



Formação em Cibersegurança



MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO



Programação dos Cursos

Confira agora a grade completa da formação Hackers do Bem:

Nivelamento - 80h

1 - Introdução à cibersegurança

- Aula 1 - O que são hackers e seus tipos- White/Grey/Black hat
- Aula 2 - Ethical hackers - Conceito de ética/O que é ethical hacking?
- Aula 3 - Profissões em cibersegurança - Red Team/Blue Team/Forense/Governança, Risco e Compliance/DevSecOps
- Aula 4 - Conceitos iniciais - Vírus/Worms/Phishing/Cavalo de Troia
- Aula 5 - Como se proteger - Noções de boas práticas para senhas/sites/e-mails

2 - Identificar componentes de hardware de computador

- Aula 1 - Grandezas computacionais/Sistemas numéricos
- Aula 2 - Arquitetura de hardware - CPU/Placa mãe/Memória/BIOS
- Aula 3 - Arquitetura de hardware - Armazenamento/Fontes/Gabinete/Placas de expansão
- Aula 4 - Virtualização
- Aula 5 - Instalação de SO (Windows/Linux via pendrive)

3 - Compreender internet e camada de acesso à rede

- Aula 1 - História da internet
- Aula 2 - Tipos de Conexões (DSL/Coaxial/FTTH/MPLS/Dedicado)
- Aula 3 - LAN/WAN/Topologias
- Aula 4 - Intranet/Extranet
- Aula 5 – Ativos de rede (Switch/Roteador/Firewall/AP)
- Aula 6 - Conectividade - Camada Física - Full/Half duplex
- Aula 7 - Par metálico
- Aula 8 - Fibra
- Aula 9 - Rádio (sem fio)

4 - Compreender acesso à rede e camada de internet (IP)

- Aula 1 - Camada de acesso à rede (física e enlace OSI) - Frame/Quadro endereçamento camada 2
- Aula 2 - Endereço MAC e como o dado trafega pelas redes de comunicação dos ativos das camadas 1 e 2
- Aula 3 - Protocolo ARP
- Aula 4 - Endereçamento IPv4 - Binário - Redes/Host/Broadcast - Classfull/Classless - Multicast/Broadcast/Únicas
- Aula 5 - IP Público/Privado/NAT
- Aula 6 - Subrede

5 - Compreender IPv6 e camada de transporte

- Aula 1 - Endereçamento IPv6 - Necessidade IPv6/Mostrar cabeçalho/Hexadecimal/Hexadecateto
- Aula 2 - Tipos de endereço (GUA/LLA/Loopback/Unique local) - Unicast/Multicast/Anycast
- Aula 3 - Abreviações IPv6
- Aula 4 - Subrede IPv6
- Aula 5 - Camada transporte/Cabeçalho e portas TCP/UDP/Netstat/Portas e serviços de redes principais
- Aula 6 - Protocolo TCP
- Aula 7 - Protocolo UDP

6 - Compreender camada de aplicação/serviços de rede

- Aula 1 - E-mail
- Aula 2 - Web (HTTP/HTTPS)
- Aula 3 - DNS
- Aula 4 - DHCP
- Aula 5 – Acessos remotos (Telnet, SSH, RDP, via aplicativos)
- Aula 6 - Transferência de arquivo (SMB, CIFS, Torrent, FTP)
- Aula 7 - Controle de usuário (LDAP, RADIUS)
- Aula 8 - SNMP/NTP/SYSLOG

7 - Utilizar sistemas operacionais

- Aula 1 - Versões licenciamento/Server e desktop/Histórico e versões
- Aula 2 - Estrutura de diretórios
- Aula 3 - Entendendo o File System
- Aula 4 - Criar, renomear, apagar, visualizar arquivos/pastas, comandos básicos (Gráfica e Prompt)
- Aula 5 - Criação de usuários, grupos e permissões de segurança e compartilhamento
- Aula 6 - Backup/Pontos de restauração/Registro
- Aula 7 - Instalações de programas/Pacotes/Drivers

8 - Lógica de programação

- Aula 1 - Fluxograma/Lógica de programação
- Aula 2 - Programas compilados e interpretados
- Aula 3 - Programação estruturada
- Aula 4 - Algoritmo
- Aula 5 - Entrada e saída
- Aula 6 - Variável
- Aula 7 - Estrutura condicional
- Aula 8 - Estrutura de repetição

9 - Desenvolvimento de scripts

- Aula 1 - Scripts Windows
- Aula 2 - Scripts Linux



Básico - 64h**1 - Compreender os tipos, modelos e conceitos da computação em nuvem**

- Aula 1 - Histórico da computação em nuvem
- Aula 2 - Diferenças entre on-premise e nuvem
- Aula 3 - Características da nuvem
- Aula 4 - Modelos de implantação em nuvem (pública, privada e híbrida)
- Aula 5 - Modelos de serviços em nuvem (IaaS, PaaS e SaaS)
- Aula 6 - Principais provedores de nuvem

2 - Compreender os principais conceitos de desenvolvimento

- Aula 1 - Principais tipos de linguagem de programação
- Aula 2 - Principais tipos de aplicações
- Aula 3 - Metodologias de desenvolvimento
- Aula 4 - Conceitos básicos de banco de dados

3 - Identificar as principais ameaças cibernéticas

- Aula 1 - Tipos de ataques
- Aula 2 - Atores de ameaças
- Aula 3 - Engenharia social
- Aula 4 - Malwares

4 - Compreender os principais elementos associados e vulnerabilidades

- Aula 1 - Conceitos
- Aula 2 - Frameworks e padrões
- Aula 3 - Ferramentas e processos

5 - Compreender as principais aplicações de criptografia 1 e 2

- Aula 1 - Protocolos seguros
- Aula 2 - Hash
- Aula 3 - Tipos de chaves
- Aula 4 - Certificado digital
- Aula 5 - Infraestrutura de chave pública

6 - Compreender os principais elementos relacionados a Governança, Risco e Compliance 1 e 2

- Aula 1 - Confidencialidade, integridade e disponibilidade
- Aula 2 - Principais frameworks
- Aula 3 - Controles de segurança
- Aula 4 - Políticas
- Aula 5 - Aspectos legais, proteção de dados e privacidade (LGPD)
- Aula 6 - Ética



Fundamental - 96h

1 - Princípios de segurança e engenharia social

- Aula 1 - Fundamentos da segurança da informação: Triade CIA, Least Privilege, Segurança em Profundidade
- Aula 2 - Atores de ameaças, atributos, vetores de ataque e fontes de inteligência
- Aula 3 - Engenharia social
- Aula 4 - Segurança ofensiva x defensiva: Ferramentas, técnicas e papéis

2 - Ameaças, malwares e controles

- Aula 1 - Tipos de malware
- Aula 2 - Análise de indicadores de malware e prevenção de malware
- Aula 3 - Categorias de controle de segurança
- Aula 4 - Fontes de ameaça: Darknet e Darkweb

3 - Técnicas utilizadas na identificação de ameaças

- Aula 1 - Gerenciamento de vulnerabilidades
- Aula 2 - Scanner de vulnerabilidades: Ativo x Passivo
- Aula 3 - Honeybots e outras armadilhas
- Aula 4 - Análise de tráfego TCP/IP

4 - Controles de acesso

- Aula 1 - Gerenciamento de identidade e acesso
- Aula 2 - Autenticação baseada em conhecimento
- Aula 3 - Tecnologias de autenticação
- Aula 4 - Autenticação por biometria

5 - Gerenciamento de identidades e contas

- Aula 1 - Tipos de contas e identidades
- Aula 2 - Políticas de contas
- Aula 3 - Soluções de autorização e políticas de pessoal
- Aula 4 - Políticas de pessoal

6 - Proteção Web e desenvolvimento seguro

- Aula 1 - Ataques e proteção Web - Parte 1
- Aula 2 - Ataques e proteção Web - Parte 2
- Aula 3 - Práticas de codificação segura e análise de código
- Aula 4 - Scripts em ambientes seguros

7 - Redundância, backup, segurança física e destruição de dados

- Aula 1 - Redundância e replicação
- Aula 2 - Backup
- Aula 3 - Segurança física
- Aula 4 - Técnicas para destruição segura de dados

8 - Conceitos de criptografia

- Aula 1 - Propriedades da criptografia
- Aula 2 - Criptografia simétrica
- Aula 3 - Funções Hash
- Aula 4 - Criptografia assimétrica

9 - Infraestrutura de chaves públicas

- Aula 1 - Autoridades certificadoras
- Aula 2 - Certificado digital
- Aula 3 - Gerenciamento de infraestrutura de chaves públicas (PKI)
- Aula 4 - Blockchain

10 - Segurança no host

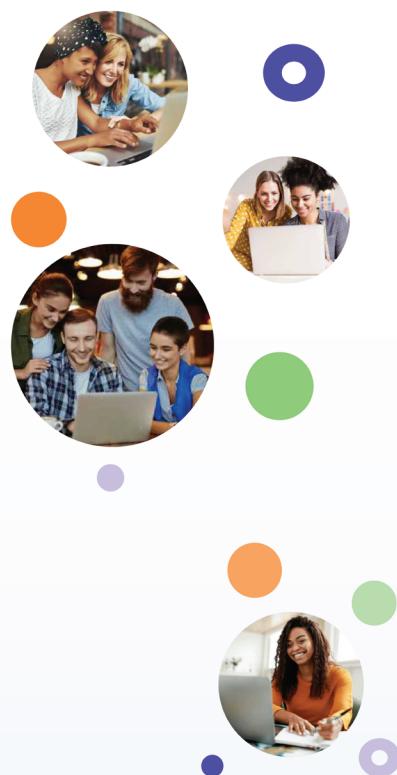
- Aula 1 - Proteção do endpoint
- Aula 2 - Segurança em sistemas embarcados
- Aula 3 - Firmware seguro
- Aula 4 - Segurança em virtualização e nuvem

11 - Equipamentos de segurança

- Aula 1 - Balanceadores de carga, VPN e NAC
- Aula 2 - Segmentação de rede e port security
- Aula 3 - Equipamentos de segurança de rede (Firewall, IDS/IPS)
- Aula 4 - Segurança em redes sem fio

12 - Resposta a incidentes e protocolos seguros

- Aula 1 - Processo de resposta a incidentes
- Aula 2 - Protocolos seguros
- Aula 3 - Governança, compliance e gerenciamento de risco
- Aula 4 - Forense digital



Especializado - 80 h

Especialização Governança, Risco e Compliance

1 - Governança

- Aula 1 - Conceitos fundamentais de gestão da segurança
- Aula 2 - Visão geral da ISO 27001, 27002 e 27701
- Aula 3 - Política de segurança da informação
- Aula 4 - Verificação da conformidade com requisitos legais, políticas e normas de segurança da informação
- Aula 5 - Mapeamento de processos

2 - Risco

- Aula 1 - Conceitos fundamentais de gestão de riscos
- Aula 2 - A norma NBR ISO/IEC 27005 e 31000
- Aula 3 - Metodologias de gestão de riscos
- Aula 4 - Processo de tratamento, redução e retenção dos riscos
- Aula 5 - Processo de comunicação e monitoramento dos riscos

3 - Compliance

- Aula 1 - Fundamentos da governança corporativa e governança corporativa de TIC
- Aula 2 - Governança corporativa de TIC x Gestão de TIC x Auditoria de TIC
- Aula 3 - Modelo do COSO
- Aula 4 - Modelo do COBIT
- Aula 5 - Normas brasileiras de compliance de TI

04 - Estudo de caso

- Aula 1 - Estudo de caso

Especialização Blue Team

1 - Design de rede segura e segurança

- Aula 1 - Arquitetura e design de rede segura
- Aula 2 - Ataques e estratégias de defesa
- Aula 3 - Infraestrutura de chaves públicas
- Aula 4 - Gerenciamento de configuração e infraestrutura como serviço
- Aula 5 - Segurança em estações de trabalho

2 - Segurança em sistemas operacionais e ativos de rede

- Aula 1 - Segurança em sistema Windows
- Aula 2 - Segurança em sistema Linux
- Aula 3 - Segurança de ativos de rede
- Aula 4 - Segurança em ambientes virtualizados
- Aula 5 - Protocolos seguros de rede

3 - Monitoramento e segurança em demais tecnologias

- Aula 1 - Gerenciando e monitorando vulnerabilidades
- Aula 2 - Segurança em redes sem fio
- Aula 3 - Técnicas de autenticação
- Aula 4 - Monitoramento e análise de tráfego
- Aula 5 - Gerenciamento de logs centralizados

4 - Estudo de caso

- Aula 1 - Estudo de caso

Especialização Red Team

1 - Metodologias de pentest

- Aula 1 - Introdução ao pentest
- Aula 2 - Pré-engajamento
- Aula 3 - Reconhecimento
- Aula 4 - Scan e enumeração - Parte 01
- Aula 5 - Scan e enumeração - Parte 02

2 - Teste de penetração em sistemas operacionais e ativos de rede

- Aula 1 - Ataque de engenharia social
- Aula 2 - Ataques em demais tecnologias
- Aula 3 - Ataque Web – Client-Side
- Aula 4 - Ataque Web – Server-Side
- Aula 5 - Ataques de força Bruta

03 - Teste de penetração em demais tecnologias

- Aula 1 - Reconhecimento em Linux
- Aula 2 - Escalação de privilégios em Linux
- Aula 3 - Reconhecimento em Windows
- Aula 4 - Escalação de privilégios em Windows
- Aula 5 - Coleta de evidências e relatório

04 - Estudo de caso

- Aula 1 - Estudo de caso

Especialização Resposta a Incidentes e Forense

1 - Tratamento de incidentes

- Aula 1 - Ameaças cibernéticas (Cyber Threats) e metodologia de cadeia de eliminação (Kill Chain Methodology)
- Aula 2 - Tratamento de incidentes e processo de resposta
- Aula 3 - Tratamento de incidentes - Malware e e-mail
- Aula 4 - Tratamento de incidentes - Rede e aplicativo web
- Aula 5 - Criando uma equipe de resposta a incidentes

2 - Tratamento de dados

- Aula 1 - Coleta, tratamento e análise de dados usando um SIEM/SOAR
- Aula 2 - Detecção aprimorada de incidentes com inteligência de ameaças
- Aula 3 - Processo de investigação
- Aula 4 - Coleta de evidências: discos rígidos e sistemas de arquivos
- Aula 5 - Coleta de evidências: memória e rede

3 - Forense computacional

- Aula 1 - Introdução à forense computacional - Windows e Linux
- Aula 2 - Análise forense em discos rígidos e sistemas de arquivos
- Aula 3 - Análise forense em memória
- Aula 4 - Análise forense em rede
- Aula 5 - Investigando ataques na web

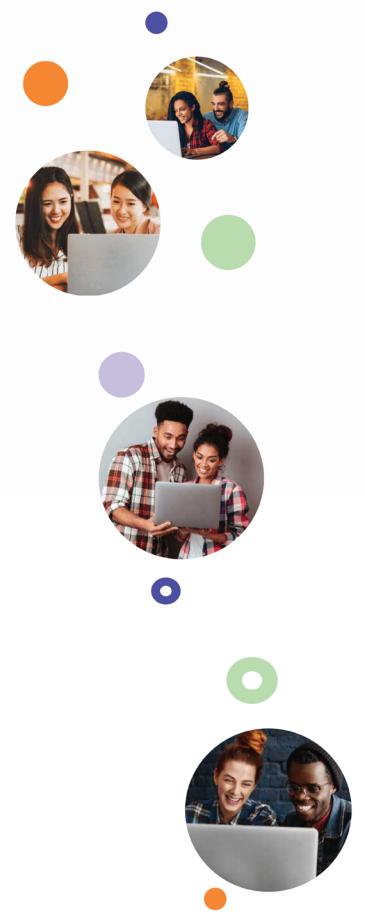
4 - Estudo de caso

- Aula 1 - Estudo de caso

Especialização DevOps/DevSecOps

1 - Processo de desenvolvimento seguro

- Aula 1 - Introdução ao SDLC (Software Development Lifecycle)
- Aula 2 - Modelos de SDLC (Waterfall, Lean e Agile)
- Aula 3 - Modelo DevOps
- Aula 4 - Secure SDLC
- Aula 5 - Containers



2 - DevOps e InfraAgil

- Aula 1 - Introdução ao Git e GitLab
- Aula 2 - Infraestrutura ágil com o GitLab - Continuação
- Aula 3 - Controle de versão e resolução de conflitos com GitLab
- Aula 4 - Pipelines e integração contínua com GitLab
- Aula 5 - Testes automatizados e sua importância

3 - DevSecOps

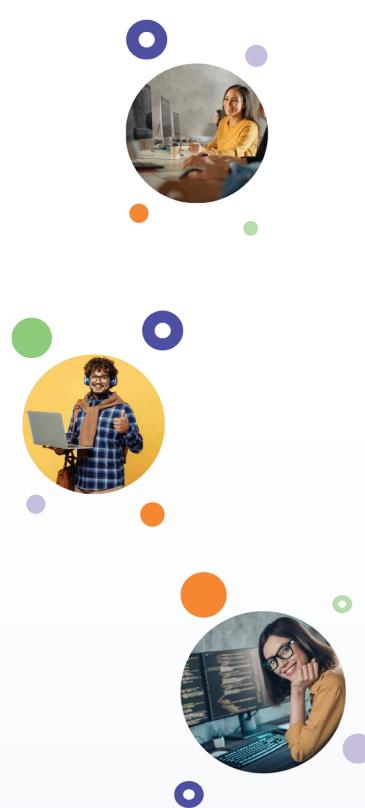
- Aula 1 - Introdução ao DevSecOps
- Aula 2 - Segurança de software e análise de vulnerabilidades
- Aula 3 - Desenvolvimento seguro e automação de tarefas de segurança
- Aula 4 - Monitoramento e resposta a incidentes em DevSecOps
- Aula 5 - Práticas em DevSecOps

4 - Estudo de caso

- Aula 1 - Estudo de caso

Residência Tecnológica

Em breve maiores informações.





Manual

Aprovação, Gamificação,
Rankeamento e Classificação



MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO



SUMÁRIO

1. APRESENTAÇÃO	3
2. ESTRUTURA DA FORMAÇÃO	3
3. CRONOGRAMA BASE.....	4
4. CRITÉRIOS DE APROVAÇÃO.....	5
4.1. APROVAÇÃO NIVELAMENTO	6
4.2. APROVAÇÃO BÁSICO	6
4.3. APROVAÇÃO FUNDAMENTAL	7
4.4. APROVAÇÃO ESPECIALIZADO	8
4.5. APROVAÇÃO RESIDÊNCIA.....	9
5. GAMIFICAÇÃO	9
5.1. GAMIFICAÇÃO CURSO NIVELAMENTO.....	10
5.2. GAMIFICAÇÃO CURSO BÁSICO	10
5.3. GAMIFICAÇÃO CURSO FUNDAMENTAL	12
5.4. GAMIFICAÇÃO CURSO ESPECIALIZADO.....	21
5.5. GAMIFICAÇÃO RESIDÊNCIA	21
6. RANQUEAMENTO E CLASSIFICAÇÃO	21
6.1. RANQUEAMENTO E CLASSIFICAÇÃO: NIVELAMENTO PARA O BÁSICO	22
6.2. RANQUEAMENTO E CLASSIFICAÇÃO: BÁSICO PARA O FUNDAMENTAL.....	22
6.3. RANQUEAMENTO E CLASSIFICAÇÃO: FUNDAMENTAL PARA O ESPECIALIZADO ..	23
6.4. RANQUEAMENTO E CLASSIFICAÇÃO: ESPECIALIZADO PARA A RESIDÊNCIA.....	24
7. CONSIDERAÇÕES IMPORTANTES.....	24

1. APRESENTAÇÃO

O presente documento estabelece as regras e critérios para aprovação, gamificação e ranqueamento (avanço entre os cursos), dos alunos participantes do Programa Hackers do Bem.

A formação oferecida pelo Hackers do Bem é completamente gratuita. No primeiro momento, o aluno terá acesso ao curso chamado "Nivelamento". Ao concluir esse curso, ele estará preparado para avançar para o próximo nível, o curso "Básico", que também conta com aulas gravadas.

Dando continuidade à formação, será oferecido os cursos - Fundamental e Especialização, que incluem aulas ao vivo e atividades práticas em laboratório. Estes dois últimos cursos, com calendários previamente divulgados que se estenderão até 2025, e com acesso condicionado às regras que detalharemos neste documento.

1. ESTRUTURA DA FORMAÇÃO

O Programa Hackers do Bem foi estruturado com os seguintes cursos de formação:

Curso	Responsável pelo conteúdo	Modalidade	Carga Horária total
Nivelamento	SENAI – SP	Assíncrono	80
Básico	SENAI – SP	Assíncrono	64
Fundamental	ESR – RNP	Síncrono	96
Especializado	ESR – RNP	Síncrono	80
Residência	ESR – RNP	Híbrido	*A definir

Tanto para o Nivelamento quanto o Básico, o progresso entre os cursos é livre. Isso significa que o aluno irá iniciar pelo Nivelamento e, ao concluir, poderá avançar para o Básico sem restrições.



MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

No entanto, para progredir para os cursos Fundamental e Especializado, foram estabelecidos critérios de aprovação. Estes critérios são baseados no desempenho do aluno na avaliação final e nas atividades práticas. Além da aprovação, o aluno também precisará alcançar uma boa colocação no ranqueamento geral. Este ranqueamento é construído através de um sistema de *Gamificação* que leva em consideração aspectos como o consumo de conteúdo, o desempenho nos Quizzes avaliativos, Atividades Práticas, Avaliação Final, entre outros.

2. CRONOGRAMA BASE

O cronograma para a formação Hackers do Bem foi estruturado em ondas, planejadas para cobrir um período de 2 (dois) anos de oferta do programa. Entende-se como “Onda” a oferta de todos os 5 cursos do programa: Nivelamento, Básico, Especializado e Residência

Neste documento, apresentaremos as informações referentes à 1º (primeira) e 2º(segunda) onda de oferta, que será completamente distribuída ao longo dos anos de 2024 e 2025.

CRONOGRAMA 1º ONDA

FORMAÇÃO HACKERS DO BEM



CRONOGRAMA 2º ONDA

FORMAÇÃO HACKERS DO BEM

Básico

Início: 25/03/2024

Término: Livre

22/01/2024

25/03/2024

21/10/2024

Especializado

Início: 17/02/2025

Término: 13/04/2025

12/05/2025

Nivelamento

Início: 22/01/2024

Término: Livre

Fundamental

Início: 21/10/2024

Término: 22/12/2024

Residência

Início: 12/05/2025

Término: 09/11/2025

IMPORTANTE:

Os cursos de Nivelamento e Básico estarão disponíveis e poderão ser iniciados em qualquer momento durante toda a formação do Hackers do Bem. No entanto, é necessário se atentar a data limite para conclusão, a fim de ingressas nos próximos cursos.

3. CRITÉRIOS DE APROVAÇÃO

Os critérios de aprovação consistem nos requisitos ou padrões estabelecidos para avaliar se o aluno alcançou os objetivos de aprendizagem estabelecidos e se pode avançar para a próxima fase da formação Hackers do Bem. Dentre eles:

AVALIAÇÃO FINAL:

Uma avaliação final de um curso é a avaliação que ocorre ao término do curso e é projetada para medir os conhecimentos, habilidades e competências desenvolvidas pelos alunos ao longo do programa. Geralmente, a avaliação final é abrangente e aborda os principais conceitos, tópicos e objetivos de aprendizagem do curso.

ATIVIDADES PRÁTICAS (laboratórios virtuais):

São exercícios ou tarefas que os alunos realizam em ambientes virtuais simulados, geralmente utilizando software de virtualização, para desenvolver



habilidades práticas e conhecimentos técnicos relacionados a sistemas operacionais, redes, segurança da informação e outras áreas da TI. Essas atividades práticas oferecem uma oportunidade para os alunos aplicarem os conceitos teóricos aprendidos em sala de aula em cenários do mundo real, experimentando configurações, resolvendo problemas e realizando tarefas práticas.

ESTUDOS DE CASO:

Um estudo de caso é uma análise detalhada e aprofundada de uma situação ou problema específico relacionado à área de estudo. Oferece uma oportunidade para os alunos analisarem e resolverem problemas do mundo real, contribuindo para o desenvolvimento de habilidades práticas e conhecimento aplicado.

Cada curso, com exceção do Nivelamento, terá seus critérios de aprovação, que serão considerados pré-requisitos para que o aluno possa ser incluído no ranqueamento e tenha a oportunidade de avançar para o curso seguinte.

	Nivelamento	Básico	Fundamental	Especializado	Residência
Avaliação Final	✗	✓	✓	✓	✗
Atividades Práticas	✗	✗	✓	✓	✗
Estudo de Caso	✗	✗	✗	✓	✗

3.1. APROVAÇÃO - NIVELAMENTO

Para o Curso de Nivelamento, não serão estabelecidos critérios de aprovação, isso significa dizer que não há requisitos específicos que os alunos precisam atender para conclusão do curso. O objetivo principal do curso é de fornecer acesso a conhecimentos relevantes em Cibersegurança, sem a necessidade de avaliação formal ou atribuição de notas.

3.2. APROVAÇÃO - BÁSICO

O curso Básico estabelecerá apenas 1 (um) critério de aprovação, que será o pré-requisito para a conclusão do curso e obtenção do Certificado. Em caso de reaprovação, o aluno não terá a oportunidade de participar do ranqueamento e,

consequentemente, não poderá avançar para o curso Fundamental. Entretanto, como regra, todos os alunos terão 2 (duas) oportunidades para realizar a Avaliação Final, seja para melhorar sua nota ou em caso de reprovação na primeira tentativa. No entanto, vale ressaltar que sempre contabilizaremos para a aprovação a nota mais alta, independentemente de ter sido obtida na 1º (primeira) ou 2º (segunda) tentativa.

A Avaliação Final do curso consistirá em um instrumento com 10 (dez) questões objetivas de múltipla escolha. Para ser aprovado, o aluno precisará atingir um desempenho igual ou superior a 60% (sessenta por cento) de acerto das questões (6 questões). As questões abrangem uma variedade de conteúdos e conceitos apresentados durante o curso, com o objetivo de avaliar se o aluno desenvolveu uma compreensão ampla dos tópicos discutidos.

3.3. APROVAÇÃO - FUNDAMENTAL

Ao avançar para o curso Fundamental, o aluno terá 2 (dois) critérios de aprovação a serem considerados.

A Avaliação Final, assim como o curso Básico, contará com um instrumento com 10 (dez) questões objetivas de múltipla escolha e, para ser aprovado, o aluno precisará atingir um desempenho igual ou superior a 60% (sessenta por cento) de acerto das questões (6 questões). Também, como regra, todos os alunos terão 2 (duas) oportunidades de realização, seja para melhorar sua nota ou em caso de reprovação na primeira tentativa. No entanto, vale ressaltar que sempre contabilizaremos para a aprovação a nota mais alta, independentemente de ter sido obtida na 1º (primeira) ou 2º (segunda) tentativa.

Quanto as Atividades Práticas, o aluno entregará via Ambiente Virtual de Aprendizagem (AVA) um relatório de execução, ao qual, será submetido a uma correção pelo Docente e atribuído uma nota de 0 (zero) a 10 (dez), por atividade. Caso não entregue alguma das atividades práticas obrigatórias propostas, automaticamente será atribuído nota 0 (zero) para aquela entrega. Para aprovação, o aluno terá de garantir média de 60% (sessenta por cento), ou seja, garantir uma nota de no mínimo 6 (seis) pontos na soma de toda as atividades obrigatórias do curso.

Veja 2 (dois) exemplos abaixo:

ALUNO A = Nota 7,1 pontos APROVADO



MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INovação

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

ALUNO A					
Módulo	Total de atividades práticas obrigatórias	Total de atividades do curso	Nota obtida pelo aluno em cada atividade	Soma das notas das atividades práticas	Média obtida pela divisão da soma das notas pelo total de atividades
Módulo 1	3	18	9	128	7,1
			10		
			4		
			7		
			10		
			8		
			5		
			7		
			7		
			8		
			9		
			10		
Módulo 2	3	18	10	128	7,1
			8		
			5		
			7		
			10		
			0		
			6		
			4		
			7		
			7		
			7		
Módulo 3	3	18	7	128	7,1
			8		
			9		
			10		
			7		
			5		
			7		
			8		
			10		
			0		
			6		
			4		
Módulo 4	3	18	8	128	7,1
			9		
			10		
			7		
			5		
			7		
			8		
			10		
			0		
			6		
			4		
			7		
Módulo 5	3	18	7	128	7,1
			10		
			0		
			6		
			4		
			7		
			7		
			7		
			7		
			7		
			7		
			7		
Módulo 6	3	18	7	128	7,1
			7		
			7		
			7		
			7		
			7		
			7		
			7		
			7		
			7		
			7		
			7		

ALUNO B = Nota 5,7 pontos REPROVADO

ALUNO B					
Módulo	Total de atividades práticas obrigatórias	Total de atividades do curso	Nota obtida pelo aluno em cada atividade	Soma das notas das atividades práticas	Média obtida pela divisão da soma das notas pelo total de atividades
Módulo 1	3	18	2	103	5,7
			10		
			4		
			7		
			5		
			5		
			5		
			6		
			3		
			8		
			3		
			10		
Módulo 2	3	18	7	103	5,7
			5		
			5		
			7		
			6		
			3		
			8		
			3		
			10		
			7		
			4		
			6		
Módulo 3	3	18	4	103	5,7
			10		
			7		
			5		
			5		
			3		
			8		
			3		
			10		
			7		
			4		
			6		
Módulo 4	3	18	3	103	5,7
			10		
			7		
			4		
			6		
			4		
			7		
			7		
			7		
			7		
			7		
			7		
Módulo 5	3	18	7	103	5,7
			4		
			6		
			4		
			6		
			4		
			7		
			7		
			7		
			7		
			7		
			7		
Módulo 6	3	18	7	103	5,7
			7		
			7		
			7		
			7		
			7		
			7		
			7		
			7		
			7		
			7		
			7		

3.4. APROVAÇÃO - ESPECIALIZADO

Para concluir o Curso Especializado, o aluno terá de passar por 3 (três) critérios de aprovação para obtenção de certificado e garantir a oportunidade de

avanço para o próximo curso. Todas as regras serão discutidas previamente e comunicadas em uma próxima versão deste documento.

3.5. APROVAÇÃO RESIDÊNCIA

Todas as regras para a Residência serão discutidas previamente e comunicadas em uma próxima versão deste documento.

4. GAMIFICAÇÃO

A gamificação no ensino digital é uma abordagem que utiliza elementos e mecânicas de jogos para engajar o aluno em seu processo de aprendizagem. O objetivo é tornar o processo de aprendizagem mais interativo, divertido e motivador, promovendo ao mesmo tempo a retenção de conhecimento e o desenvolvimento de habilidades.

Ao incorporar elementos de Gamificação em seu ambiente educacional, o Programa Hackers do Bem busca criar um processo de aprendizagem mais dinâmico e estimulante, incluindo a utilização de pontuações e rankings para incentivar os alunos a alcançarem seus objetivos de aprendizagem e avanço para os próximos cursos.

O progresso entre os cursos da formação será determinado não apenas pela aprovação, mas também pelos pontos obtidos na Gamificação e sua Classificação no Ranking Geral. Isso implica, que para avançar para o próximo curso, com exceção do Nivelamento para o Básico, os alunos precisarão demonstrar um bom desempenho de acordo com as regras estabelecidas, pois isso influenciará sua posição no ranking. Dado que os cursos Fundamental, Especializado e Residência possuem vagas limitadas, a performance na gamificação será crucial para garantir um lugar nessas etapas subsequentes.

É importante observar que, embora o aluno tenha 2 (duas) oportunidades para responder à Avaliação Final, os pontos da gamificação serão contabilizados apenas 1 (uma) vez. Será levado em consideração o total de acertos do seu melhor desempenho, seja ele na 1º (primeira) ou na 2º (segunda) tentativa. Por exemplo, se na 1º (primeira) tentativa o aluno acertou um total de 3 (três) questões na Avaliação Final e na 2º (segunda) tentativa acertou 7 (sete) questões, ele será considerado aprovado e sua pontuação na Gamificação será proporcional aos 7 (sete) acertos, ou seja, 70 pontos.



ATENÇÃO

1. A pontuação da gamificação é acumulativa. Isso significa que, ao avançar de um curso para o outro, o aluno levará sua pontuação do nível anterior. Portanto, o bom ou mau desempenho em um curso anterior poderá influenciar diretamente as posições no ranking de classificação.

4.1. GAMIFICAÇÃO CURSO NIVELAMENTO

Para o curso de Nivelamento, a gamificação foi idealizada considerando o consumo dos conteúdos disponíveis. Ao progredir entre os diferentes conteúdos e módulos, os alunos acumularão uma pontuação previamente estabelecida. No entanto, essa pontuação não será um requisito para avançar para o curso Básico, já que suas vagas são ilimitadas e todos os alunos terão a oportunidade de avançar para essa etapa da formação.

Abaixo, disponibilizamos a tabela de pontos distribuídos para cada elemento da Gamificação no curso Nivelamento:

Gamificação do curso Nivelamento - Tabela de Pontuação			
Conteúdos dos módulos			
Módulo	Nome do conteúdo	Pontos de experiência (xp)	Acúmulo de xp
1	Introdução a Cibersegurança	10	10
1	Ebook - Introdução a Cibersegurança	5	15
2	Identificar componentes de hardware de computador	10	25
2	Ebook - Identificar componentes de hardware de computador	5	30
3	Compreender Internet e Camada de acesso a rede	15	45
3	Ebook - Compreender Internet e Camada de acesso a rede	5	50
4	Compreender acesso a rede e camada de internet (IP)	15	65
4	Ebook - Compreender acesso a rede e camada de internet (IP)	5	70
5	Compreender IPv6 e camada de transporte	20	90
5	Ebook - Compreender IPv6 e camada de transporte	5	95
6	Compreender camada de Aplicação / Serviços de rede	20	115
6	Ebook - Compreender camada de Aplicação / Serviços de rede	5	120
7	Utilizar Sistemas Operacionais Windows	25	145
7	Ebook - Utilizar Sistemas Operacionais Windows	5	150
8	Utilizar Sistemas Operacionais - Linux	25	175
8	Ebook - Utilizar Sistemas Operacionais - Linux	5	180
9	Compreender lógica de programação	30	210
9	Ebook - Compreender lógica de programação	5	215
10	Desenvolvimento de Scripts	30	245
10	Ebook - Desenvolvimento de Scripts	5	250
Total		250	

4.2. GAMIFICAÇÃO CURSO BÁSICO

No curso Básico, adotamos uma estrutura ligeiramente mais elaborada que o Nivelamento. Além do consumo de conteúdo pelos alunos, haverá também a



atribuição de pontos para a realização de *Quizzes* de Fixação. Esses *Quizzes* consistirão em 3 questões objetivas de múltipla escolha por módulo, além da Avaliação Final, que conterá 10 questões na mesma estrutura.

É importante destacar que para progredir do Curso Básico para o Fundamental, o aluno precisará obter aprovação na Avaliação Final e demonstrar um bom desempenho nos pontos atribuídos na gamificação. Somente assim, ele poderá alcançar uma posição favorável no ranking e assegurar sua vaga no curso seguinte.

Abaixo disponibilizamos a tabela de pontos distribuídos para cada elemento da Gamificação no curso Básico:

Gamificação do curso Básico - Tabela de Pontuação				
Conteúdos dos módulos				
Módulo	Nome do conteúdo	Total de tentativas	Pontos de experiência (xp)	Acúmulo de xp
1	Compreender os tipos, modelos e conceitos da computação em nuvem	N/A	10	260
1	Ebook - Compreender os tipos, modelos e conceitos da computação em nuvem	N/A	7	267
1	Quizz de Fixação (3 questões)	1	15 (5 pontos por acerto de questão)	282
2	Compreender os principais conceitos de desenvolvimento	N/A	10	292
2	Ebook - Compreender os principais conceitos de desenvolvimento	N/A	8	300
2	Quizz de Fixação (3 questões)	1	15 (5 pontos por acerto de questão)	315
3	Identificar as principais ameaças cibernéticas	N/A	15	330
3	Ebook - Identificar as principais ameaças cibernéticas	N/A	9	339
3	Quizz de Fixação (3 questões)	1	15 (5 pontos por acerto de questão)	354
4	Compreender os principais elementos associados e vulnerabilidades	N/A	15	369

4	Ebook - Compreender os principais elementos associados e vulnerabilidades	N/A	10	379
4	Quizz de Fixação (3 questões)	1	15 (5 pontos por acerto de questão)	394
5	Compreender as principais aplicações de criptografia 1 e 2	N/A	20	414
5	Ebook - Compreender as principais aplicações de criptografia 1 e 2	N/A	11	425
5	Quizz de Fixação (3 questões)	1	15 (5 pontos por acerto de questão)	440
6	Compreender os principais elementos relacionados a Governança, Risco e Compliance 1 e 2	N/A	20	460
6	Ebook - Compreender os principais elementos relacionados a Governança, Risco e Compliance 1 e 2	N/A	12	472
6	Quizz de Fixação (3 questões)	1	15 (5 pontos por acerto de questão)	487
7	Avaliação Final	2	100 (10 pts por acerto)	587
8	Pesquisa de Satisfação do Curso	N/A	15	602
	Total		602 pts	

4.3. GAMIFICAÇÃO CURSO FUNDAMENTAL

A gamificação no curso Fundamental, assim como no Básico, estará diretamente relacionada ao progresso para o curso Especializado. O aluno só poderá avançar do Curso Fundamental para o Especializado se obtiver aprovação em todos os instrumentos avaliativos (Atividades Práticas e Avaliação Final), além de garantir uma boa colocação no ranking, novamente determinada pela pontuação adquirida na Gamificação.

Neste curso, implementaremos uma estrutura ainda mais abrangente do que nos cursos anteriores. Como resultado, haverá uma distribuição significativa de pontos que contemplam o consumo de conteúdo, a precisão nas respostas das

questões objetivas, a entrega das atividades propostas e a participação nos encontros online.

Gamificação do curso Fundamental - Tabela de Pontuação			
Conteúdos dos módulos			
Nome do conteúdo	Total de tentativas	Pontos de experiência (xp)	Acúmulo de xp
Enquete Inicial - Diagnóstica	N/A	15	617
Módulo 1 - Princípios de segurança e engenharia social			
Nome do conteúdo	Total de tentativas	Pontos de experiência (xp)	Acúmulo de xp
Aula 1 - Fundamentos da Segurança da Informação: Triade CIA, Least Privilege, Segurança em Profundidade	N/A	7	624
Aula 2 - Atores de ameaças, atributos, vetores de ataque e fontes de inteligência	N/A	8	632
Aula 3 - Engenharia social	N/A	9	641
Aula 4 - Segurança Ofensiva vs Defensiva: Ferramentas, Técnicas e Papéis	N/A	10	651
Vídeoaula	N/A	5	656
Slides	N/A	0	656
Questão objetiva obrigatória (1 questão)	1	10 (acerto da questão)	666
Atividade Prática obrigatória 1	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	676
Atividade Prática obrigatória 2	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	686
Atividade Prática obrigatória 3	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	696
Encontro Online 1	N/A	15	711
Encontro Online 2	N/A	15	726
Gravação Encontro Online 1	N/A	7	733
Gravação Encontro Online 2	N/A	8	741
Atividade Prática Extra	N/A	7	748
Questão objetiva Extra (11 questões)	1	55 (5 pts por acerto)	803
Módulo 2 - Ameaças, Malwares e Controles			

Nome do conteúdo	Total de tentativas	Pontos de experiência (xp)	Acúmulo de xp
Aula 1 - Tipos de Malware	N/A	7	810
Aula 2 - Análise de indicadores de Malware e prevenção de Malware	N/A	8	818
Aula 3 - Categorias de controle de segurança	N/A	9	827
Aula 4 - Fontes de ameaça: Darknet e Darkweb	N/A	10	837
Vídeoaula	N/A	5	842
Slides	N/A	0	842
Questão objetiva obrigatória	1	10 (acerto da questão)	852
Atividade Prática obrigatória 1	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	862
Atividade Prática obrigatória 2	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	872
Atividade Prática obrigatória 3	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	882
Encontro Online 1	N/A	15	897
Encontro Online 2	N/A	15	912
Gravação Encontro Online 1	N/A	7	919
Gravação Encontro Online 2	N/A	8	927
Atividade Prática Extra	N/A	7	934
Questão objetiva Extra (11 questões)	1	55 (5 pts por acerto)	989

Módulo 3 - Técnicas utilizadas na identificação de ameaças

Nome do conteúdo	Total de tentativas	Pontos de experiência (xp)	Acúmulo de xp
Aula 1 - Gerenciamento de vulnerabilidades	N/A	7	996
Aula 2 - Scanner de vulnerabilidades: Ativo x Passivo	N/A	8	1004
Aula 3 - Honeypots e outras “armadilhas”	N/A	9	1013
Aula 4 - Análise de Tráfego TCP/IP	N/A	10	1023
Vídeoaula	N/A	5	1028
Slides	N/A	0	1028
Questão objetiva obrigatória	1	10 (acerto da questão)	1038
Atividade Prática obrigatória 1	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1048
Atividade Prática obrigatória 2	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1058

Atividade Prática obrigatória 3	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1068
Encontro Online 1	N/A	15	1083
Encontro Online 2	N/A	15	1098
Gravação Encontro Online 1	N/A	7	1105
Gravação Encontro Online 2	N/A	8	1113
Atividade Prática Extra	N/A	7	1120
Questão objetiva Extra (11 questões)	1	55 (5 pts por acerto)	1175

Módulo 4 - Controles de acesso

Nome do conteúdo	Total de tentativas	Pontos de experiência (xp)	Acúmulo de xp
Aula 1 - Gerenciamento de identidade e acesso	N/A	7	1182
Aula 2 - Autenticação baseada em conhecimento	N/A	8	1190
Aula 3 - Tecnologias de autenticação	N/A	9	1199
Aula 4 - Autenticação por biometria	N/A	10	1209
Vídeoaula	N/A	5	1214
Slides	N/A	0	1214
Questão objetiva obrigatória	1	10 (acerto da questão)	1224
Atividade Prática obrigatória 1	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1234
Atividade Prática obrigatória 2	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1244
Atividade Prática obrigatória 3	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1254
Encontro Online 1	N/A	15	1269
Encontro Online 2	N/A	15	1284
Gravação Encontro Online 1	N/A	7	1291
Gravação Encontro Online 2	N/A	8	1299
Atividade Prática Extra	N/A	7	1306
Questão objetiva Extra (11 questões)	1	55 (5 pts por acerto)	1361

Módulo 5 - Gerenciamento de identidades e contas

Nome do conteúdo	Total de tentativas	Pontos de experiência (xp)	Acúmulo de xp
Aula 1 - Tipos de contas e identidades	N/A	7	1368
Aula 2 - Políticas de contas	N/A	8	1376
Aula 3 - Soluções de autorização e políticas de pessoal	N/A	9	1385
Aula 4 - Políticas de pessoal	N/A	10	1395
Vídeoaula	N/A	5	1400
Slides	N/A	0	1400

Questão objetiva obrigatória	1	10 (acerto da questão)	1410
Atividade Prática obrigatória 1	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1420
Atividade Prática obrigatória 2	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1430
Atividade Prática obrigatória 3	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1440
Encontro Online 1	N/A	15	1455
Encontro Online 2	N/A	15	1470
Gravação Encontro Online 1	N/A	7	1477
Gravação Encontro Online 2	N/A	8	1485
Atividade Prática Extra	N/A	7	1492
Questão objetiva Extra (11 questões)	1	55 (5 pts por acerto)	1547

Módulo 6 - Proteção Web e desenvolvimento seguro

Nome do conteúdo	Total de tentativas	Pontos de experiência (xp)	Acúmulo de xp
Aula 1 - Ataques e proteção Web - Parte 1	N/A	7	1554
Aula 2 - Ataques e proteção Web - Parte 2	N/A	8	1562
Aula 3 - Práticas de codificação segura e análise de código	N/A	9	1571
Aula 4 - Scripts em ambientes seguros	N/A	10	1581
Vídeoaula	N/A	5	1586
Slides	N/A	0	1586
Questão objetiva obrigatória	1	10 (acerto da questão)	1596
Atividade Prática obrigatória 1	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1606
Atividade Prática obrigatória 2	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1616
Atividade Prática obrigatória 3	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1626
Encontro Online 1	N/A	15	1641
Encontro Online 2	N/A	15	1656
Gravação Encontro Online 1	N/A	7	1663
Gravação Encontro Online 2	N/A	8	1671
Atividade Prática Extra	N/A	7	1678
Questão objetiva Extra (11 questões)	1	55 (5 pts por acerto)	1733

Módulo 7 - Redundância, Backup, Segurança física e Destrução de dados



MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

Nome do conteúdo	Total de tentativas	Pontos de experiência (xp)	Acúmulo de xp
Aula 1 - Redundância e replicação	N/A	7	1740
Aula 2 - Backup	N/A	8	1748
Aula 3 - Segurança física	N/A	9	1757
Aula 4 - Técnicas para destruição segura de dados	N/A	10	1767
Vídeoaula	N/A	5	1772
Slides	N/A	0	1772
Questão objetiva obrigatória	1	10 (acerto da questão)	1782
Atividade Prática obrigatória 1	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1792
Atividade Prática obrigatória 2	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1802
Atividade Prática obrigatória 3	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1812
Encontro Online 1	N/A	15	1827
Encontro Online 2	N/A	15	1842
Gravação Encontro Online 1	N/A	7	1849
Gravação Encontro Online 2	N/A	8	1857
Atividade Prática Extra	N/A	7	1864
Questão objetiva Extra (11 questões)	1	55 (5 pts por acerto)	1919

Módulo 8 - Conceitos de criptografia

Nome do conteúdo	Total de tentativas	Pontos de experiência (xp)	Acúmulo de xp
Aula 1 - Propriedades da criptografia	N/A	7	1926
Aula 2 - Criptografia simétrica	N/A	8	1934
Aula 3 - Funções Hash	N/A	9	1943
Aula 4 - Criptografia assimétrica	N/A	10	1953
Vídeoaula	N/A	5	1958
Slides	N/A	0	1958
Questão objetiva obrigatória	1	10 (acerto da questão)	1968
Atividade Prática obrigatória 1	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1978
Atividade Prática obrigatória 2	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1988
Atividade Prática obrigatória 3	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	1998
Encontro Online 1	N/A	15	2013
Encontro Online 2	N/A	15	2028
Gravação Encontro Online 1	N/A	7	2035

Gravação Encontro Online 2	N/A	8	2043
Atividade Prática Extra	N/A	7	2050
Questão objetiva Extra (11 questões)	1	55 (5 pts por acerto)	2105

Módulo 9 - Infraestrutura de Chaves Públicas

Nome do conteúdo	Total de tentativas	Pontos de experiência (xp)	Acúmulo de xp
Aula 1 - Autoridades certificadoras	N/A	7	2112
Aula 2 - Certificado Digital	N/A	8	2120
Aula 3 - Gerenciamento de Infraestrutura de Chaves Públicas (PKI)	N/A	9	2129
Aula 4 - Blockchain	N/A	10	2139
Vídeoaula	N/A	5	2144
Slides	N/A	0	2144
Questão objetiva obrigatória	1	10 (acerto da questão)	2154
Atividade Prática obrigatória 1	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	2164
Atividade Prática obrigatória 2	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	2174
Atividade Prática obrigatória 3	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	2184
Encontro Online 1	N/A	15	2199
Encontro Online 2	N/A	15	2214
Gravação Encontro Online 1	N/A	7	2221
Gravação Encontro Online 2	N/A	8	2229
Atividade Prática Extra	N/A	7	2236
Questão objetiva Extra (11 questões)	1	55 (5 pts por acerto)	2291

Módulo 10 - Segurança no host

Nome do conteúdo	Total de tentativas	Pontos de experiência (xp)	Acúmulo de xp
Aula 1 - Proteção do Endpoint	N/A	7	2298
Aula 2 - Segurança em sistemas embarcados	N/A	8	2306
Aula 3 - Firmware seguro	N/A	9	2315
Aula 4 - Segurança em virtualização e nuvem	N/A	10	2325
Vídeoaula	N/A	5	2330
Slides	N/A	0	2330
Questão objetiva obrigatória	1	10 (acerto da questão)	2340
Atividade Prática obrigatória 1	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	2350

Atividade Prática obrigatória 2	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	2360
Atividade Prática obrigatória 3	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	2370
Encontro Online 1	N/A	15	2385
Encontro Online 2	N/A	15	2400
Gravação Encontro Online 1	N/A	7	2407
Gravação Encontro Online 2	N/A	8	2415
Atividade Prática Extra	N/A	7	2422
Questão objetiva Extra (11 questões)	1	55 (5 pts por acerto)	2477

Módulo 11 - Equipamentos de segurança

Nome do conteúdo	Total de tentativas	Pontos de experiência (xp)	Acúmulo de xp
Aula 1 - Balanceadores de carga, VPN e NAC	N/A	7	2484
Aula 2 - Segmentação de rede e port security	N/A	8	2492
Aula 3 - Equipamentos de segurança de rede (Firewall, IDS/IPS)	N/A	9	2501
Aula 4 - Segurança em redes sem fio	N/A	10	2511
Vídeoaula	N/A	5	2516
Slides	N/A	0	2516
Questão objetiva obrigatória	1	10 (acerto da questão)	2526
Atividade Prática obrigatória 1	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	2536
Atividade Prática obrigatória 2	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	2546
Atividade Prática obrigatória 3	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	2556
Encontro Online 1	N/A	15	2571
Encontro Online 2	N/A	15	2586
Gravação Encontro Online 1	N/A	7	2593
Gravação Encontro Online 2	N/A	8	2601
Atividade Prática Extra	N/A	7	2608
Questão objetiva Extra (11 questões)	1	55 (5 pts por acerto)	2663

Módulo 12 - Resposta a incidentes e protocolos seguros

Nome do conteúdo	Total de tentativas	Pontos de experiência (xp)	Acúmulo de xp
Aula 1 - Processo de resposta a incidentes	N/A	7	2670
Aula 2 - Protocolos seguros	N/A	8	2678

Aula 3 - Governança, compliance e gerenciamento de risco	N/A	9	2687
Aula 4 - Forense digital	N/A	10	2697
Vídeoaula	N/A	5	2702
Slides	N/A	0	2702
Questão objetiva obrigatória	1	10 (acerto da questão)	2712
Atividade Prática obrigatória 1	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	2722
Atividade Prática obrigatória 2	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	2732
Atividade Prática obrigatória 3	N/A	Até 10pts (de acordo com a nota atribuída pelo docente)	2742
Encontro Online 1	N/A	15	2757
Encontro Online 2	N/A	15	2772
Gravação Encontro Online 1	N/A	7	2779
Gravação Encontro Online 2	N/A	8	2787
Atividade Prática Extra	N/A	7	2794
Questão objetiva Extra (11 questões)	1	55 (5 pts por acerto)	2849

Avaliação Final do Curso

Nome do conteúdo	Total de tentativas	Pontos de experiência (xp)	Acúmulo de xp
Avaliação Final (10 questões)	2	100 (10 pts por acerto)	2949

Pesquisa de Satisfação do Curso

Nome do conteúdo	Total de tentativas	Pontos de experiência (xp)	Acúmulo de xp
Pesquisa de Satisfação do Curso	N/A	15	2964
Total	2696 pts		

ATENÇÃO

1. A pontuação da gamificação referente a participação nos Encontros Online será computada mediante registro de presença, a ser realizado durante o encontro e pelo próprio aluno.
2. As pontuações da gamificação referente as Atividades Práticas Obrigatórias serão computadas de acordo com as notas atribuídas pelo Docente, não apenas pela entrega das mesmas, diferente da Atividade Prática não Obrigatória que será pontuada apenas pela sua entrega e validação do Docente.

4.4. GAMIFICAÇÃO CURSO ESPECIALIZADO

Para o curso Especializado, a gamificação desempenhará um papel fundamental para o avanço para a etapa da Residência. Além disso, serão considerados outros elementos para sua composição. Todos esses aspectos serão cuidadosamente discutidos e comunicados aos alunos antes do início do curso, garantindo transparência e clareza quanto aos critérios Gamificação e Ranqueamento.

4.5. GAMIFICAÇÃO RESIDÊNCIA

Na Residência, devido à sua natureza prática e necessidade de imersão intensiva, inicialmente não implementaremos uma estrutura de gamificação.

5. RANQUEAMENTO E CLASSIFICAÇÃO

O processo de ranqueamento e classificação envolve a avaliação e ordenação automática dos alunos com base nos critérios anteriormente estabelecidos, a fim de determinar sua posição relativa dentro do grupo. Este processo será utilizado com a finalidade de admissão dos alunos nos cursos Fundamental, Especializado e na Residência.

O Ranqueamento será conduzido com base em uma combinação de fatores, incluindo inicialmente a Aprovação do aluno e o seu desempenho na Gamificação. Sendo assim, cada um dos elementos gamificados contribuirão para uma pontuação geral do aluno, que é então comparada com a dos demais participantes.

A classificação resultante será apresentada em 3 (três) listas classificatórias, onde os alunos serão ordenados do melhor para o pior desempenho. Em cada lista o aluno receberá a notificação de sua classificação, e terá um prazo (data) específico para se matricular, caso contrário, poderá perder a sua vaga no curso. A execução de cada lista ficará condicionada ao preenchimento das vagas ofertada no curso, ou seja, se na primeira lista tivermos o preenchimento de 100% (cem por cento) das vagas com alunos matriculados, não será necessária a realização das demais.

Os alunos convocados na 1º lista que não se matricularem dentro do prazo estabelecido serão temporariamente considerados desistentes, podendo ou não, participar da 2º onda de oferta (a depender de sua colocação no ranking classificatório), e suas vagas serão destinadas à 2º lista. Esta lista será composta pelos próximos colocados no ranqueamento que não foram convocados



anteriormente. O mesmo procedimento será repetido para a 3º lista, que será composta pelas vagas não preenchidas na anterior.

5.1. RANQUEAMENTO E CLASSIFICAÇÃO: NIVELAMENTO PARA BÁSICO

No curso Básico do programa Hackers do Bem, não há limitação de vagas, permitindo que o aluno avance do curso Nivelamento para o Básico sem restrições. **Para isso, basta que complete a degustação de todo o conteúdo e emita o certificado.**

5.2. RANQUEAMENTO E CLASSIFICAÇÃO: BÁSICO PARA FUNDAMENTAL

O aluno que deseja ingressar no curso Fundamental deve observar cuidadosamente alguns critérios, regras e datas pré-estabelecidas, além dos critérios de Aprovação e Gamificação discutidos anteriormente.

Cronograma de execução das listas:

Principais datas Avanço curso Básico para Fundamental						
Onda	Data de Inscrição	Data de Liberação da 1º Lista	Data de Liberação da 2º Lista	Data de Liberação da 3º Lista	Início do Curso	Final do Curso
1º onda	22/04/2024 a 03/05/2024	Liberação: 22/04/2024	Liberação: 27/04/2024	Liberação: 01/05/2024	06/05/2024	01/07/2024
		Inscrições estarão disponíveis do dia 22/04/2024 a 26/04/2024	Inscrições estarão disponíveis do dia 27/04/2024 a 30/04/2024	Inscrições estarão disponíveis do dia 01/05/2024 a 03/05/2024		
2º onda	30/09/2024 a 16/10/2024	Liberação: 30/09/2024	Liberação: 06/10/2024	Liberação: 11/10/2024	21/10/2024	16/12/2024
		Inscrições estarão disponíveis do dia 30/09/2024 a 05/10/2024	Inscrições estarão disponíveis do dia 06/10/2024 a 10/10/2024	Inscrições estarão disponíveis do dia 11/10/2024 a 15/10/2024		

- Na 1º(primeira) onda, prevista para início de convocação em 22/04/2024, estima-se a convocação de 1.690 (mil seiscentas e noventa) alunos.
- Na 2º(segunda) onda, prevista para início de convocação em 30/09/2024, estima-se a convocação de contaremos com 1.625 (mil seiscentas e vinte e cinco) alunos.

Em caso de empate e impossibilidade de seleção dos últimos alunos classificados, serão estabelecidos os seguintes critérios de desempate:

- 1º) Maior nota na Avaliação Final
- 2º) Maior nota no Quizz de fixação



MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INovação

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

- 3º) Maior pontuação no consumo do conteúdo
 4º) Menor data de término do curso Básico (início/fim)

A data limite de finalização do curso Básico para ingresso no Fundamental pela 1º lista é de 1 (um) dia anterior à data de liberação da mesma. Alunos que finalizaram o curso Básico entre a liberação das 3 (três) listas, serão considerados na próxima lista a ser liberada. Caso o aluno finalize o curso pós a data de liberação da última lista, ele terá a oportunidade de entrar apenas na próxima onda, se houver.

5.3. RANQUEAMENTO E CLASSIFICAÇÃO: FUNDAMENTAL PARA ESPECIALIZADO

O aluno que deseja ingressar no curso Especializado deve observar cuidadosamente alguns critérios, regras e datas pré-estabelecidas, além dos critérios de Aprovação e Gamificação discutidos anteriormente.

Cronograma de execução das listas:

Principais datas Avanço curso Fundamental para Especializado						
Onda	Data de Incrição	Data de Liberação da 1º Lista	Data de Liberação da 2º Lista	Data de Liberação da 3º Lista	Início do Curso	Final do Curso
1º onda	15/07/2024 a 26/07/2024	Liberação: 15/07/2024	Liberação: 20/07/2024	Liberação: 24/07/2024	05/08/2024	16/09/2024
		Inscrições estarão disponíveis do dia 15/07/2024 a 19/07/2024	Inscrições estarão disponíveis do dia 20/07/2024 a 23/07/2024	Inscrições estarão disponíveis do dia 24/07/2024 a 27/07/2024		
2º onda	28/01/2025 a 12/02/2025	Liberação: 28/01/2025	Liberação: 03/02/2025	Liberação: 08/02/2025	17/02/2025	07/04/2025
		Inscrições estarão disponíveis do dia 28/01/2025 a 02/02/2025	Inscrições estarão disponíveis do dia 03/02/2025 a 07/02/2025	Inscrições estarão disponíveis do dia 08/02/2025 a 12/02/2025		

- Na 1º(primeira) onda, prevista para início de convocação em 15/07/2024, estima-se a convocação de 1.030 (mil e trinta) alunos.
- Na 2º (segunda), prevista para início da convocação em 28/01/2025, estima-se a convocação de 1.240 (mil duzentos e quarenta) alunos.

	Especialização	Total de Vagas
1º onda	GRC -	250
	BluTeam	195
	RedTeam	195
	Forense	195
	DevSecOps	195
2º onda	GRC -	200
	BluTeam	260
	RedTeam	260
	Forense	260
	DevSecOps	260

Em caso de empate e impossibilidade de seleção dos últimos alunos classificados, serão estabelecidos os seguintes critérios de desempate:

- 1º) maior nota das atividades práticas,
- 2º) maior nota na avaliação final
- 3º) maior nota no *Quizz* obrigatório
- 4º) maior nota nas atividades extras: prática e *Quizzes*
- 5º) maior pontuação no consumo do conteúdo

5.4. RANQUEAMENTO E CLASSIFICAÇÃO: ESPECIALIZADO PARA RESIDÊNCIA

As regras de Ranqueamento e Classificação do Especializado para a Residência, assim como a estrutura da gamificação, serão desenvolvidas e comunicadas em um momento oportuno.

6. CONSIDERAÇÕES IMPORTANTES

- a) A análise dos recursos e contestações de aprovação/reprovação e ranqueamento é de responsabilidade da RNP.
- b) Com a comunicação prévia da lista de classificados para avanço entre os cursos, o participante assume a responsabilidade pelo cumprimento dos prazos estabelecidos.

- c) Independentemente da posição no ranqueamento, o aluno deverá selecionar a turma, turno, curso(especializado) e\ou horário. Caberá ao aluno selecionar seu interesse, de acordo com os limites de vagas pré-estabelecidos em cada turma. Após o preenchimento das vagas, a turma ficará indisponível, e o aluno só poderá se matricular nas turmas que ainda possuírem vagas.
- d) O aluno não terá permissão para troca de turma, turno, curso(especializado) e\ou horário após efetuação da matrícula.
- e) A RNP poderá realocar alunos de turmas, mediante comunicação prévia, de acordo com as necessidades de operacionalização.
- f) O ranqueamento não concederá prioridade aos alunos com base em sua colocação. Com a abertura do período de matrícula, todos os alunos terão igual oportunidade de selecionar uma turma de interesse.
- g) A responsabilidade pelo registro de presença nos encontros online é do aluno. Não serão aceitas contestações por esquecimento ou justificativas de falta, já que a presença não é um critério determinante para a aprovação, sendo relevante apenas para a gamificação.

IMPORTANTE!

O aluno terá 2 (duas) oportunidades para realizar a Avaliação Final. Além disso, disponibilizaremos todo o conteúdo dos cursos, para livre acesso do aluno ao longo do Programa, sem que isso sensibilize sua pontuação no ranking geral.





MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO



Projeto apoiado pelo Ministério da Ciência, Tecnologia e Inovações, com recursos da Lei no 8.248, de 23 de outubro de 1991