

Sistemas Computacionais e

Segurança

Annely Desireé Junemann- 824217739

Francisco Alexandre dos Santos Melo- 824219751

Larissa da Silva Maschio- 824221401

Natasha Melo de Sousa- 82429222

Yasmin Victória Alves de Sousa- 824210011

ANO 2024

A certificação CISM (Certified Information Security Manager) é reconhecida internacionalmente e atesta profissionais que projetam e gerenciam sistemas de segurança em uma organização. Iremos explorar todos os aspectos desta certificação.

O ideal é ter no mínimo 5 anos de experiência em alguma área de gestão de segurança da informação. Seja ela: Governança de Segurança da Informação; Gerenciamento de Riscos da Informação; Desenvolvimento e Gerenciamento de Programas de Segurança; ou Gestão de Incidentes e Resposta.

* **Requisitos para certificação**

Dentre os requisitos para certificação está a aprovação no exame CISM, que predomina quatro diretrizes: Governança de Segurança da Informação, Gestão de Risco de Segurança da Informação, Gestão de Incidentes de Segurança e Desenvolvimento e Gestão de Programas de Segurança.

* .**Setores de atuação**

A certificação CISM é utilizada em diversas categorias, como:

* Tecnologia da Informação: Empresas que prestam serviços para consultorias de TI.
* Finanças e Bancos: Instituições financeiras, bancos que necessitam de robustas práticas de segurança para proteger dados sensíveis.
* Saúde: Organizações de saúde que precisam garantir a proteção de informações pessoais e registros médicos.
* Governo: Agências governamentais que requerem altos padrões de segurança para proteger informações públicas.
* Indústria: Empresas que buscam proteger a propriedade intelectual e dados operacionais.
* **Benefícios**

Os benefícios de se obter essa certificação são muitos, dentre eles o reconhecimento profissional, credibilidade, aprimoramento da carreira, conformidade com padrões internacionais.

* **Diferenças na abordagem de gestão de risco**

A CISM tem o seu foco principal direcionado a profissionais responsáveis pela gestão e segurança da informação em uma organização. Certifica os indivíduos com habilidades em desenvolver e gerenciar programas eficazes de segurança da informação. Os funcionários certificados tentam ao máximo evitar riscos de ataques através da engenharia social e também propondo possíveis soluções quando não conseguem evitá-los.

A certificação CISSP (*Certified Information Systems Security Professional)* é amplamente reconhecida na área de segurança da informação. Veremos os principais aspectos dela.

* **Requisitos para Certificação**:

• Experiência: É necessário ter pelo menos 5 anos de experiência em segurança da informação, abrangendo pelo menos 2 dos 8 domínios do CISSP, como Segurança de Rede, Segurança de Software, e Gestão de Identidade e Acesso.

• Certificação: Aprovação no exame CISSP, que abrange os 8 domínios: Segurança e Gestão de Risco; Segurança de Ativos; Arquitetura e Engenharia de Segurança; Segurança de Rede e Comunicação; Gerenciamento de Identidade e Acesso; Avaliação e Teste de Segurança; Operações de Segurança; e Segurança no Desenvolvimento de Software.

• Código de Ética: Comprometimento com o código de ética da (ISC)².

• Educação Continuada: Para manter a certificação, é necessário acumular créditos de educação contínua anualmente.

* **Setores de Atuação:**

A certificação CISSP é aplicável em diversas áreas, como:

• Tecnologia da Informação: Empresas de TI e segurança cibernética.

• Finanças: Instituições financeiras e bancos, que necessitam proteger dados sensíveis.

• Saúde: Organizações de saúde que precisam assegurar a proteção de informações pessoais e registros médicos.

• Governo: Agências governamentais que requerem altos padrões de segurança para informações públicas.

• Indústria: Empresas que buscam proteger a propriedade intelectual e dados críticos.

* **Benefícios da Certificação:**

A obtenção da certificação CISSP oferece vantagens significativas, incluindo:

• Reconhecimento Global: Uma das certificações mais respeitadas na área de segurança da informação.

• Melhores Oportunidades de Emprego: Facilita a progressão na carreira em cargos de liderança.

• Salários Mais Altos: Profissionais certificados costumam ter remunerações superiores.

• Valorização da Carreira: Demonstra compromisso e conhecimento profundo em segurança da informação.

4. Gestão de Riscos:

A abordagem da CISSP em gestão de riscos inclui:

• Foco Abrangente: Considera a segurança da informação como parte integral da estratégia organizacional.

• Análise Contínua: Promove a adaptação de controles de segurança.

• Conformidade: Garantir que as práticas de segurança atendem às leis e regulamentos aplicáveis.

****

Referências:

<https://www.linkedin.com/pulse/certifica%C3%A7%C3%B5es-cisa-e-cism-elevando-carreira-em-ti-seguran%C3%A7a-silva-afh5f/>

<https://canaltech.com.br/>

<https://www.kasolution.com.br/>

<https://www.infosec.com.br/>

<https://formuladascertificacoes.com.br/>

<https://engage.isaca.org/brasiliachapter/certificacao/certificacoesisaca/cism#:~:text=A%20Certifica%C3%A7%C3%A3o%20em%20Gest%C3%A3o%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o,e%20gerenciam%20programas%20de%20seguran%C3%A7a%20das%20informa%C3%A7%C3%B5es%20corporativas>

<https://carreiraemti.com.br/glossary/certificacao-cism-certified-information-security-manager/>

<https://www.codia.com.br/glossario/certificacao-cism-certified-information-security-manager/>