CertiProf®
Professional Knowledge

CAMINHO DE CARREIRA EM SEGURANÇA CIBERNÉTICA

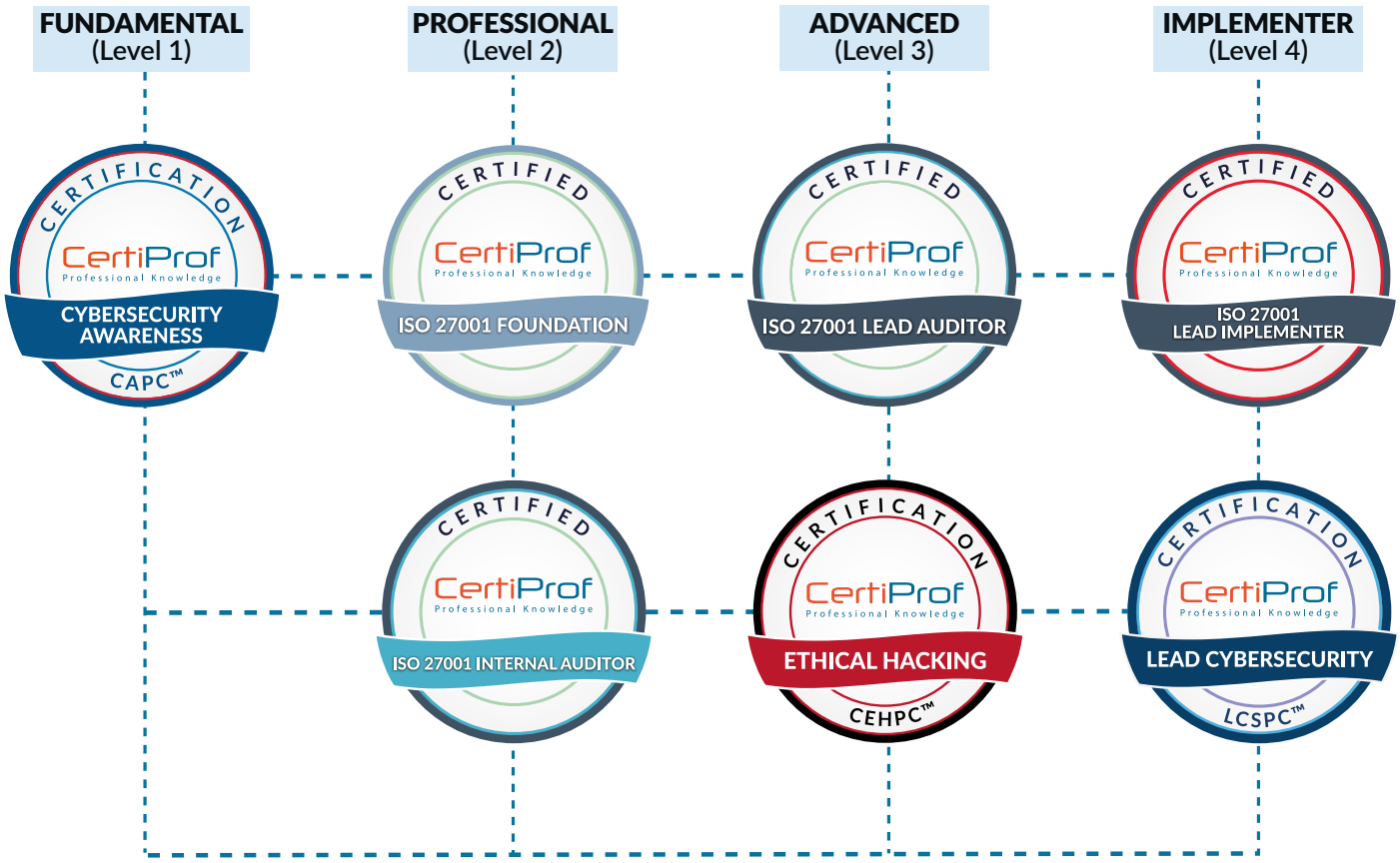
Desenvolver um plano de carreira em cibersegurança requer uma abordagem estruturada e progressiva. Um caminho recomendado é detalhado aqui, começando com a obtenção de conhecimentos básicos e terminando com a obtenção de um especialista em segurança cibernética certificado mediante programas de certificação CertiProf.

À medida que você progride em cada fase, você desenvolverá um conjunto abrangente de habilidades e conhecimentos que lhe permitirão enfrentar os desafios de segurança cibernética em qualquer ambiente organizacional.

Desde a compreensão dos fundamentos até as principais auditorias e gerenciamento de riscos complexos, este plano de carreira irá prepará-lo para ser um especialista em segurança cibernética altamente competitiva no mercado de trabalho.

Essa abordagem estruturada garante que cada passo que você dá o aproxima de seus objetivos profissionais, fornecendo um caminho claro para a excelência em segurança cibernética.

Saiba mais sobre nosso caminho de carreira em segurança cibernética



01

Cybersecurity Awareness Professional Certification CAPC™

Objetivos:

Fornecer conhecimento básico de segurança cibernética, identificar ameaças comuns e aplicar medidas de proteção essenciais.

Habilidades desenvolvidas:

Compreensão dos conceitos básicos de segurança cibernética, reconhecimento de ameaças comuns, implementação de ameaças e implementação de medidas básicas de segurança.

Perfis apropriados:

Profissionais de diferentes disciplinas, uma vez que sua aplicação no ambiente de trabalho é essencial, especialmente para desenvolver conhecimentos que agreguem valor a todos os perfis de trabalho na aplicação de medidas cruciais de segurança cibernética.

Benefícios:

- **Conhecimento Básico:** Fornece uma compreensão fundamental dos conceitos de segurança cibernética.
- **Conscientização sobre ameaças:** Ajuda a identificar ameaças e vulnerabilidades comuns,
- melhorar as capacidades de resposta a incidentes.
- **Práticas recomendadas:** Ensina as melhores práticas para proteger informações pessoais e profissionais.
- **Acessibilidade:** Não requer conhecimento prévio e é aplicável a qualquer profissional.
- **Cultura de Segurança:** Promove uma cultura de segurança dentro da organização.

Requisitos *(opcional)*:

Nenhum

02

CertiProf Certified ISO/IEC 27001:2022 Foundation I27001F™

Objetivos:

Compreender os princípios, conceitos e requisitos da norma ISO 27001 e desenvolver habilidades para a interpretação dos requisitos do SGSI.

Habilidades desenvolvidas:

Compreensão dos conceitos da ISO 27001, interpretação dos requisitos da Norma para implementação do SGSI.

Perfis apropriados:

PROFISSIONAIS DE TI, auditores internos, pessoal de segurança da informação, consultores de SEGURANÇA DE TI, líderes de equipe de auditoria.

Benefícios:

Compreender os conceitos para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) conforme a ISO 27001 permite que as organizações reduzam significativamente os riscos associados à segurança da informação. Isso é conseguido pela implementação de controles adequados para mitigar ameaças, reduzindo tanto a probabilidade quanto os impactos de incidentes de segurança da informação.

Requisitos *(opcional)*:

Cybersecurity Awareness Professional Certification

03

CertiProf Certified ISO/IEC 27001:2022 Internal Auditor I27001A™

Objetivos:

Compreender os princípios, conceitos e requisitos da ISO 27001 e desenvolver as habilidades para realizar auditorias internas de SGSI.

Habilidades desenvolvidas:

Realizar auditorias internas eficazes, desenvolvimento e implementação do SGSI, conformidade com a ISO 27001.

Perfis apropriados :

PROFISSIONAIS DE TI, auditores internos, pessoal de segurança da informação.

Benefícios:

- **Auditoria ISMS :** Desenvolver habilidades para realizar auditorias internas de Sistemas de Gestão de Segurança da Informação (ISMS).
- **Conformidade regulamentar:** Ajude a garantir que a organização esteja conforme as normas internacionais de segurança da informação.
- **Melhoria Contínua:** Facilitar a identificação de áreas para melhoria na gestão da segurança da informação.
- Aberto a profissionais com conhecimentos básicos em Cibersegurança.
- **Credibilidade:** Melhore a credibilidade profissional demonstrando conhecimentos específicos em auditoria de segurança.

Requisitos *(opcional)*:

Cybersecurity Awareness Professional Certification

04

Ethical Hacking
Professional Certification
CEHPC™

Objetivos:

Centra-se no ensino de técnicas e metodologias para identificar e corrigir vulnerabilidades nos sistemas de informação.

Requisitos *(opcional)*:

Cybersecurity Awareness, ISO 27001 Internal/Lead Auditor

Perfis apropriados :

- Administradores de sistema que gerenciam a INFRAESTRUTURA DE TI.
- Engenheiros de rede que projetam e gerenciam redes de comunicação.
- Especialistas em segurança que protegem informações e aplicam políticas de segurança.
- Analistas de segurança que monitoram e analisam incidentes.
- Consultores e Auditores de Cibersegurança que aconselham sobre estratégias e realizam avaliações de conformidade.
- Desenvolvedores e Arquitetos de Software que integram práticas de segurança e projetam sistemas resilientes.
- Auditores internos e profissionais de conformidade que garantem o cumprimento de regras e regulamentos.
- Estudantes DE TI ou cibersegurança e recém-formados que procuram se especializar e obter certificações para se destacar no mercado de trabalho de cibersegurança.

Benefícios:

- Proficiência em técnicas avançadas de hacking ético, incluindo testes de penetração, exploração de vulnerabilidade vulnerabilidades e uso de ferramentas de hacking.
- Compreensão profunda das ameaças cibernéticas e. Vulnerabilidades cibernéticas, que lhe permitirão proativamente identificar e mitigar riscos de forma proativa.

Habilidades desenvolvidas:

- Coleta de informações e detecção de vulnerabilidades
- vulnerabilidades em sistemas, aplicativos e redes sem serem detectadas.
- Exploração de vulnerabilidades para avaliar seu impacto na segurança.
- Realização de testes de penetração total.
- Compromisso de redes Wi-Fi e com fio usando várias técnicas de hacking.

05

CertiProf Certified ISO/IEC 27001:2022 Lead Auditor I27001LA™

Objetivos:

Fornecer conhecimento avançado da norma ISO 27001 e desenvolver habilidades para liderar equipes de auditoria de equipes de auditoria de sistemas de gerenciamento de segurança da informação ISMS (SGSI).

Habilidades desenvolvidas:

Liderança em auditorias, implementação de melhores práticas de SGSI, compreensão do Sistema de Gestão de Segurança da Informação (SGSI), compreensão avançada da ISO 27001

Perfis apropriados :

Auditores internos avançados, consultores de segurança da informação, líderes da equipe de auditoria.

Benefícios:

- **Liderança de Auditoria:** Treina para liderar auditorias de SGSI, o que é crucial para papéis mais responsáveis de maior responsabilidade.
- **Conhecimento Avançado:** Fornece uma compreensão profunda da ISO 27001 e seus requisitos.
- **Gestão Eficaz:** Melhora a gestão e as competências organizacionais na implementação e manutenção do SGSI
- **Competitividade:** Aumenta a competitividade no mercado de trabalho, mantendo uma certificação avançada.
- **Aplicabilidade Global:** Reconhecido internacionalmente, que expande as oportunidades de emprego globais.

Requisitos *(opcional):*

Cybersecurity Awareness Professional Certification

06

Lead Cybersecurity Professional Certification LCSPC™

Objetivos:

Ensinar os fundamentos da segurança cibernética, gerenciamento de riscos e como implementar uma estrutura de segurança cibernética eficaz

Habilidades desenvolvidas:

Gestão de riscos de cibersegurança, implementação de estruturas de segurança, proteção de infraestruturas digitais.

Perfis apropriados:

Administradores de sistemas, engenheiros de rede, especialistas em segurança da informação, analistas de segurança, consultores de segurança cibernética, TI, desenvolvedores de software.

Benefícios:

- **Gerenciamento de Risco:** Desenvolver habilidades avançadas na identificação, avaliação e mitigação de riscos de cibersegurança.
- **Implementação de segurança:** Fornece conhecimento prático para implementar estruturas de segurança cibernética.
- **Melhoria da infraestrutura:** Treina para melhorar a infraestrutura de segurança cibernética de uma organização.
- **Ampla aplicabilidade:** Adequado para uma ampla gama de PROFISSIONAIS DE TI e segurança cibernética.
- **Colaboração Internacional:** Promove uma compreensão da importância da colaboração internacional em cibersegurança.

Requisitos *(opcional):*

Cybersecurity Awareness, ISO 27001 Internal/Lead Auditor

07

ISO 27001 Certified Lead Implementer

Objetivos:

Compreender e implementar um sistema de gerenciamento de segurança da informação como líder de implementação, focado em riscos corporativos, incluindo políticas, planos, procedimentos, processos e recursos.

Habilidades desenvolvidas:

Desenvolver habilidades para identificar, avaliar e gerenciar informações Gerenciar riscos de segurança da informação, implementar processos sistemáticos, desenvolver planos de tratamento, estabelecer políticas alinhadas com a estratégia organizacional e integrar requisitos SGSI.

Perfis apropriados:

Administradores de sistemas, engenheiros de rede, especialistas em segurança da informação, analistas de segurança, analistas de segurança cibernética, consultores de segurança cibernética, líderes DE TI, desenvolvedores de software, TI e segurança da informação Desenvolvedores de software, profissionais DE TI e administradores de sistemas de segurança da informação, engenheiros de rede, especialistas em segurança da informação, analistas de segurança, auditores internos e externos, profissionais de conformidade.

Benefícios:

- Fornecer explicação e orientação sobre a ISO/IEC 27001 com base na ISO/IEC 27003:2017 para a concepção e implementação de um sistema de gestão de segurança (SGSI).
- Entender os componentes necessários para determinar o estado atual de um sistema de gerenciamento de segurança da informação para servir como um sistema de gerenciamento de segurança da informação para servir como ponto de partida para avaliar a conformidade com a ISO 27001 de conformidade com a norma ISO 27001
- Determinar a implementação dos requisitos necessários para alcançar um sistema compatível que passará por terceiros

Requisitos *(opcional)*:

Cybersecurity Awareness, ISO 27001 Foundation, ISO 27001 Internal/Lead Auditor

Impulsione sua carreira em segurança cibernética!

CertiProf®

info@certiprof.com

1401 Sawgrass - Corporate Parkway
Sunrise, FL 33323

+1-305-676-7373

@Certiprof @CertiProf @Certiprof_llc @Certiprof CertiProf LLC