade da rede e/ou em investigações criminais, de fraude, de contra espionagem ou de aplicação da lei	
	Total	**100**

3. ESPECIFICAÇÃO E ESTRATÉGIA DE AVALIAÇÃO

3.1 ORIENTAÇÕES GERAIS

A avaliação é baseada na Estratégia de Avaliação da São Paulo Skills. A Estratégia define os princípios e as técnicas com as quais as avaliações da São Paulo Skills devem estar de acordo.

A prática de avaliação do Avaliador é o cerne da São Paulo Skills. É por este motivo que está sujeita à análise e ao desenvolvimento profissional contínuo. O crescimento do conhecimento especializado na avaliação informará o uso futuro e a direção dos principais instrumentos de avaliação utilizados pela São Paulo Skills: o Sistema de Classificação, o Projeto de Teste, e o Sistema Informatizado de Competições (CIS).

A avaliação no São Paulo Skills é feita de duas maneiras: medição e julgamento. Para ambos os tipos de avaliação, o uso de referências explícitos para avaliar cada aspecto é essencial para garantir a qualidade.

O Esquema de Avaliação deve seguir os coeficientes de pontuação descritos na Especificação de Padrões. O Projeto Teste é o veículo de avaliação para a competição, e segue a Especificação de Padrões. O CIS possibilita o registro temporal e preciso das pontuações; sua capacidade de detalhamento, suporte e feedback está em contínua expansão.

Em linhas gerais, o Esquema de Avaliação irá liderar o processo do Projeto Teste. Depois disso, o Projeto Teste e o Esquema de Avaliação serão projetados e desenvolvidos através de um processo iterativo a fim de assegurar tanto que se otimizem seus relacionamentos com a Especificação de Padrões quanto com a Estratégia de Avaliação. Eles serão submetidos à Coordenação da competição para aprovação em conjunto, a fim de demonstrar sua qualidade e conformidade com a Especificação de Padrões.

O desenvolvimento do projeto teste deve garantir que todos os requisitos solicitados para serem desenvolvidos pelos competidores possam ser avaliados através do esquema de avaliação desenvolvido. Todos os aspectos descritos no

esquema de avaliação, bem como seus benchmarks, para avaliação devem estar descritos claramente na descrição do projeto teste. Esta correlação é um dos quesitos de qualidade para o desenvolvimento da competição e visa garantir que não exista esforço realizado sem que seja avaliado e nem aspectos de avaliação que estejam avaliando requisitos não descritos aos competidores através do Projeto Teste.

Antes da submissão para aprovação à Coordenação da São Paulo Skills, o Esquema de Avaliação e o Projeto de Teste serão revisados pelos Gestores das Ocupações da Coordenação da São Paulo Skills para se adequar-se às capacidades do CIS.

4. FICHA DE AVALIAÇÃO

4.1 ORIENTAÇÕES GERAIS

Esta seção descreve o papel e o local do Esquema de Avaliação, como os Avaliadores avaliarão o trabalho dos Competidores conforme demonstrado pelo Projeto Teste e os procedimentos e requisitos para a pontuação.

O Esquema de Avaliação é o instrumento fundamental da São Paulo Skills, na medida em que relaciona a avaliação com os padrões que representam a ocupação. Ele é projetado para alocar pontos para cada aspecto de desempenho avaliado de acordo com as ponderações definidas na Especificação de Padrões.

Ao refletir os coeficientes da Especificação de Padrões, o Esquema de Avaliação estabelece os parâmetros para o planejamento do Projeto Teste. Dependendo da natureza da habilidade e suas necessidades de avaliação, inicialmente pode ser apropriado desenvolver o Esquema de Avaliação com mais detalhes como um guia para o Projeto Teste. A partir deste ponto, o Esquema de Avaliação e o Projeto Teste devem ser desenvolvidos em conjunto.

A Seção 2.1 acima indica até que ponto o Esquema de Avaliação e o Projeto Teste podem divergir das pontuações indicadas na Especificação de Padrões, se não houver uma alternativa aplicável.

O Esquema de Avaliação e o Projeto Teste podem ser desenvolvidos externamente por uma ou várias pessoas, ou por todos os avaliadores. O projeto detalhado e a versão final do esquema de avaliação projetado externamente

devem ser aprovados por todos os avaliadores antes da submissão para garantia de qualidade, salvo os casos em que o Projeto Teste é projeto para ser uma prova surpresa. Nesse caso, a pessoa externa deve receber modelos de prova para que a concepção do Projeto Teste siga um padrão de qualidade. Alternativamente, é possível que a validação do Projeto Teste realizado por pessoa externa seja feita por algum profissional capacitado, desde que ela não participe do treinamento de nenhum envolvido no processo.

Além disso, os avaliadores são encorajados a enviar seus Esquemas de Avaliação e Projetos Teste para comentários e aprovação provisória antes de sua conclusão, a fim de evitar decepções ou contratempos em uma fase tardia. Também são aconselhados a trabalhar com os supervisores da ocupação nesta fase intermediária, a fim de aproveitar ao máximo as possibilidades do CIS.

Em todos os casos, o Esquema de Avaliação completo e aprovado deve ser inserido no CIS pelo menos oito semanas antes da Competição usando a planilha padrão do CIS ou outros métodos acordados. O Supervisor da Ocupação é o responsável por esse processo.

4.2 CRITÉRIOS DE AVALIAÇÃO

As principais sessões do Esquema de Avaliação são os Critérios de Avaliação. Essas sessões são criadas em conjunto com o Projeto Teste. Em algumas ocupações, os Critérios de Avaliação podem ser semelhantes aos cabeçalhos da seção na Especificação de Padrões; em outros, eles podem ser totalmente diferentes. Normalmente haverá entre cinco e nove critérios de avaliação, o Esquema de Avaliação deve refletir os coeficientes de pontuação da Especificação de Padrões.

Os critérios de avaliação são criados pelas pessoas que desenvolvem o Esquema de Avaliação, que são livres para definir critérios que considerem mais adequados para a avaliação e pontuação do Projeto Teste. Cada critério de avaliação é definido por uma letra (de A a M).

O Formulário de Resumo gerado pelo CIS compreenderá uma lista dos Critérios de Avaliação.

As pontuações atribuídas a cada critério serão calculadas pelo CIS. Esta será a soma cumulativa das pontuações atribuídas a cada aspecto dentro desse Critério de Avaliação.

4.3 SUBCRITÉRIOS

Cada Critério de Avaliação é dividido em um ou mais Subcritérios. Cada Subcritério se torna o título para um formulário de avaliação na São Paulo Skills.

Cada formulário de avaliação (Subcritério) possui uma data específica na qual será pontuada.

Cada formulário de avaliação (Subcritério) contém Aspectos a serem avaliados e pontuados por medição ou julgamento. Alguns Subcritérios possuem tanto Aspectos avaliados por medição, quanto por julgamento, caso em que há um formulário de avaliação para cada um desses aspectos

4.4 ASPECTOS

Cada Aspecto define, em detalhes, um único item a ser avaliado e pontuado juntamente com as pontuações, ou instruções sobre como as pontuações devem ser atribuídas. Os aspectos são avaliados por medição ou julgamento e aparecem no formulário de avaliação apropriado.

O formulário de avaliação lista, em detalhes, todos os Aspectos a serem avaliados juntamente com a pontuação atribuída a ele e uma referência à seção da habilidade conforme estabelecido na Especificação de Padrões.

A soma das pontuações atribuídas a cada Aspecto deve estar dentro do limite de pontuações especificadas na seção de Especificação de Padrões da ocupação. Essa informação será exibida na Tabela de Atribuição de Pontuações do CIS quando o Esquema de Avaliação for revisado.

É importante lembrar que avaliação deve ter entre 75 e 200 aspectos e a pontuação máxima que pode ser atribuída para cada aspecto é de 2 pontos.

4.5 AVALIÇÃO E PONTUAÇÃO USANDO JULGAMENTO

O julgamento usa uma escala de 0-3. Para aplicar a escala com rigor e consistência, o julgamento deve ser conduzido usando:

- Referências (critérios) para obter orientação detalhada para cada Aspecto (em palavras, imagens, artefatos ou notas de orientação separadas)
- A Escala de 0-3:
    - 0: desempenho não atende ao padrão da indústria
    - 1: desempenho atende parcialmente ao padrão da indústria
    - 2: o desempenho atende ao padrão da indústria
    - 3: desempenho excede positivamente as expectativas da indústria

Desejavelmente, três Avaliadores irão julgar cada Aspecto com um quarto atuando como juiz quando for necessário para evitar avaliação de competidor da própria unidade do avaliador. Exceções a essa regra podem ser aplicadas quando o contingente não permitir.

4.6 AVALIAÇÃO E PONTUAÇÃO USANDO MEDIÇÃO

Serão necessários pelo menos três avaliadores para julgar cada aspecto. Exceto se afirmado em contrário, serão atribuídas apenas a nota máxima e zero. Nos casos em que forem utilizadas, as notas parciais serão definidas claramente dentro do Aspecto.

4.7 O USO DE AVALIAÇÃO POR MEDIÇÃO E JULGAMENTO

As decisões relativas à seleção de critérios e métodos de avaliação serão feitas durante a concepção da competição através do Esquema de Avaliação e Projeto Teste. Os avaliadores podem definir previamente, por meio de registro no fórum da competição, um número desejável de critérios de julgamento por Projeto Teste.

4.8 CONCLUSÃO DA ESPECIFICAÇÃO DE AVALIAÇÃO DA OCUPAÇÃO

A avaliação dos Projetos Testes será feita de maneira transparente e de acordo com o regulamento da competição. Detalhes poderão ser definidos em comum

acordo entre os avaliadores e formalizados através do fórum de discussões da São Paulo Skills.

4.9 PROCEDIMENTO DE AVALIAÇÃO DA OCUPAÇÃO

Todos os Avaliadores devem ser designados para uma equipe de avaliação dos módulos. O trabalho do Competidor não pode ser alterado de forma alguma para facilitar a avaliação, a menos que tal alteração esteja incluída na Ficha de Avaliação.

Os Avaliadores da Competição são divididos em grupos menores dentro das suas equipes de avaliação, que ficarão a cargo de avaliar cada seção específica dos critérios de avaliação. A avaliação de todas as seções da Competição é feita progressivamente.

A avaliação de cada módulo deverá ser concluída no mesmo dia da aplicação da prova, para que a pontuação seja atribuída progressivamente.

Ficha de Avaliação:

- Cada Competidor recebe o Formulário de Resumo da Avaliação com os pontos a serem avaliados
- A Ficha de Avaliação completa só será disponibilizado aos Avaliadores, pois ela contém as respostas para cada um dos desafios; a Ficha de Avaliação completa daria as respostas ao Competidor. A Ficha de Avaliação só será entregue aos avaliadores após o início do módulo em questão.
- Para o Módulo C os avaliadores não terão acesso a ficha CIS caso a prova seja desenvolvida por uma pessoa externa e/ou empresa especializada.
-

5. PROJETO TESTE

5.1 OBSERVAÇÕES GERAIS

As seções 3 e 4 regem o desenvolvimento do Projeto Teste. Estas observações pretendem apenas complementar as informações.

Seja na forma de um projeto único ou de uma série de módulos independentes ou conectados, o Projeto Teste permitirá avaliar o conhecimento aplicado, as competências e os comportamentos definidos em cada seção do Regulamento e Código de Ética da São Paulo Skills.

O objetivo do Projeto Teste é fornecer oportunidades completas, equilibradas e autênticas de avaliação e pontuação dos Requisitos, juntamente com a Ficha de Avaliação. A relação entre o Projeto Teste, a Ficha de Avaliação e os Padrões será um indicador chave da qualidade, assim como sua relação com o desempenho real na prática.

O Projeto Teste não abrangerá áreas que não estão definidas nos Padrões, nem afetará o equilíbrio das notas dentro dos Padrões, exceto nos casos indicados na Seção 2. O presente Descritivo Técnico indicará quaisquer questões que afetem a capacidade do Projeto Teste de suportar toda a gama de avaliação definida nos Padrões.

O Projeto Teste permitirá a avaliação do conhecimento e da compreensão exclusivamente por meio de suas aplicações no trabalho prático. O Projeto Teste não avaliará o conhecimento das regras e regulamentos da São Paulo Skills.

As informações fornecidas abaixo estarão sujeitas ao conhecimento disponível no momento da elaboração deste Descritivo Técnico e à exigência de confidencialidade.

Consulte a versão mais recente do Regulamento da Competição para mais detalhes.

5.2 FORMATO/ESTRUTURA DO PROJETO TESTE

O Projeto Teste será realizado em três módulos e exigirá que os competidores lidem com práticas de segurança em redes, software e aplicativos, realizem respostas a incidentes de forense digital e efetuem testes de invasão em servidores Linux e Windows, empregando técnicas de Red Team, de modo a atender as demandas da indústria na área de Segurança Cibernética.

O Projeto Teste apresentará um cenário que demandará que o competidor implemente segurança em uma infraestrutura virtualizada, controle o acesso de usuários a recursos, gerencie sistemas de informação e serviços e realize a proteção de ambientes contra roubo, modificação e destruição de dados, visando garantir a Confidencialidade, Integridade e Disponibilidade. Os competidores também desempenharão atividades relacionadas à investigação de incidentes de segurança da informação, análise e revisão de códigos programação a fim de encontrar trechos vulneráveis a ataques e realizar engenharia reversa em códigos maliciosos a fim de performar análise de malware, identificando possíveis riscos para usuários e ambientes corporativos.

O Projeto Teste será dividido em três módulos a serem realizados em um período de 3 (três) dias de provas

- Módulo A - *Hardening*: Segurança de infraestrutura corporativa (dia 1) – **30 pontos**
- Módulo B - Forense: Resposta a incidentes de segurança cibernética, investigações forenses digitais e segurança de aplicativos (dia 2); - **30 pontos**
- Módulo C - CTF: Desafio de captura da bandeira (dia 3). – **40 pontos**

Somados, os três módulos da prova resultarão em 100 pontos, pontuação máxima para a ocupação de Segurança Cibernética. O módulo A e o módulo B valerão 30 pontos cada, enquanto o módulo C terá uma pontuação máxima de 40 pontos.

5.3 REQUISITOS DO PROJETO TESTE

Cada módulo do Projeto Teste deve ser:

- Confeccionado para que o competidor possa completar;
- Projetado usando uma folha de rosto padrão para cada modelo disponível no site da seletiva;
- Autoexplicativo.
- Realizado em dupla. A forma de gerenciamento e distribuição das atividades entre os integrantes de cada equipe faz parte da estratégia dos competidores.

Módulo A

Contextualização

Esse é um módulo dedicado à implementação de segurança de infraestrutura corporativa. Nessa etapa, o Competidor deve ser capaz de configurar serviços em servidores Linux CentOS e Windows Server de modo a reduzir as chances de ataque e exploração de falhas por um possível invasor mal intencionado.

O Competidor deve mostrar domínio sobre os principais serviços oferecidos por cada um desses sistemas operacionais, sendo capaz de operá-los de acordo com as diretrizes definidas pelo Projeto Teste. É esperado que o Competidor também tenha domínio sobre *routing* e *switching*, já que a configuração de ativos de rede será necessária para que as conexões entre os servidores e clientes sejam feitas de maneira segura. Nesse módulo, a configuração de firewalls, criação de VPNs de acesso remoto e instalação software de criptografia de dados para proteger informações confidenciais são exemplos de tarefas a serem executadas. É, ainda, esperado que as equipes demonstrem habilidades de monitoramento de rede em busca de violações de segurança, utilizando softwares de IDS/IPS e SIEM, investigando quando as falhas acontecerem.

Os conhecimentos dos Competidores serão avaliados através dos Projetos Testes. Os participantes devem demonstrar:

• Conhecimento dos requisitos e recursos de comunicação de dispositivos de rede;

• Conhecimento de possíveis vulnerabilidades de dispositivos e softwares;

• Conhecimento de controles de contas de acesso a sistemas;

• Conhecimento das opções para limitar o acesso à rede local e aos dispositivos (por exemplo, usando senhas seguras);

• Conhecimento de instalação e configuração de dispositivos de segurança necessários relacionadas à segurança cibernética (roteador, firewall, servidor proxy);

• Conhecimento de análise e, se necessário, melhoria de medidas de segurança em relação à atualização.

O Projeto Teste será realizado em um cenário emulado disponibilizado a cada uma das duplas, não sendo necessário que os competidores lidem com configuração de recursos físicos. A emulação de todos os servidores, clientes, ativos e passivos de rede será realizada por softwares como PNETLab, EVE-NG e VMWare.

O Projeto Teste desse módulo deve vir acompanhado de detalhes da configuração do cenário, dispondo de uma imagem detalhada que descreva as topologias física e lógica, quando aplicável.

Requisitos para o Projeto Teste

Caso a prova seja preparada pelos Avaliadores ela deve seguir uma série de requisitos para que seja considerada válida. Para isso, ela deve conter uma quantidade mínima de equipamentos configuráveis. Sendo eles:

- 2 servidores Linux CentOS 7, provendo serviços para o cenário;
- 2 servidores Windows Server 2016, provendo serviços para o cenário;
- 1 firewall Cisco ASA;
- 1 roteador Cisco;
- 2 Switches Cisco gerenciáveis com aplicação de configurações de segurança;
- 2 computadores clientes (Windows ou Linux) que consumirão serviços dos servidores/ativos de rede ou serão utilizados para testes;
- No mínimo duas etapas discursivas para listagem de medidas de *hardening;*
- No mínimo uma VPN (*anyconnect* ou site-to-site).

A prova deverá possuir um nível compatível com a competição. Provas com níveis acima ou abaixo da média esperada estarão sujeitas à desclassificação.

Todos os equipamentos listados acima devem possuir itens para configuração. Todos os itens devem possuir motivos claros e sensatos para serem incluídos no cenário. Caso o Projeto Teste não estabeleça nenhuma configuração para o equipamento, este não será considerado.

Elaboração do Projeto Teste

A elaboração dos Projetos Teste deve ser baseada em versões anteriores de Projetos Testes da Seletiva Nacional ou São Paulo Skills.

Os Projetos Teste serão definidos por meio de sorteio. Apenas provas que tenham sido aplicadas em competições oficiais poderão participar do sorteio para Definição do Projeto a ser aplicado na São Paulo Skills.

Os Projetos classificados serão postados no Fórum pelo Avaliador Líder 5 meses antes da competição. Qualquer Avaliador pode apresentar Projetos Teste ao Avaliador Líder para que eles sejam incluídos no sorteio, desde que eles se enquadrem em algum das condições abaixo.

Serão aceitos como propostas:

- Provas oficiais de Competições Nacionais;
- Propostas de prova de Competições Nacionais (desde que tenham sido validades);
- Provas de Competições Internacionais;
- Pré-projetos de Competições Internacionais.

Será necessário, no mínimo, a apresentação de 3 projetos para que o sorteio aconteça.

2 meses antes da competição as provas passarão por ajustes e alterações para que os módulos sejam adaptados à competição (caso haja necessidade) e se enquadrem às diretrizes da Skills. Os Avaliadores se reunirão para discutir as adaptações. A reunião poderá acontecer presencial ou remotamente, desde que os Projetos Teste modificados sejam formalizados via fórum da competição

O sorteio do Projeto Teste será realizado no dia da ambientação (C-1)

Deve-se divulgar uma lista de infraestrutura e todas as propostas devem ser concebidas de forma a serem exequíveis a partir da utilização dessa lista e sua respectiva quantidade de materiais.

A lista de infraestrutura precisará ser adaptada para que se adeque aos requisitos dos Projetos Teste selecionados. As imagens dos Sistemas Operacionais que serão emulados precisam ter todos os softwares e pacotes necessários para a execução da prova devidamente instalados. A adequação das imagens dos

Sistemas Operacionais deve ser realizada com antecedência para que elas sejam disponibilizadas ao Chefe de Oficina para a preparação do ambiente. Na semana da competição, as imagens já devem estar prontas.

Cada Projeto Teste deverá ser acompanhado por uma ficha de avaliação com as pontuações correspondentes aos critérios a serem avaliados, tal como consta no Descritivo Técnico, bem como por uma lista detalhada dos Aspectos e Subcritérios definidos nos Formulários de Avaliação Objetiva e de Julgamento. **Apenas serão aceitas propostas de prova que estiveram acompanhados de ficha de avaliação (CIS) devidamente preenchidas. É importante que a ficha de avaliação contenha um roteiro de correção para cada um dos aspectos.** O CIS das propostas poderão ser modificados no C-1.

No dia de ambientação (C-1) as provas com propostas de alteração válidas serão sorteadas; a proposta selecionada no sorteio será aplicada na competição oficial da São Paulo Skills. Apenas as provas que já tiverem sido aprovadas pelo Avaliador Líder e adaptadas 2 meses antes da competição estarão aptas para aplicação na competição. Os Projetos Teste originais não poderão ser aplicados sem as adaptações necessárias.

A pontuação total desse módulo é de 30 pontos.

Módulo B

O Módulo B apresenta aos competidores cenários de forense digital. Nesse módulo, é função das Equipes analisar os cenários propostos e elaborar uma proposta de intervenção a partir da investigação de incidentes de segurança, revisão de códigos inseguros, análise de malware através de exploração de arquivos binários e identificação de comportamentos mal intencionados de software.

O Módulo B é dividido em 4 tarefas, também conhecidas como *tasks*. Cada *task* apresenta um cenário com análises forenses que envolvem habilidades reais demandadas no mercado de trabalho de segurança cibernética. As *tasks* são divididas da seguinte maneira:

Task 1: Reposta à Incidentes

Nessa task os competidores devem abordar e gerenciar as consequências de uma violação de segurança ou ataque cibernético, também conhecido como incidente de TI, incidente de computador ou incidente de segurança. O objetivo é lidar com a situação de uma forma que limite os danos e reduza o tempo e os custos de recuperação. Geralmente, o competidor deverá acessar alguma máquina comprometida por um ataque, identificar o invasor e forma de acesso e reparar os danos ocasionados no cenário.

Task 2: Detecção e Reparo de Vulnerabilidades

Nessa tarefa, é esperado que a equipe seja responsável por detectar uma vulnerabilidade em um servidor (geralmente servidor Linux) e corrigi-la. O competidor precisará descrever como a vulnerabilidade funciona e quais as ameaças que ela oferece, apresentando formas de mitiga-la.

Task 3: Investigação Forense Digital

O Forense Digital é um ramo da Segurança que se concentra em identificar, adquirir, processar, analisar e relatar dados armazenados eletronicamente.

A evidência eletrônica é um componente de quase todas as atividades criminosas e o suporte forense digital é crucial para as investigações policiais. O principal objetivo da perícia digital é extrair dados da evidência eletrônica, processá-los em inteligência acionável e apresentar as descobertas para acusação. Todos os processos utilizam técnicas forenses sólidas para garantir que as descobertas sejam admissíveis no tribunal.

Para esse módulo, um projeto teste pode apresentar logs de acesso em sistemas, capturas de tráfego de rede, imagens de disco ou memória e solicitar que os competidores relatem o ocorrido a partir do uso de ferramentas especializadas.

Task 4: Code Review

Uma revisão de código, conhecida por code review, é uma tarefa especializada que envolve revisão manual e/ou automatizada do código-fonte de um aplicativo na tentativa de identificar pontos fracos (falhas) relacionados à segurança no código. Uma revisão de código segura não tenta identificar todos os problemas no código, mas procura fornecer informações sobre quais tipos de problemas existem

e ajudar os desenvolvedores do aplicativo a entender quais classes de problemas estão presentes

Essa tarefa deve possuir, no mínimo, 4 códigos vulneráveis e solicitar que a equipe de Competidores identifique a falha, discorra sobre os potenciais danos que ela pode ocasionar e mostre soluções viáveis para corrigi-la utilizando linguagens de programação de alto ou baixo nível. Para essa task, é indicada a utilização de códigos em PHP ou Linguagem C.

O Módulo B tem uma pontuação máxima de 30 pontos. A pontuação deve ser distribuída igualmente entre as tasks. Logo, cada task, possuirá um valor de 7,5 pontos.

O Módulo B será definido por meio de sorteio. Os objetos do sorteio serão desafios de edições nacionais ou internacionais anteriores, ou ainda outros desafios, desde que sigam padrões de competições mundiais.

O sorteio ocorrerá por tasks. Os detalhes, datas e diretrizes do sorteio serão definidos em conjunto com os Avaliadores e, posteriormente, formalizados pelo fórum da competição.

2 meses antes da competição as provas passarão por ajustes e alterações para que os módulos sejam adaptados à competição (caso haja necessidade) e se enquadrem às diretrizes da SPSkills. Os Avaliadores se reunirão para discutir as adaptações. A reunião poderá acontecer presencial ou remotamente, desde que os Projetos Teste modificados sejam formalizados via fórum da competição

Para que a proposta de uma task seja considerada válida, ela deve ser possível de ser resolvida com as ferramentas disponíveis na lista de infraestrutura, estar acompanhada do CIS, possuir um passo a passo de resolução e conter todos os arquivos necessários para o seu desenvolvimento. Cada Projeto Teste deverá ser acompanhado por uma ficha de avaliação com as pontuações correspondentes aos critérios a serem avaliados, tal como consta no Descritivo Técnico, bem como por uma lista detalhada dos Aspectos e Subcritérios definidos nos Formulários de Avaliação Objetiva e de Julgamento. **Apenas serão aceitas propostas de prova que estiveram acompanhados de ficha de avaliação (CIS) devidamente preenchidas. É importante que a ficha de avaliação contenha um roteiro de correção para cada um dos aspectos.** O CIS das propostas poderão ser modificados no C-1.

No dia de ambientação (C-1) as provas com propostas de alteração válidas serão sorteadas; a proposta selecionada no sorteio será aplicada na competição oficial da São Paulo Skills. Apenas as provas que já tiverem sido aprovadas pelo Avaliador Líder e adaptadas 2 meses antes da competição estarão aptas para aplicação na competição. Os Projetos Teste originais não poderão ser aplicados sem as adaptações necessárias.

Módulo C

O módulo C adota o formato de Capture The Flag, ou CTF. CTFs são exercícios para testar habilidades de segurança ofensiva. O objetivo de CTFs é encontrar o maior número de flags (bandeiras) a partir do uso de técnicas de invasão em servidores, páginas web, banco de dados, hashes criptográficos, etc. Flags são pequenos trechos de códigos escondidos em programas, sites ou servidores que são vulneráveis propositalmente.

CTFs são ferramentas eficazes para avaliar o nível de habilidade de segurança cibernética e para ensinar novas habilidades em um cenário gamificado. Os criadores de CTF podem projetar as competições para testar uma variedade de habilidades em qualquer nível. Por exemplo, alguns CTFs podem se concentrar em testes de penetração e definir desafios testando as habilidades ofensivas de segurança cibernética dos participantes. Outros CTFs podem ser projetados para testar recursos ofensivos e defensivos com equipes tentando violar as redes uns dos outros e proteger suas próprias contra ataques. Os CTFs também podem ter focos mais específicos, testando habilidades em engenharia reversa, análise de tráfego de rede ou outros subcampos da segurança cibernética.

Na São Paulo Skills, os CTFs devem ser construídos de tal forma que abordem as os seguintes assuntos de segurança ofensiva:

- Enumeração
- Ataques Web
- Ataques a Banco de Dados
- Acesso Root
- Criptografia
- Esteganografia

Na competição, o CTF será uma prova surpresa a ser elaborada por pessoa ou empresa neutra. 5 meses antes da competição, o nome da pessoa responsável

pela criação do CTF deve ser divulgado e esta não pode mais ser envolvida na preparação dos competidores, sob pena de desclassificação do competidor.

O CTF deve conter no mínimo 15 flags em níveis variáveis. O modelo do CTF pode ser definido em consenso pelos avaliadores, desde que seja devidamente registrado no fórum da competição.

A pontuação total desse módulo é de 40 pontos.

Duração dos módulos

Os módulos devem ser realizados em 3 dias. Apenas 1 módulo pode ser aplicado por dia. A duração das provas de cada um dos módulos são as seguintes:

- Módulo A: 5 horas de duração (dia C1)
- Módulo B: 5 horas de duração (dia C2)
- Módulo C: 6 horas de duração (dia C3)

Antes de cada um dos módulos, os competidores poderão dispor de 15 minutos, não inclusos no tempo de competição, para estuda-lo e realizar perguntas e esclarecimentos de dúvidas (não relativas a soluções do projeto). Aos Competidores serão dados os documentos, o material explicativo e os Formulários de Avaliação Resumo.

Antes dos módulos acontecerem haverá um dia dedicado para ambientação/familiarização dos competidores com seus postos de trabalhos com a finalidade de testagem do cenário (dia C-1). A ambientação deve durar 5 horas. Nesse dia, caso sejam encontrados problemas de infraestrutura, esses precisarão ser sanados de maneira a garantir as mesmas condições dos postos de trabalho para todos os competidores.

As correções dos Projetos Teste serão feitas pelos avaliadores no mesmo dia da execução de cada módulo. A correção será iniciada após a finalização do tempo de prova.

Um dia após a execução de todos os módulos haverá mais dia com períodos dedicados a realização de possíveis ajustes finais, compartilhamento de documentos, desmontagem dos postos de trabalho e cerimônia de encerramento.

A duração dos módulos pode sofrer alterações, desde que acordado entre todos os avaliadores e registrado formalmente em fórum.

5.4 DESENVOLVIMENTO DO PROJETO TESTE

O Projeto Teste DEVE ser submetido usando os modelos fornecidos pela São Paulo Skills. Use o modelo do Word para documentos de texto e o modelo DWG para desenhos.

5.4.1 Quem desenvolve o Projeto Teste ou os módulos

Os módulos A e B serão definidos por sorteio de provas aplicadas em edições nacionais ou internacionais. O Módulo C é um módulo surpresa e deverá ser realizado por pessoa ou empresa neutra. Os detalhes dos requisitos do processo de desenvolvimento e sorteio dos projetos podem ser encontrados na seção 5.3 (Requisitos do Projeto Teste)

5.4.2 Como e onde o Projeto Teste e os módulos são desenvolvidos

A ocupação de Segurança Cibernética possui três módulos: A, B e C. As propostas base dos módulos A e B serão sorteadas entre provas escolhidas previamente, desde que tenham sido aplicadas em edições nacionais ou internacionais e sofrido as adaptações necessárias para aplicação na São Paulo Skills. Para cada task, serão sorteadas propostas; a proposta vencedora do sorteio será a escolhida para a task em questão. O módulo C é um módulo surpresa e deverá ser realizado por pessoa ou empresa neutra. A seguir, são mostrados mais detalhes sobre a elaboração das propostas:

Módulo A

O Módulo A será definido por sorteio de provas oficiais anteriores, apresentadas no fórum da competição 5 meses antes da competição. As provas oficiais sofrerão alterações para que elas se adequem à lista de infraestrutura ou aos moldes da competição da São Paulo Skills. As propostas candidatas ao sorteio devem ser postadas em Fórum pelo menos 5 meses antes da São Paulo Skills.

2 meses antes da competição as provas passarão por ajustes e alterações para que os módulos sejam adaptados à competição (caso haja necessidade) e se enquadrem às diretrizes da São Paulo Skills. Os Avaliadores se reunirão para

discutir as adaptações. A reunião poderá acontecer presencial ou remotamente, desde que os Projetos Teste modificados sejam formalizados via fórum da competição

A elaboração dos Projetos Testes deve ser baseada em versões anteriores de Projetos Testes da São Paulo Skills, Seletiva Nacional ou São Paulo Skills. Deve-se divulgar uma lista de infraestrutura e todas as propostas devem ser concebidas de forma a serem exequíveis a partir da utilização dessa lista e sua respectiva quantidade de materiais. A lista de infraestrutura precisará ser adaptada para que se adeque aos requisitos dos Projetos Teste selecionados. As imagens dos Sistemas Operacionais que serão emulados precisam ter todos os softwares e pacotes necessários para a execução da prova devidamente instalado. A adequação das imagens dos Sistemas Operacionais deve ser realizada com antecedência para que elas sejam disponibilizadas ao Chefe de Oficina para a preparação do ambiente. As imagens já devem estar prontas na semana da competição. Cada Projeto Teste deverá ser acompanhado por uma ficha de avaliação com as pontuações correspondentes aos critérios a serem avaliados, tal como consta no Descritivo Técnico, bem como por uma lista detalhada dos Aspectos e Subcritérios definidos nos Formulários de Avaliação Objetiva e de Julgamento. **Apenas serão aceitas propostas de prova que estiveram acompanhados de ficha de avaliação (CIS) devidamente preenchidas. É importante que a ficha de avaliação contenha um roteiro de correção para cada um dos aspectos.** O CIS das propostas poderão ser modificados no C-1.

No dia de ambientação (C-1) as provas com propostas serão sorteadas; a proposta selecionada no sorteio será aplicada na competição oficial da São Paulo Skills.

Módulo B

De maneira semelhante ao Módulo A, a criação das propostas do Módulo B será feita por meio de sorteio. Os objetos do sorteio serão desafios de edições nacionais ou internacionais anteriores, ou ainda outros desafios, desde que sigam padrões de competições mundiais. O sorteio ocorrerá por tasks. Os detalhes, datas e diretrizes do sorteio serão definidos em conjunto com os Avaliadores e, posteriormente, formalizados no fórum da competição.

2 meses antes da competição as provas passarão por ajustes e alterações para que os módulos sejam adaptados à competição (caso haja necessidade) e se

enquadrem às diretrizes da São Paulo Skills. Os Avaliadores se reunirão para discutir as adaptações. A reunião poderá acontecer presencial ou remotamente, desde que os Projetos Teste modificados sejam formalizados via fórum da competição

Para que a proposta de uma task seja considerada válida, ela deve ser possível de ser resolvida com as ferramentas disponíveis na lista de infraestrutura, estar acompanhada do CIS, possuir um passo a passo de resolução e conter todos os arquivos necessários para o seu desenvolvimento. Cada Projeto Teste deverá ser acompanhado por uma ficha de avaliação com as pontuações correspondentes aos critérios a serem avaliados, tal como consta no Descritivo Técnico, bem como por uma lista detalhada dos Aspectos e Subcritérios definidos nos Formulários de Avaliação Objetiva e de Julgamento. **Apenas serão aceitas propostas de prova que estiveram acompanhados de ficha de avaliação (CIS) devidamente preenchidas. É importante que a ficha de avaliação contenha um roteiro de correção para cada um dos aspectos.** O CIS das propostas poderão ser modificados no C-1.

Módulo C

Na competição, o CTF será uma prova surpresa a ser elaborada por pessoa ou empresa neutra. 4 meses antes da competição, o nome da pessoa responsável pela criação do CTF deve ser divulgado e esta não pode mais ser envolvida na preparação dos competidores, sob pena de desclassificação do competidor.

O CTF deve conter no mínimo 15 flags em níveis variáveis. O modelo do CTF pode ser definido em consenso pelos avaliadores, desde que seja devidamente registrado no fórum da competição.

5.4.3 Quando o Projeto Teste é desenvolvido

Para o Módulo A e B, as propostas que participarão do sorteio devem ser postadas no fórum oficial 5 meses antes da competição. Os demais módulos devem estar prontos até 2 dias antes da competição. Projetos que sejam desenvolvidos após essa data não poderão ser considerados.

5.5 VALIDAÇÃO DO PROJETO TESTE

O Projeto Teste do Módulos A e B será validado pela equipe de avaliadores. Para o Módulo C, um modelo da prova deve ser fornecido, bem como toda a documentação necessária para ser examinada de modo que a pessoa/empresa externa adeque o Projeto Teste às habilidades descritas no Descritivo Técnico.

5.6 SELEÇÃO DO PROJETO TESTE

A seleção para os Módulos A e B será feita a partir de sorteios. O Módulo C será realizado por empresa externa.

5.7 CIRCULAÇÃO DO PROJETO TESTE

Para os módulos A e B, as provas anteriores serão postadas no fórum 5 meses antes da competição e passarão por adaptações 2 meses antes da competição. A proposta de modificação e as tasks do Módulo B serão divulgados tão logo seja feito o sorteio, antes da competição (dia C-1).

5.8 COORDENAÇÃO DO PROJETO TESTE (PREPARAÇÃO PARA A COMPETIÇÃO)

O Projeto Teste é coordenado pelo Avaliador Líder, Avaliador Adjunto e Organização da São Paulo Skills.

5.9 MUDANÇAS DO PROJETO TESTE DA COMPETIÇÃO

Após a divulgação do projeto teste para todos os participantes, caso seja necessário realizar ajustes ou modificações antes do início da competição, essas serão divulgadas através de Boletim Técnico.

5.10 MUDANÇAS DO PROJETO TESTE DA COMPETIÇÃO

A lista de infraestrutura necessária para permitir que o Competidor conclua o Projeto Teste está disponível no fórum da competição.

Não serão fornecidas ferramentas ou instrumentos aos competidores além dos especificados na lista de infraestrutura, salvo quando é de uso comum/compartilhado e acordado previamente entre os avaliadores.

6. COMUNICAÇÃO E GERENCIAMENTO DA OCUPAÇÃO

6.1 FÓRUM DE DISCUSSÃO

Antes da competição, toda a discussão, comunicação, colaboração e tomada de decisão sobre a competição deve ocorrer no Fórum fornecido pela organização

(https://sesisenaisp.sharepoint.com/sites/senaispskills). As decisões relacionadas com a ocupação só serão válidas se ocorrerem no fórum. O avaliador líder será o moderador deste fórum.

6.2 INFORMAÇÕES DO COMPETIDOR

Todas as informações para os Competidores devem ser fornecidas pelo seu avaliador cadastrado e estarão disponíveis no site da São Paulo Skills (https://sesisenaisp.sharepoint.com/sites/senaispskills).

- Essas informações incluem:
- Regras da Competição
- Descritivos Técnicos
- Esquema de Pontuação
- Projetos teste
- Lista de infraestrutura
- Outras Informações relacionadas à Competição

6.3 GERENCIAMENTO DIÁRIO

O gerenciamento diário da ocupação durante a Competição é definido no Plano de Gerenciamento da Ocupação que é criado pela Equipe de Gerenciamento da Ocupação liderada pelo Gestor. A Equipe de Gerenciamento da Ocupação é composta pelo Gestor e pelo Avaliador Líder. O Plano de Gerenciamento da Ocupação é desenvolvido progressivamente nos meses antes da Competição e é finalizado na Competição por acordo com os Avaliadores.

7. REQUISITOS DE SEGURANÇA ESPECÍFICOS DA OCUPAÇÃO

Consulte a Política e Regulamentação de Saúde, Segurança e Meio Ambiente locais para mais informações sobre a legislação regional.

Tarefa	Calçados resistentes totalmente fechados
EPI geral para áreas seguras	√
Todos os processos na estação de trabalho	√

8. MATERIAIS E EQUIPAMENTOS

8.1 LISTA DE INFRAESTRUTURA

A lista de infraestrutura detalha todos os equipamentos, materiais e instalações fornecidos pelo organizador da competição.

A Lista de infraestrutura está disponível em https://sesisenaisp.sharepoint.com/sites/senaispskills

A Lista de Infraestrutura especifica os itens e quantidades solicitados pelos Avaliadores para a próxima Competição. O organizador da competição atualizará progressivamente a lista de infraestrutura, especificando a quantidade, tipo, marca e modelo reais dos itens. Os itens fornecidos pelo organizador da competição são mostrados em uma coluna separada.

Em cada Competição, os Avaliadores devem revisar e atualizar a Lista de Infraestrutura em preparação para a próxima Competição. Os Avaliadores devem aconselhar o Diretor de Competições da Ocupação sobre qualquer aumento de espaço e / ou equipamento.

Não será permitido o uso de itens diferentes do que foi especificado na lista de infraestrutura e/ou que foi acordado por todos no fórum de discussões.

Caso ocorra quebra dessa regra, serão aplicadas as seguintes ações:

1. Identificado durante a inspeção nos computadores dos competidores: Retirar o item do competidor.
2. Identificado durante a competição: Retirar o item do competidor, e reduzir pontos no módulo ou resultado, conforme regras específicas da ocupação.

8.2 CAIXA DE FERRAMENTAS DO COMPETIDOR

Os competidores não devem trazer uma caixa de ferramentas. Os competidores podem apenas trazer os materiais citados na lista de infraestrutura que estiverem marcados como “itens de responsabilidade do competidor”, caso haja.

8.3 MATERIAIS, EQUIPAMENTOS E FERRAMENTAS FORNECIDOS PELOS COMPETIDORES EM SUAS CAIXAS DE FERRAMENTAS

Os competidores não são obrigados a trazer materiais, ferramentas ou equipamentos para a competição, mas deverão utilizar os softwares e materiais especificados na Lista de Infraestrutura a seguir.

Local	Período	Modalidade	Competidores Inscritos
???	**27/02/2023 – 03/03/2023**	**#54 Segurança Cibernética**	**6 competidores (3 duplas)**

Perfil de Atuação	Nome	e-mail	Telefone
Coordenação			
Avaliador Líder	Gabriel Araújo Vieira	gabriel.vieira@sep.senai.br	(11) 96071-9910
Aval. Líder Adjunto	Regis Cisotto	regis.cisotto@sp.senai.br	(11) 96595-9663
Chefe de Oficina			

Recusos Físicos					
Item	**Descrição do Item**	**Unid**	**Relação (quant. por..)**		**Qt Total**
1	Servidor para Virtualização (2x Xeon E2-234 3.60GHz / Cache8MB / 04 Núcleos (total 8 núcleos) / 2x SSD 01TB (total 2TB) / 64GB RAM / 02 Interfaces de Rede Gigabit	unid.	1	a cada 2 comp.	3
2	Nobreak com no mínimo 1200va	unid.	1	a cada 2 comp.	3

3	Nobreak com no mínimo 3200va	unid.	1	por servidor	3
4	Switch Cisco Catalyst 24P Gigabit Ethernet Gerenciável	unid.	2	por ocupação	2
5	Computador Intel Core i7, 32 GB RAM, SSD 1TB e Windows 10 x64, com duas saídas de vídeo	unid.	1	por competidor	6
6	Monitor LED de no mínimo 23"	unid.	2	por competidor	12
7	Laptop - Intel Core i5, 8GB DDR4, SSD 240GB,Windows 10 x64	unid.	1	por avaliador	3
8	Patch cord CAT 5e, 3m	unid.	20	por ocupação	20
9	Projetor e Tela de Projeção	unid.	1	por ocupação	1

Softwares para montagem da Infraestrutura					
Item	**Descrição do Item**	**Unid**	**Relação (quant. por..)**		**Qt Total**
10	VMWare ESXI 6.7	unid.	1	por servidor	3
11	Plataforma CTFd	unid.	1	por ocupação	1
12	PNET Lab 4.2.10	unid.	1	por servidor	3
13	VMWare vSphere ESXi 6.7	unid.	1	por servidor	3

Softwares para Emulação					
Item	**Descrição do Item**	**Unid**	**Relação (quant. por..)**		**Qt Total**
14	Imagem Router Cisco (virtualizado)	unid.	1	por servidor	3

15	Imagem Switch Cisco Catalyst 2960 (virtualizado)	unid.	1	por servidor	3
16	Imagem padrão ASAv para PNETLab (virtualizado)	unid.	1	por servidor	3
17	Imagem padrão CentOS 7 com pacotes necessários para a montagem do cenário. (virtualizado) - pacotes serão definidos pelos avaliadores	unid.	1	por ocupação	1
18	Imagem padrão CentOS 7 Desktop com pacotes necessários para a montagem do cenário. (virtualizado) - pacotes serão definidos pelos avaliadores	unid.	1	por ocupação	1
19	Imagem padrão de Servidor Windows 2016 x64 para PNETLab com configurações necessárias para montagem do cenário (virtualizado) - configurações serão definidas pelos avaliadores	unid.	1	por ocupação	1
20	Imagem Windows 10 Enterprise x64 para PNETLab com programas necessários para a montagem do cenário. (virtualizado) - configurações serão definidas pelos avaliadores	unid.	1	por ocupação	1

Softwares para Instalação no Computador do Competidor					
Item	**Descrição do Item**	**Unid**	**Relação (quant. por..)**		**Qt Total**
21	7-ZIP (Windows Server Virtualizado)	unid.	1	por competidor	6
22	FTK Imager	unid.	1	por competidor	6
23	Google Chrome (Windows Host)	unid.	1	por competidor	6
24	Kali Linux 2022.2 virtualizado com VMWare	unid.	1	por competidor	6
25	Leitor de PDF (Windows Host)	unid.	1	por competidor	6
26	Microsoft Office 2019 (Windows Host)	unid.	1	por competidor	6
27	Mozzilla Firefox (Windows Host)	unid.	1	por competidor	6
28	Putty Utilities (Windows Host)	unid.	1	por competidor	6
29	Real VNC (Windows Host)	unid.	1	por competidor	6

30	VMWAre Workstation 16 PRO	unid.	1	por competidor	6
31	VSCode	unid.	1	por competidor	6
32	Windows 10 Enterprise x64	unid.	1	por competidor	6

Softwares para Instalação nas imagens emuladas (Windows Server)					
Item	**Descrição do Item**	**Unid**	**Relação (quant. por..)**		**Qt Total**
33	7-ZIP (Windows Server Virtualizado)	unid.	1	por imagem	1
34	7-ZIP (Windows Server Virtualizado)	unid.	1	por imagem	1
35	Google Chrome (Windows Host)	unid.	1	por imagem	1
36	Mozzilla Firefox (Windows Server Virtualizado)	unid.	1	por imagem	1
37	Splunk Server (Windows Server Virtualizado)	unid.	1	por imagem	1
38	Splunk Universal Forwarder	unid.	1	por imagem	1
39	TFTPD (Windows Server Virtualizado)	unid.	1	por imagem	1
40	WinSCP (Windows Server Virtualizado)	unid.	1	por imagem	1

Softwares para Instalação nas imagens emuladas (Windows Client)					
Item	**Descrição do Item**	**Unid**	**Relação (quant. por..)**		**Qt Total**
41	7-ZIP	unid.	1	por imagem	1

42	Cisco AnyConnect Secure Mobility Client	unid.	1	por imagem	1
43	Google Chrome	unid.	1	por imagem	1
44	Mozilla Firefox	unid.	1	por imagem	1
45	Splunk Universal Forwarder	unid.	1	por imagem	1
46	TFTPD	unid.	1	por imagem	1
47	WinSCP	unid.	1	por imagem	1

Softwares para Instalação nas imagens emuladas (CentOS 7)					
Item	**Descrição do Item**	**Unid**	**Relação (quant. por..)**		**Qt Total**
48	bind-chroot (Centos 7 Virtualizado)	unid.	1	por imagem	1
49	bind-utils (Centos 7 Virtualizado)	unid.	1	por imagem	1
50	bison (Centos 7 Virtualizado)	unid.	1	por imagem	1
51	daq-2.0.6 (Centos 7 Virtualizado)	unid.	1	por imagem	1
52	dns-utils (Centos 7 Virtualizado)	unid.	1	por imagem	1
53	dnsutis (Centos 7 Virtualizado)	unid.	1	por imagem	1
54	flex (Centos 7 Virtualizado)	unid.	1	por imagem	1
55	freeradius-utils (Centos 7 Virtualizado)	unid.	1	por imagem	1
56	ftp (Centos 7 Virtualizado)	unid.	1	por imagem	1
57	gcc (Centos 7 Virtualizado)	unid.	1	por imagem	1
58	httpd (Centos 7 Virtualizado)	unid.	1	por imagem	1
59	libdnet-devel (Centos 7 Virtualizado)	unid.	1	por imagem	1
60	libgcc (Centos 7 Virtualizado)	unid.	1	por imagem	1
61	libsfbpf (Centos 7 Virtualizado)	unid.	1	por imagem	1
62	mod_proxy (Centos 7 Virtualizado)	unid.	1	por imagem	1
63	mod_security (Centos 7 Virtualizado)	unid.	1	por imagem	1

64	mod_security (Centos 7 Virtualizado)	unid.	1	por imagem	1
65	mod_security_crss (Centos 7 Virtualizado)	unid.	1	por imagem	1
66	mod_ssl (Centos 7 Virtualizado)	unid.	1	por imagem	1
67	net-tools (Centos 7 Virtualizado)	unid.	1	por imagem	1
68	radiusd (Centos 7 Virtualizado)	unid.	1	por imagem	1
69	selinux (Centos 7 Virtualizado)	unid.	1	por imagem	1
70	snort 2.9.16.1 (Centos 7 Virtualizado)	unid.	1	por imagem	1
71	splunk (Centos 7 Virtualizado)	unid.	1	por imagem	1
72	splunk-8.1.0 (Centos 7 Virtualizado)	unid.	1	por imagem	1
73	Splunk Universal Fowarder (CentOS 7 Virtualizado)	unid.	1	por imagem	1
74	squid (Centos 7 Virtualizado)	unid.	1	por imagem	1
75	tar (Centos 7 Virtualizado)	unid.	1	por imagem	1
76	tcpdump (Centos 7 Virtualizado)	unid.	1	por imagem	1
77	unrar (Centos 7 Virtualizado)	unid.	1	por imagem	1
78	unzip (Centos 7 Virtualizado)	unid.	1	por imagem	1
79	vim (Centos 7 Virtualizado)	unid.	1	por imagem	1
80	wget (Centos 7 Virtualizado)	unid.	1	por imagem	1
81	zlib (Centos 7 Virtualizado)	unid.	1	por imagem	1
82	zlib-devel (Centos 7 Virtualizado)	unid.	1	por imagem	1

Ferramentas para uso do Competidor (no Kali Linux virtualizado)					
Item	**Descrição do Item**	**Unid**	**Relação (quant. por..)**		**Qt Total**
83	Autopsy (Kali Linux Virtualizado)	unid.	1	por competidor	6
84	Exiftool	unid.	1	por competidor	6
85	Exiftool (Kali Linux Virtualizado)	unid.	1	por competidor	6
86	FTK	unid.	1	por competidor	6
87	GDB Debbuger (Kali Linux Virtualizado)	unid.	1	por competidor	6
88	Ghidra (Kali Linux Virtualizado)	unid.	1	por competidor	6
89	GIMP (Kali Linux Virtualizado)	unid.	1	por competidor	6
90	Gobuster (Kali Linux Virtualizado)	unid.	1	por competidor	6
91	IDA Pro (Kali Linux Virtualizado)	unid.	1	por competidor	6
92	knockd (Kali Linux Virtualizado)	unid.	1	por competidor	6
93	LibreOffice (Kali Linux Virtualizado)	unid.	1	por competidor	6
94	linPEAS (Kali Linux Virtualizado)	unid.	1	por competidor	6
95	ltrace (Kali Linux Virtualizado)	unid.	1	por competidor	6

96	OllyDbg	unid.	1	por competidor	6
97	pwntools (biblioteca Python)	unid.	1	por competidor	6
98	Sonic Visualiser (Kali Linux Virtualizado)	unid.	1	por competidor	6
99	Steghide (Kali Linux Virtualizado)	unid.	1	por competidor	6
100	strace (Kali Linux Virtualizado)	unid.	1	por competidor	6
101	Telnet	unid.	1	por competidor	6
102	telnet (Kali Linux Virtualizado)	unid.	1	por competidor	6
103	Volatility 2 (Kali Linux Virtualizado)	unid.	1	por competidor	6
104	Volatility 3 (Kali Linux Virtualizado)	unid.	1	por competidor	6
105	VSCode	unid.	1	por competidor	6
106	Wine	unid.	1	por competidor	6

Recursos de Responsabilidade do COMPETIDOR			
Item	**Descrição do Item**	**Unid**	**Quant.**
1	Mouse sem recurso de Macro	unid.	1
2	Teclado (QWERTY) sem recurso de Macro	unid.	1

8.4 MATERIAIS E EQUIPAMENTOS PROIBIDOS NA ÁREA DE COMPETIÇÃO

Os competidores poderão apenas trazer os trazer os materiais citados na lista de infraestrutura que estiverem marcados como “itens de responsabilidade do competidor”.

9. REGRAS ESPECÍFICAS DA OCUPAÇÃO

As regras específicas de ocupação não podem contradizer ou ter prioridade sobre as Regras da Competição. Elas fornecem detalhes específicos e clareza em áreas que podem variar de ocupação para ocupação. Isso inclui, mas não se limita a equipamentos de TI, dispositivos de armazenamento de dados, acesso à Internet, procedimentos e fluxo de trabalho, além de gerenciamento e distribuição de documentação

TÓPICO/TAREFA	REGRA ESPECÍFICA DA OCUPAÇÃO
Uso de dispositivos USB, pendrives e cartões de memória	• Não será permitido o uso de pendrives ou cartão de memória pelos Competidores. Caso exista a necessidade de uso desse tipo de dispositivos os mesmos serão fornecidos pela Organização da Competião e não sairãodo ambiente da ocupação em qualquer hipótese. • Os dispositivos de memória deverão ser devolvidos ao avaliador líder no final de cada dia para verificação.
Laptops pessoais	• Avaliadores – Poderá ser permitido o uso de laptops pessoais, mas os laptops snão poderão mais sair do ambiente da ocupação enquanto a prova estiver acontecendo. • Competidores - Nenhum laptop

	pessoal épermitido na competição.
Câmeras Pessoais	• Avaliadores – A filmagem ou fotografia no ambiente de competição estarão sujeitas à aprovação do Avaliador Líder da Ocupação, em concordância com a Coordenação da São Paulo Skills. • Competidores - Não será permitido o uso decâmeras pessoais na ocupação.
Dispositivos móveis	• Avaliadores – Os dispositivos móveis (incluindo telefones celulares) só poderão serusados fora do ambiente da ocupação ou em locais permitidos pelo avaliador líder e/ou coordenação geral da seletiva. • Competidores - Os dispositivos eletrônicos (incluindo telefones celulares) devem permanecer nas malas dos competidores ou em armários disponibilizados pela organização durante todo o tempo de prova, inclusive em pausas para alimentação.
Pausas para alimentação	• Durante cada um dos módulos podem ocorrer pausas para alimentação. O tempo daa pausa será definido pelo Avaliador Líder.
Armazenamento de arquivos para consulta	• Em hipótese alguma o competidor pode armazenar arquivos para consulta em seu posto de trabalho. Durante a prova não poderá haver nenhuma consulta a materiais como livros, cadernos, e-books, anotações manuscritas, folhas, etc.
Usa da Internet	• O uso da internet não é permitido pelos competidores. Todos postos de trabalho devem estar desconectados da internet.

Comunicação entre competidor e Avaliador	• Durante a prova, é terminantemente proibida qualquer comunicação entre os competidores e o Avaliador da mesma unidade. A comunicação na pausa para alimentação é permitida, exceto em casos envolver a solução de defeitos/falha técnica ou em módulos que tenham havido sorteio prévio. Assim, os Competidores e Avaliadores deverão se alimentar separadamente. Durante a competição, para comunicação oficial entre Avaliadores e Competidores da mesma Unidade do SENAI, serão programados intervalos de tempo com duração de 15 minutos, todo início de manhã e final de tarde.
Sorteio dos postos de trabalho	• No primeiro dia de trabalho será feito unm sorteio de modo a definir os postos de trabalho que serão utilizados por cada equipe durante a semana de cometição.
Músicas e fones de ouvido	• Por ser uma modalidade em dupla, não será permitida reprodução de de música ou utilização de fones de ouvido, para que a comunicação não seja prejudicada.

10. SELETIVAS

A Seletiva é uma etapa que antecede a competição estadual e é destinada às modalidades enquadradas no Grupo A. As modalidades desse grupo possuem mais escolas inscritas do que o número de vagas disponíveis para a fase Estadual. A Seletiva consistirá em uma avaliação prática, com duração de no máximo 8 horas, a ser aplicada na própria Unidade do Competidor ou em uma das Unidades Satélite.

Na seletiva, os competidores que obtiverem nota superior à média dos demais competidores da Ocupação serão aprovados para a próxima etapa, conforme o número de vagas preestabelecidas para a Ocupação de Segurança Cibernética.

10.1 LOCAL DE APLICAÇÃO

A Seletiva será aplicada na própria Unidade do Competidor ou em uma das Unidades Satélite. A decisão final será definida pela organização geral da São Paulo Skills.

10.2 DATA DA APLICAÇÃO

O período de aplicação das seletivas será de 31 de outubro a 09 de dezembro de 2022.

10.3 CARACTERÍSTICAS DA PROVA

Durante a Seletiva da modalidade de Segurança Cibernética serão realizados 2 (dois) módulos de 4 horas cada, sendo eles:

- Prova de *Hardening* de Redes: essa prova será elaborada pelos avaliadores participantes do processo e divulgada para todas as Unidades com 7 (sete) dias de antecedência da data da aplicação da seletiva, independentemente de feriados ou inclusões de finais de semana no período. A prova será realizada em um ambiente virtualizado e envolverá conhecimentos de segurança de infraestrutura corporativa. Obrigatoriamente a prova deve conter configuração de serviços e segurança em servidores Linux CentOS 7, Windows Server 2016, ativos de rede (switches, firewall, roteadores) e clientes Windows 10.

- Desafio de *Capture The Flag*: essa prova consistirá em um desafio de *Capture The Flag* com características *boot to root* com duração de 4 horas. A prova deverá ser desenvolvida em um ambiente Linux e resolvida através do sistema Kali Linux. A fim de manter a lisura e integridade do processo, esse módulo não poderá ser divulgado previamente. A proposta deverá ser sorteada no dia da competição a partir de uma seleção de 15 máquinas a serem definidas previamente pelos avaliadores. A organização pode decidir sortear até duas máquinas.

Para atender o princípio da economicidade, os dois módulos deverão ser aplicados no mesmo dia.

O competidor cuja unidade SENAI for a mesma dos elaboradores, aplicadores e/ou avaliadores das provas seletivas deverá ser o primeiro a realizar, sendo que um avaliador de outra unidade será convidado para também atuar como aplicador.

10.4 ELABORAÇÃO DA PROVA

As provas serão elaboradas pelos Avaliadores participantes da seletiva.

10.5 DIVULGAÇÃO DA PROVA

A prova de *hardening* será divulgada através do fórum 7 dias antes da competição. A seleção de máquinas do desafio de Capture the Flag será realizada 1 mês antes da competição e o sorteio para a definição da(s) máquina(s) selecionada(s) será feito no dia da competição.

10.6 INFRAESTRUTURA PARA A SELETIVA

Além dos itens listados na lista de infraestrutura, a Secretaria da São Paulo Skills irá divulgar conforme preestabelecido no Regulamento da Competição, os demais itens que deverão ser providenciados pela Unidade do Competidor para a execução da Seletiva.

Essa relação será encaminhada ao Diretor da Unidade participante, com cópia ao Avaliador. Os prazos para envio serão conforme estabelece o Regulamento da Competição.

11. DESEMPATES

O Desempate consistirá em uma avaliação prática nos mesmos moldes da São Paulo Skills, a ser aplicada em Unidade Neutra.

- Haverá Desempate para as Ocupações do Grupo B;
- O vencedor do desempate será o competidor que totalizar mais pontos considerando-se a somatória da nota da etapa estadual e do desempate;
- As despesas do aplicador da Seletiva serão ressarcidas pela Secretaria da São Paulo Skills;
- Não haverá Desempate nas Ocupações do Grupo B quando a diferença de pontuação do 1º e 2º colocados for superior a 30% do resultado do 1º na São Paulo Skills, considerando-se a escala de 0-100. Essa regra não se aplica caso a fase nacional não ocorra.

11.1 LOCAL DE APLICAÇÃO

A Coordenação da São Paulo Skills irá determinar o local do Desempate. Esta irá sempre que possível selecionar um local neutro, que possua toda, ou quase toda, infraestrutura necessária. Caso não seja possível, a preferência será dada à Unidade de origem do campeão da fase estadual.

11.2 DATA DE APLICAÇÃO

Os desempates ocorrerão entre os meses de fevereiro e março de 2023. Caso seja necessária alteração as Unidades serão informadas com antecedência.

11.3 CARACTERÍSTICAS DA PROVA

O Desempate consistirá em uma avaliação prática nos mesmos moldes da São Paulo Skills.

11.4 ELABORAÇÃO DA PROVA

A Coordenação da São Paulo Skills indicará o responsável pela elaboração da prova.

11.5 DIVULGAÇÃO DA PROVA

A Coordenação da São Paulo Skills decidirá em conjunto com o indicado pela elaboração da prova se essa será ou não divulgada, assim como os prazos.

11.6 INFRAESTRUTURA PARA O DESEMPATE

Além dos itens listados na lista de infraestrutura, a Secretaria da São Paulo Skills irá divulgar conforme preestabelecido no Regulamento da Competição, os demais itens que deverão ser providenciados pela Unidade do Competidor para a execução da Seletiva.

Essa relação será encaminhada ao Diretor da Unidade participante, com cópia ao Avaliador. Os prazos para envio serão conforme estabelece o Regulamento da Competição.