# Guia de Estudos

*Certificação TI Safe CASE (Certified Automation Security Engineer) v. 1.0*
*Revisada em 09/05/2012*

PÁGINA INTENCIONALMENTE DEIXADA EM BRANCO

**Prefácio**

Este documento tem o objetivo de apresentar o “Guia de estudos para o exame CASE”.

**Propriedade intelectual**



**Aviso**

Este documento tem o objetivo de ser completo e claro. A TI Safe não se responsabiliza por quaisquer danos, perdas financeiras ou de negócios resultantes de omissões ou imperfeições contidas neste. Este documento está sujeito a alterações sem aviso prévio. Recomenda-se contactar a TI Safe para obter atualizações e/ou informações adicionais.

**Contato**

A TI Safe disponibiliza diferentes canais de comunicação com seus clientes, fornecedores e associados:

Rio de Janeiro

Centro Empresarial Cittá America - Barra da Tijuca
Av. das Américas, 700, bloco 01, sala 331
CEP - 22640-100 - Rio de Janeiro, RJ – Brasil
Telefones: +55 (21) 2173-1159
Fax: (21) 2173-1165

São Paulo

Rua Dr. Guilherme Bannitz, nº 126 - 2º andar
Cj 21, CV 9035 - Itaim Bibi
CEP - 04532-060 - São Paulo, SP - Brasil
Telefones: +55 (11) 3040-8656
Fax: (11) 3040-8656

e-mail: contato@tisafe.com
website: www.tisafe.com
skype (somente voz): ti-safe
Twitter: @tisafe

**Certificado de documentação de alterações**

| Versão | Data | Autor | Descrição |
|---|---|---|---|
| 1.00 | 09.05.2012 | Marcelo Branquinho | Geração do primeiro documento |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Prefácio

Quando o exame CASE foi desenvolvido, os especialistas no assunto trabalharam juntos para definir o papel que o indivíduo certificado irá exercer. Eles definiram todas as tarefas e conhecimentos que este profissional precisará ter para implantar políticas e arquiteturas seguras para redes e sistemas de automação. Estes conceitos formam a base dos domínios de conhecimento que o candidato precisará estudar para solucionar as questões que surgirão no exame da certificação.

Este guia servirá como linha base para a revisão dos conhecimentos necessários para a prova. Você sabe como projetar arquiteturas seguras? Você conhece os riscos aos quais uma rede de automação está exposta? Conhece as normas de segurança utilizadas em redes industriais? Caso não esteja confortável em responder a estes questionamentos é provável que você tenha que estudar mais antes de realizar o exame. Existe 95% de possibilidade que exista uma pergunta no exame de certificação sobre algum destes temas.

Depois de revisar os objetivos e estar confortável para um teste, baixe e complete o simulado que está disponível no website. Ele poderá conter questões reais do exame e servirá como uma base para que você verifique como está o seu nível de conhecimento para o exame. Caso obtenha menos de 7 acertos nas 10 questões, estude um pouco mais.

**Nome do Exame**

TI Safe CASE (*Certified Automation Security Engineer*)

**Área do conhecimento (de acordo com a tabela do CNPq)**

Ciências Exatas e da Terra > Ciência da Computação (1.03.00.00-7) > Sistemas de Informação (1.03.03.04-9)

**Justificativa da oferta**

Profissionais qualificados são a mais importante peça no quebra-cabeça de segurança de automação. Os candidatos que alcançam uma certificação que exige proficiência além do conhecimento obtido com livros é um valioso método para diferenciar os níveis de qualificação destes profissionais.

Benefícios da certificação TI Safe CASE para o profissional:

- Demonstra o conhecimento teórico de segurança de redes industriais e SCADA.
- Confirma o compromisso com a profissão de segurança da informação.
- Serve como um diferencial no recente mercado de trabalho de segurança de automação industrial.
- Fornece acesso a uma rede de pessoas certificadas.

Benefícios da certificação TI Safe CASE para as empresas:

- Estabelece parâmetro para o nível de habilidade necessário para profissionais de segurança industrial.
- Garante que os indivíduos possuam as competências para realizar o trabalho.
- Permite o acesso a uma rede de especialistas no assunto.

**Metodologia do Exame**

A prova para a certificação CASE é presencial e composta de 60 perguntas de múltipla escolha que devem ser resolvidas pelo candidato em 90 minutos. As questões têm pesos diferentes e o aluno será aprovado caso obtenha quantidade de acertos igual ou superior a 70% do valor total dos pontos atribuídos ao exame. Em caso de aprovação o aluno receberá o certificado CASE por e-mail e seu nome poderá ser verificado em listagem no site da TI Safe.
Os certificados tem 2 anos (24 meses) de validade a partir de sua data de emissão.
As provas do CASE serão realizadas sempre na tarde do último dia de aula de cada turma da Formação de Segurança em Automação Industrial, no mesmo local onde o treinamento foi realizado.
As questões da prova estão em língua portuguesa e o aluno não poderá consultar qualquer fonte, seja em formato impresso ou eletrônico. Todo o material necessário para o preenchimento da prova será dado no local.

**Bibliografia recomendada**

Recomendamos que os candidatos ao exame CASE busquem complementar seus conhecimentos através da leitura dos seguintes livros:

- "*Securing SCADA Systems*", escrito por Ronald L. Krutz – Editora Wiley
- "*Techno Security's Guide to Securing SCADA: A Comprehensive Handbook On Protecting The Critical Infrastructure*" escrito por Jack Wiles, Ted Claypoole, Phil Drake, Paul A. Henry, Lester J. Johnson Jr, Sean Lowther, Greg Miles, Marc Weber Tobias e James H. Windle – Editora Syngress
- "*Protecting Industrial Control Systems from Electronic Threats*", escrito por Joseph Weiss. Editora Momentum Press.
- "*Inside Cyber Warfare*", escrito por Jeffrey Carr. Editora O´Reilly.

Todos os livros acima podem ser adquiridos através do site amazon.com.

**Domínios de conhecimento:**

**I - Introdução às redes Industriais e sistemas de controle e monitoramento (SCADA):** conhecimento do histórico dos sistemas industriais e sua evolução até os sistemas SCADA.
Tópicos relacionados:

- Histórico da Automação industrial.
- Arquitetura de sistemas industriais.

**II - Infraestruturas Críticas e Cyber-terrorismo:** definição do que são infraestruturas críticas e sua importância para a nação. Definição de cyber-terrorismo. Compreensão das principais técnicas utilizadas por invasores para atacar servidores dentro de uma redes de computadores.
Tópicos relacionados:

- O que são Infraestruturas críticas?
- Cyber-terrorismo.
- Ataques a redes e sistemas industriais.
- Anatomia de uma invasão
- Principais ataques: levantamento de perfil, *Sniffing* de rede, *PortScan, Brute force*, *DoS/DDoS*, ARP-*Poison*, *Spoofing*, *Man-in-the-Middle*.
- O Impacto de uma invasão.

**III – Governança para redes industriais:** conhecimento das principais normas internacionais que balizam a implantação de políticas e procedimentos de segurança da informação em redes corporativas e industriais. Conhecimentos de conceitos de governança em redes industriais e de como desenvolver um plano de continuidade de negócios (PCN).
Tópicos relacionados:

- Normas de referência
    - A norma ANSI/ISA 99
    - A norma NIST 800-82
- Desenvolvimento e implantação de Políticas de Segurança para áreas de automação.
- Desenvolvimento e implantação de um Plano de Continuidade de Negócios (PCN).

**IV – Análise de riscos em redes industriais:** como elaborar uma análise de riscos segundo definido pelo NIST no documento SP800-30. Conhecimento das principais vulnerabilidades e ameaças a sistemas industriais segundo as normas de segurança e avaliação do risco caso estas ameaças se concretizem.
Tópicos relacionados:

- Definição de análise de riscos
- Etapas de uma análise de riscos:
    - Etapa 1: Inventário
    - Etapa 2: Análise
    - Etapa 3: Avaliação
    - Etapa 4: Treinamento

- Gerenciamento do risco
- Vulnerabilidades e ameaças a sistemas industriais
- Aspectos específicos para análises de riscos em ambientes industriais.

**V - Malware em redes industriais e sistemas de controle**: conhecimento de conceitos sobre os diferentes tipos de Malware, como eles entram em uma rede industrial e rapidamente se espalham. Estratégias para uso de antivírus e atualização de patches em computadores da rede de automação. Metodologia para a desinfecção de uma rede que tenha sido contaminada por Malware.
Tópicos relacionados:

- Principais tipos de Malware.
- Vias de infecção em redes industriais.
- Principais worms e como eles se espalham em uma rede de automação.
- Como construir um worm com o Metasploit.
- Estratégias para uso de antivírus e atualização de patches em computadores da rede de automação.
- Problemas típicos para desinfecção de redes contaminadas
- Metodologia para desinfecção
    - Ciclo para desinfecção
    - Isolamento e diagnóstico
    - Limpeza
    - Segurança de borda
    - Restauração de sistemas e
    - Controle de acesso
- Monitoramento

**VI - Segurança de perímetro em redes de automação:** Firewalls e outras soluções para segurança de perímetro em redes de automação. Segurança de redes sem fio em ambientes industriais.
Tópicos relacionados:

- Firewalls.
- Arquiteturas de Firewalls e implantação de DMZ.
- Políticas de Firewall.
- VLANs.
- Sistemas de Detecção e Prevenção de Intrusos (IDPS).
- Segurança em redes sem fio industriais.

**VII - Criptografia em redes industriais**: fundamentos de criptografia simétrica e assimétrica, e suas aplicações em segurança de redes.
Tópicos relacionados:

- Introdução à criptografia.
- Criptografia Simétrica.
- Criptografia Assimétrica.
- Aplicações em redes corporativas e industriais.

**VIII - Controle de acesso em sistemas SCADA**: conceitos e práticas para definir controles de acesso visando o estabelecimento da segurança no acesso à redes  industriais. Métodos para a implantação de políticas de controle de acesso e diretivas de grupo (GPOs) utilizando o Active Directory. Dispositivos usados para estabelecer múltiplos fatores de autenticação (tokens OTP, biometria, entre outros).
Tópicos relacionados:

- Controle de acesso: Conceitos, Metodologias e Técnicas.
- Ameaças ao controle de acesso: identificação, avaliação, resposta e prevenção.
- Implantação de políticas de controle de acesso.
- O Active Directory e diretivas de grupo (GPOs).
- Mecanismos de autenticação: Biometria, OTP, Smartcards e Tokens USB.

**IX - Implantando o CSMS (ANSI/ISA-99) na prática**: estratégia de defesa em profundidade preconizada pela norma ANSI/ISA-99. Metodologia para a a implantação do CSMS. Soluções disponíveis no mercado e novas tecnologias em fase de pesquisa para a segurança industrial.
Tópicos relacionados:

- Estratégias de defesa em profundidade.
- Modelo de Zonas e Conduítes.
- Soluções de mercado.
- Soluções open source.
- Novas tecnologias para segurança industrial.

PÁGINA INTENCIONALMENTE DEIXADA EM BRANCO