CATÁLOGO DE CURSOS

ANTEBELLUM

psi Testing Excellence

iapp

CompTIA

EXIN

Pearson VUE Authorized Test Center

Com 25 anos de experiência em Capacitação de recursos em Segurança da Informação, **a Antebellum foi fundada em 1997**, a partir da observação de um grupo de instrutores e professores de Tecnologia e Segurança da Informação, sobre as mudanças nos cenários nacional e internacional e as dificuldades encontradas pelos profissionais destas áreas para a contratação de treinamentos que se encaixassem em suas agendas e orçamentos.

Diante deste contexto os primeiros cursos foram criados, apresentando seus conteúdos de forma aprofundada e objetiva, sendo claramente notados pelo material do aluno, transformando-o em uma fonte de referências futuras e apoio ao estudo para os exames de certificação.

O pioneirismo do fundado, a qualidade dos instrutores e o extenso número de certificações de reconhecimento internacional, resultou em aproximação e parceria com as maiores autoridades no segmento de Tecnologia e Segurança da informação mundial, entregando ao mercado brasileiro, conteúdo de qualidade diferenciada, com constantes atualizações.

Algumas das conquistas realizadas pela Antebellum:

- Foi a primeira empresa no mundo a ministrar os treinamentos oficiais da PCI Council, além de ser a única empresa ter seus treinamentos ministrados em Português Brasileiro;
- Foi primeira empresa nas Américas a ministrar os treinamentos oficiais da EXIN, para a formação e certificação DPO (Data Protection Officer), baseada na GDPR da Europa;
- Em 2019 oficializou a parceria com a IAPP (international Association of Privacy Professionals), podendo ministrar treinamentos para as certificações CDPO-BR, CIPM, CIPP/E, além de ser a única parceira a oferecer o treinamento CIPT no Brasil.

Assim, ao longo desta jornada, a Antebellum acumulou experiência em capacitação de recursos em segurança da informação, tendo treinado milhares de profissionais em todo o país.

"Porque antes de tudo mais, preparar-se é o segredo do sucesso."

Henry Ford

Missão

Preparar os Profissionais com as habilidades e competências necessárias para enfrentar os desafios da tecnologia da informação, proteção e privacidade de dados

Visão

Inovar, Engajar, Transformar!

A Antebellum é movida pela paixão pelas pessoas, ajudando a transformar a carreira de cada um de seus estudantes, inovando a cada dia para engajá-los em um ciclo vitorioso de aprendizado.

Assim, nós da Antebellum trabalhamos com pessoas, com seus sonhos profissionais e suas realizações, ao longo destes 25 anos, inúmeros sonhos realizados, novos caminhos se abriram e diversas foram as conquistas, pois buscamos sempre potencializar pessoas e valorizar negócios.

Então... Qual é seu sonho profissional???

A Antebellum tem a filosofia de associar-se a empresas no exterior para trazer os melhores treinamentos em Tecnologia da Informação e Segurança da Informação para a América Latina.

A Antebellum foi a única empresa no mundo a receber a autorização para ministrar os treinamentos oficiais do PCI Council.

October 02, 2012 10:15 AM Eastern Daylight Time

PCI Security Standards Council anuncia disponibilidade de treinamento em português no Brasil. Nova organização sócia brasileira oferecerá treinamento de alta qualidade em PCI com instrutor na língua local.

O PCI Security Standards Council se associará à Antebellum, uma empresa brasileira líder em treinamento em TI, para oferecer cursos orientados por instrutores para o programa de Internal Security Assessor (ISA) e classe de Conscientização de PCI.

Todos os materiais e discussões na sala de aula serão fornecidos em português.

Fonte: http://www.businesswire.com/news/home/20121002006183/pt

DEPOIMENTO

"Temos o prazer de anunciar nossa primeira parceria internacional de treinamento e estamos muito satisfeitos em associar-nos à Antebellum, uma organização com conhecimento profundo dos padrões da PCI"

"A educação é um elemento imprescindível na segurança de pagamentos, e o Conselho da PCI está comprometido com a expansão de oportunidades de treinamento da PCI globalmente"

Bob Russo,
General Manager, PCI SSC

CLOUD COMPUTING

O Cloud Computing tem se tornado popular entre empresas e pessoas devido aos seus benefícios, onde podemos citar os principais: redução de custos, total controle e centralização da informação, elasticidade, performance, armazenamento, segurança, etc. Nossos cursos abrangem desde os fundamentos da computação em nuvem até os requisitos técnicos para aumentar a segurança dentro desses ambientes.

Ser um especialista MultiCloud potencializa exponencialmente sua carreia profissional e aumenta suas chances no mercado.

O profissional de TI tem que entender que migrar os serviços de TI para um determinado provedor de nuvem, hoje, nada mais é do que fazer a sua obrigação.

O mercado hoje é dominado por três mega grandes provedores de nuvem, AWS, Azure e Google. Cada provedor de nuvem tem suas especialidades e uns são melhores e mais baratos em alguns serviços do que os outros e o arquiteto de nuvem precisa entender essas diferenças e saber como utilizá-las em projetos de migração ou expansão é fundamental para se tornar um arquiteto MultiCloud.

E é exatamente isso que o treinamento MultiCloud Foundation faz — prepara o profissional para conhecer os detalhes de cada provedor de nuvem, como utilizar os melhores serviços de cada um para obter os benefícios comerciais e tecnológicos que incluem o aumento da inovação, o acesso ao ambiente especializado e a tirar o máximo da capacidade de cada provedor ao dimensionar a computação e o armazenamento à medida que a empresa cresce.

A Antebellum preparou o treinamento Multicloud Foundation especialmente para o profissional que precisa entender a nuvem do zero e a evoluir para o nível de arquiteto em AWS, Azure e Google.

Por que fazer este curso?

Este curso fornecerá uma visão geral dos conceitos fundamentais de Cloud Computing (MultiCloud) das principais plataformas em nuvem – AWS, Azure e Google Cloud, e na compreensão de sua arquitetura, desenho, implantação e sua incorporação à organização. Além disso, você poderá:

- Compreender as terminologias e os conceitos de Cloud Computing
- Entender os conceitos atrás das estruturas de nuvem
- Navegar pelo console de gerenciamento de nuvem
- Entender como implementar as medidas de segurança em nuvem
- Utilizar, conhecer e criar os tipos de armazenamento em nuvem
- Conhecer as opções de computação e rede em nuvem
- Entender as opções de implantação e gerenciamento em nuvem
- Entender o que são e como utilizar discos em nuvem

Objetivos deste curso

Preparar o profissional para conhecer os detalhes de cada provedor de nuvem, como utilizar os melhores serviços de cada um para obter os benefícios comerciais e tecnológicos que incluem o aumento da inovação, o acesso ao ambiente especializado e a tirar o máximo da capacidade de cada provedor ao dimensionar a computação e o armazenamento à medida que a empresa cresce.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 24 horas (online, ao vivo) de treinamento + dezenas de vídeos com as particularidades de cada plataforma, além de scripts de laboratório detalhados

Pré-requisitos

- É recomendável ter conhecimento sobre operações básicas de computador

Público-alvo

- Profissionais de TI
- Gerentes de TI
- Executivos de TI

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

PAULO COELHO

INSTRUTOR

AWS | CCDA | CCNA | CCNP | CNE | CNI | CWNA | MCSA | VMware

Certificações do curso

Programa do curso

MÓDULO 01 | Introdução ao ambiente MultiCloud

- O limite do modelo atual de TI
- Modelo tradicional de gestão de TI
- Definições da Cloud
- Modelos de implantação de cloud computing
- Modelos de serviços
- Orquestração X Automação
- Conceitos de escalabilidade
- Provedores de Cloud
- Aws, Azure e Google Cloud
- Diferenças de serviços AWS, Azure e Google Cloud

MÓDULO 02 | AWS Cloud

- Introdução à plataforma AWS
- Principais Componentes da nuvem AWS
- IAM AWS
- Storage S3
- Computação na AWS
- Network e AWS
- Banco de dados
- Alta disponibilidade
- Containers, Serverless e Kubernetes
- Serviços cognitivos
- Laboratórios práticos: Acessando o Console, entendendo e criando usuários no IAM, Criar um bucket no S3, Criando uma instancia no EC2, criando o VPC, utilizando a CLI na AWS, Estendendo a VPC para instalar um Banco de Dados, Alta disponibilidade na AWS, Serviços AWS, Serviços Cognitivos na AWS.

MÓDULO 03 | Azure Cloud

- Introdução à plataforma Azure
- Principais Componentes da nuvem Azure
- IAM AWS
- Azure Blob Storage
- Computação no Azure
- Network e VPC
- Banco de dados
- Alta disponibilidade
- Containers, Serverless e Kubernetes
- Serviços cognitivos no Azure
- Laboratórios práticos: Grupos de gerenciamento do Azure, criando usuários no Azure,Grupos de recursos, criando uma VNet, criando uma conta de armazenamento, criando uma VM, Criando uma solução sem servidor usando uma Função do Azure, Criando uma solução sem servidor usando um aplicativo lógico do Azure, Criando uma solução de IA usando um serviço de bot, criando recursos usando a CLI do Azure do Cloud Shell, explorando o Azure Service Health

MÓDULO 04 | Google Cloud

- Introdução à plataforma GCP (Google Cloud Platform)
- Principais Componentes da da nuvem GCP
- IAM GCP
- Cloud Storage
- Computação na GCP
- Network e VPC
- Banco de dados
- Alta disponibilidade
- Containers, Serverless e Kubernetes
- Serviços cognitivos
- Laboratórios: Acessando o Console GCP, entendendo e criando usuários no IAM, Criar armazenamento no cloud storage na GCP, Criando uma instancia VM, criando um VPC, utilizando a CLI na GCP, instalar um Banco de Dados, entender alta disponibilidade na plataforma GCP, Serviços GCP, Serviços Cognitivos na GCP.

DEVSECOPS

O DevSecOps incorpora automaticamente a segurança em todas as fases do ciclo de vida de desenvolvimento de software, permitindo o desenvolvimento de software seguro na velocidade do Agile e do DevOps.

A Análise de Pacotes em Redes e Aplicações aumenta sua capacidade de entender os pacotes e os protocolos e é uma habilidade crítica para administradores de rede e de sistemas, engenheiros de rede, desenvolvedores, investigadores forenses, analistas de SOC, engenheiros de segurança, profissionais de suporte e programadores.

Os pacotes apresentam a radiografia de todos os componentes operando junto, como aplicações, dispositivos de rede, servidores e protocolos. Você precisa aprender como identificar os pacotes desses componentes e suas principais características.

Por que fazer este curso?

Este curso apresentará os conceitos fundamentais, as metodologias e ferramentas necessárias para análise de redes e aplicações, tráfego de rede e protocolos em ambientes de TI e TA de qualquer tamanho. Além disso, você poderá :

- Conhecer os 04 pilares da Análise de Redes, Protocolos e Aplicações
- Calcular a latência, a utilização de banda e o Throughut da rede
- Analisar e entender redes WLan (Wi-Fi)
- Entender o Tráfego de virtualização de armazenamento

Objetivos deste curso

Capacitar profissionais para analisar aplicações nas redes de trabalho baseados na ferramenta de análise de protocolos, determinar pontos de falha e implementar segurança de infraestrutura. Elaborar VPN e garantir sua segurança.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.
- Laboratórios práticos: Laboratórios práticos para desenvolver e testar suas habilidades examinando centenas de capturas que irão fortalecer os conceitos que você aprendeu.

Carga-horária

- 40 horas de treinamento (online, ao vivo)

Pré-requisitos

- É recomendável ter conhecimento básicos de rede

Público-alvo

- Profissionais de suporte em TI
- Desenvolvedores
- Administradores de sistema
- Engenheiros de rede
- Investigadores forenses
- Analistas de SOC
- Engenheiros de software
- Programadores em geral

Instrutores

PAULO COELHO

INSTRUTOR

AWS | CCDA | CCNA | CCNP | CNE | CNI | CWNA | MCSA | VMware

Certificações do curso

Não há certificações disponíveis para este curso

Programa do curso

MÓDULO 01 | Introdução à Análise de Redes
- As 10 verdades sobre análise de rede
- Entendendo análise de rede
- Por que as redes ficam lentas?
- Metodologia de troubleshooting
- Modelo OSI e seus elementos
- Pilhas de protocolos comerciais
- Tráfegos Windows e Linux
- Identificando os problemas pelas camadas
- Laboratório prático

MÓDULO 02 | Entendendo os analisadores de protocolos
- O que são os analisadores de protocolo
- Tipos de analisadores
- Posicionamento de um analisador
- TAP X SPAN
- Analisadores por software
- Analisadores por hardware
- Laboratório prático

MÓDULO 03 | Entendendo o Wireshark
- O que é o Wireshark
- Interface básica do Wireshark
- Opções de captura
- Filtros
- Analisando TCP e UDP streams
- Estatísticas
- Analisando telefonia
- Como construir uma probe ou appliance para análise de redes
- Laboratório prático

MÓDULO 03 | Filtros Wireshark
- Componentes do Wireshark
- Função dos filtros
- Filtro de captura
- Filtro de display
- Criando filtros com a interface gráfica
- Aplicando os filtros na análise de redes e aplicações
- Laboratório prático

MÓDULO 05 | Linhas de comando Wireshark

- Comandos de linha Wireshark
- Funções dos comandos de linha
- Configurar o path
- Descrição de cada comando
- Aplicações dos comandos de linha na análise de redes e aplicações
- Laboratório prático

MÓDULO 06 | Entendendo a tecnologia Ethernet

- Camada física
- A influência da certificação do cabeamento no tráfego de rede
- Frames empregados na tecnologia Ethernet
- Tecnologias de 10Mbps a 40Mbps
- O CSMA/CD
- Tráfego half e full-duplex
- Erros na camada 2
- Tráfegos Unicast, Multicast e Broadcast
- Indicadores de desempenho em uma rede Ethernet
- Laboratório prático

MÓDULO 07 | Entendendo o tráfego de Vlan

- Conceitos de uma rede hierárquica
- Switches Blocking x Non-Blocking
- Métodos de Switching
- Fundamentos de VLAN
- VLAN Tagging
- Q-in-Q VLANs
- Laboratório prático

MÓDULO 08 | Entendendo o tráfego de Spanning Tree

- Exigências da camada core
- Principais impactos causados pela redundância
- Protocolo Spanning-Tree
- Como o Spanning-tree opera
- Terminologia Spanning-tree
- Procolo Rapid Spanning-tree
- Laboratório prático

MÓDULO 09 | Entendendo os protocolos IPV4

- A pilha de protocolos IPv4
- Protocolo ARP
    - Por que o ARP é necessário
    - Principais características do ARP
    - Descrever o tráfego de ARP
    - Identificação de IPs duplicados
    - Entender o RARP
    - Tráfego ARP que deve ser observado
    - Principais assinaturas
    - Laboratório prático

- Protocolo IP
    - Entendendo o Best Efford
    - Datagrama IP
    - Type of service
    - Fragmentação IP
    - IP Options
    - Principais assinaturas
    - Laboratório prático

- Protocolo ICMP
    - Entender a função do protocolo ICMP
    - Descrever as principais mensagens do protocolo ICMP
    - Descrever a estrutura de um pacote ICMP
    - Utilitários que empregam o ICMP
    - Principais mensagens ICMP
    - Principais assinaturas
    - Laboratório prático

- Protocolo TCP/UDP
    - O que faz a camada de transporte?
    - Portas TCP/UDP
    - Socket e Winsock
    - Protocolo TCP
    - Estrutura do segmento TCP
    - Flags TCP
    - Como os hosts se comunicam com TCP
    - Processo de estabelecimento de sessão
    - State Machine do protocoloTCP
    - Protocolo UDP
    - Principais assinaturas
    - Laboratório prático

MÓDULO 10 | Entendendo o tráfego IPV6

- Introdução ao IPv6
- Características e benefícios do IPv6
- Diferenças entre IPv4 e IPv6
- Terminologia IPv6
- Endereçamento IPv6
- Datagrama IPv6
- ICMPv6
- Principais Serviços IPv6
- Principais assinaturas
- Laboratório prático

MÓDULO 11 | Entendendo as aplicações IPV4/IPV6

- Serviço DHCP
- Serviço HTTP – Web Server
- Resolução de nomes com DNS
- Servidor FTP
- Servidor de correio SMTP
- Protocolo POP3
- Protocolo IMAP4
- Telnet
- Servidor TFTP
- Laboratórios práticos

MÓDULO 12 | Protocolo TCP Avançado

- As características avançadas do protocolo TCP
- Entendendo as retransmissões
- Timeouts de redes
- Controle de fluxo e janelamento
- Entendendo os Acks
- Zero Window
- Entendendo o congestionamento da rede
- Laboratório prático

MÓDULO 13 | Protocolos Windows

- Entendendo a pilha de protocolos Windows
- Protocolos Kerberos e AD
- Protocolo SSDP
- Protocolo LLNM
- Tráfego netbios
- SMB/CIFS
- RDP
- Principais assinaturas
- Laboratório prático

MÓDULO 14 | Entendendo o tráfego de Banco de Dados

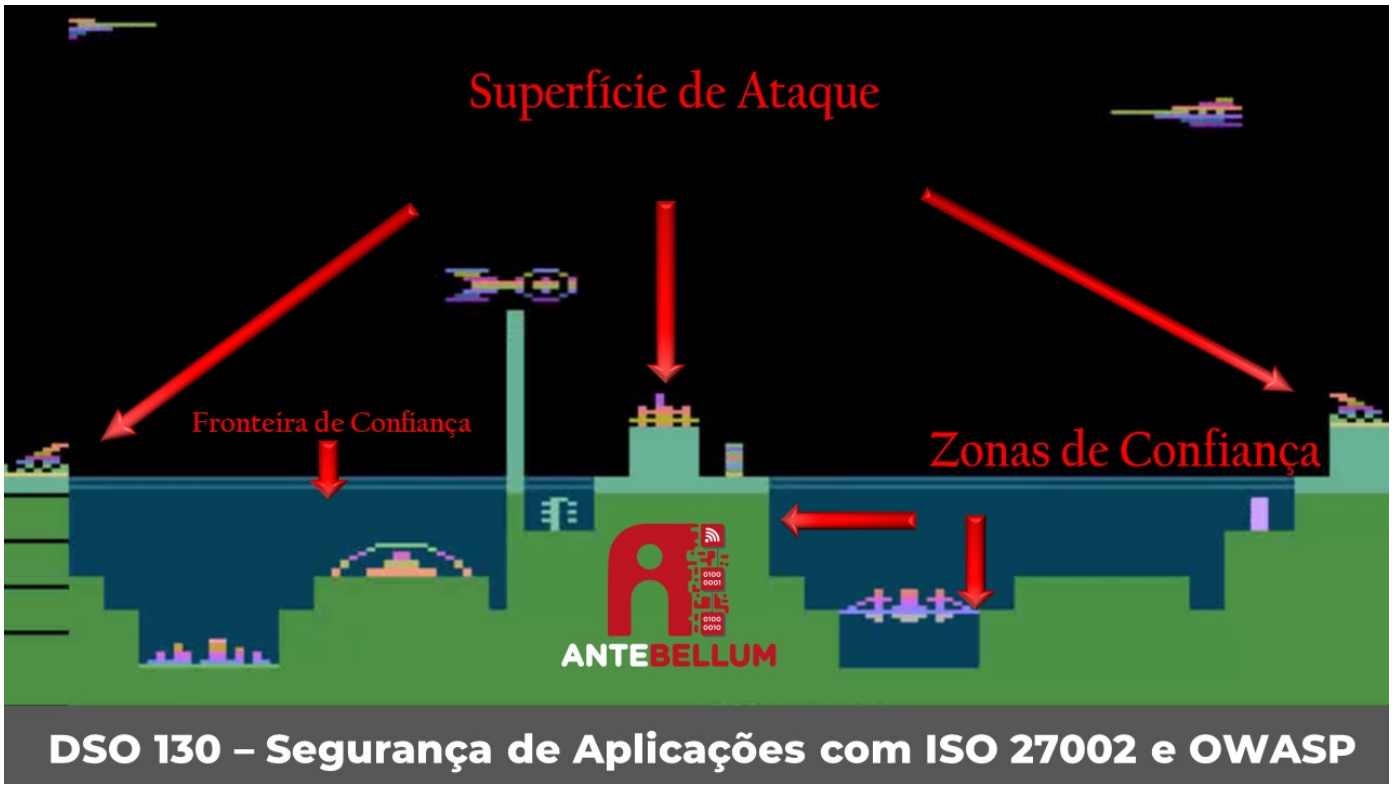
MÓDULO 15 | Entendendo o tráfego de virtualização e armazenamento
- Cluster virtualizado
- Vxlan
- Tráfego de armazenamento
- Principais assinaturas
- Laboratório prático

MÓDULO 16 | Caracterizando o tráfego de rede
- Padrões do tráfego de rede
- Por que a rede fica lenta?
- Entendendo a latência
- Dissecando os tempos da LAN
- Caracterização de serviços
- Tarefas que devem ser realizadas
- Caracterizar o tráfego
- Padrões de tráfego das aplicações
- Ferramentas do Wireshark
- Entendendo os temporizadores
- Laboratório prático

MÓDULO 17 | Analisando o tráfego de segurança
- Scan SYN
- NMAP
- Fingerprinting
- Manipulação de tráfego
- Malware
- Principais assinaturas
- Laboratório prático

MÓDULO 18 | Construindo um relatório
- Porque fazer um relatório de análise
- Dez dicas sobre relatórios
- Ferramentas
- Usando WireShark
- Modelo de Relatório

MÓDULO 19 | Outras soluções de Análise de Tráfego e Aplicações
- Monitoramento SNMP
- APM
- Análise de logs
- Laboratório prático



DSO 130 – Segurança de Aplicações com ISO 27002 e OWASP

Desenvolvimento Seguro é uma necessidade!

Cada vez mais, é imprescindível para as empresas que os desenvolvedores criem código seguro, de acordo com as melhores práticas de mercado. O curso Segurança de Aplicações com ISO 27002 e OWASP tratará destes fundamentos e práticas.

Por que fazer este curso?

Este curso te mostrará necessidade de segurança em código, técnicas de verificação de entrada, autenticação e criptografia mias seguras. Além disso, você poderá:

- Revisar itens de configuração
- Prevenir ataques de injeção de código malicioso
- Revisar sua API Rest ou Soap
- Aprender mais sobre Proteção de Dados segundo a OWASP

Objetivos deste curso

Preparar o profissional para desenvolver códigos seguros e mostrar a necessidade de aplicar técnicas de autenticação e criptografia mais seguras, de acordo com a ISO 27002, além de apresentar a Proteção de Dados segundo a OWASP

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 20 horas (online, ao vivo) de treinamento

Pré-requisitos

- Não há

Público-alvo

- Desenvolvedores
- Arquitetos de TI
- Coordenadores de TI
- Profissionais de TI
- Profissionais de Segurança da Informação

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

Certificações do curso

Não há certificações disponíveis para este curso

Programa do curso

MÓDULO 01 | Introdução

MÓDULO 02 | OWASP top 10

MÓDULO 03 | Quebra de Controle de Acesso

MÓDULO 04 | Criptografia

MÓDULO 05 | Injeção

MÓDULO 06 | Design Inseguro

MÓDULO 07 | Configuração Insegura

MÓDULO 08 | Componente desatualizado e vulnerável

MÓDULO 09 | Falha de Identificação e Autenticação

MÓDULO 10 | Falha de Integridade de Dados e Software

MÓDULO 11 | Monitoramento de falhas e registros de segurança

MÓDULO 12 | Falsificação de Solicitação do Lado Servidor (SSRF)

Você busca construir uma carreira em DevOps? Então este é o curso ideal para você adquirir o conhecimento básico, suas metodologias e seus benefícios para as organizações.

Por que fazer este curso?

Este curso apresentará as bases da cultura DevOps aplicadas a tão desejada transformação digital de empresas que buscam por renovação no método de trabalho com entregas mais ágeis para o desenvolvimento de softwares no final de cada sprint. Além disso, você poderá:

- Colocar em prática o que aprendeu, no dia-a-dia da sua empresa
- Orientar quanto às melhores práticas visando a colaboração e a comunicação entre os profissionais de TI
- Alavancar as tecnologias de automação
- Utilizar pipeline de implementação, ferramentas e avaliação

Objetivos deste curso

Preparar os profissionais de TI e de negócio para o conhecimento e entendimento básico sobre DevOps, além dos benefícios de seus princípios e práticas DevOps para a organização.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 20 horas (online, ao vivo) de treinamento

Pré-requisitos

- Recomenda-se familiaridade com a terminologia de TI e experiência de trabalho relacionada à TI

Público-alvo

- Profissionais de TI
- Profissionais de Agile, Scrum e Lean IT
- Desenvolvedores de software
- Pessoas envolvidas no gerenciamento de informações e tecnologia

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

Certificações do curso

Programa do curso

MÓDULO 01 | Conceitos básicos de DevOps
- Origens de DevOps
- Definição de DevOps
- Razões para usar DevOps
- Equívocos sobre DevOps

MÓDULO 02 | Princípios de DevOps
- Fluxo de Valor
- Pipeline de implantação
- Controle de versão
- Gerenciamento de configuração
- Definição de Pronto

MÓDULO 03 | Práticas-chave de DevOps
- Diferença em relação às práticas tradicionais
- Práticas de DevOps

MÓDULO 04 | Aplicação prática de DevOps
- Aplicabilidade
- Limitações
- Uso de software de prateleira
- Evolução da arquitetura e Modelos Organizacionais
- Progressão iterativa

DSO 252 – Devops Professional

Com a transformação digital, as organizações exigem cada vez mais agilidade, produtividade e confiabilidade por parte da TI para entrega de softwares e de serviços ao público. Isso exige automação, processos e cultura ágil.

O DevOps não é uma onda do momento, é uma necessidade! As empresas precisam de agilidade e o DevOps é o caminho.

O curso DevOps Professional trará ao profissional o impacto dessas regras organizacionais e técnicas em seu trabalho diário.

Por que fazer este curso?

Este curso apresentará o conjunto de melhores práticas que enfatizam a colaboração e a comunicação de profissionais de TI no ciclo de vida de aplicativos e serviços. Além disso, você poderá:

- Otimizar o fluxo de valor e reduzir o lead time
- Escolher uma estratégia de branch ideal
- Montar um pipeline de implantação
- Utilizar ferramentas para automatizar a construção e a configuração de ambientes

Objetivos deste curso

Preparar o aluno para familiarizar-se com as melhores práticas DevOps nas Três Maneiras: Fluxo, Feedback (retroalimentação) e Aprendizagem e Experimentação Contínuas, além de mostrar o impacto dessas mudanças organizacionais e técnicas em seu trabalho diário.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 20 horas (online, ao vivo) de treinamento

Pré-requisitos

- Recomenda-se conhecimento básico em Agile, Lean e/ou Gerenciamento de Serviços de TI

Público-alvo

- Desenvolvedores de Software e de Sites
- Engenheiros de Sistemas
- Engenheiros DevOps
- Proprietários de Produtos e de Serviços
- Gerentes de Projeto
- Engenheiros de Teste
- Equipes de operação e suporte de Gestão de Serviços de TI
- Gerentes de Processo
- Profissionais de Lean IT
- Praticantes de Agile Scrum

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

Certificações do curso

Programa do curso

MÓDULO 01 | Adoção do DevOps
- Conceitos Básicos do DevOps
- Princípios das Três Maneiras
- Organização

MÓDULO 02 | A Primeira Maneira: Fluxo
- Pipeline de Implantação
- Testes Automatizados
- Integração Contínua
- Lançamentos de baixo risco

MÓDULO 03 | A Segunda Maneira: Feedback (retroalimentação)
- Telemetria
- Feedback (retroalimentação)
- Desenvolvimento orientado a Hipóteses de Testes A/B
- Revisão e Coordenação

MÓDULO 04 | A Terceira Maneira: Aprendizagem e Experimentação Contínuas
- Aprendizagem
- Descobertas

MÓDULO 05 | Segurança da Informação e Gestão de Mudanças
- Segurança da Informação
- Gestão de Mudanças

A DevOps está associada principalmente ao desenvolvimento de software, mas seus princípios são cada vez mais aplicados a outros projetos e processos. Isso torna o curso DevOps Master interessante para os profissionais de TI que desejam estender seus conhecimentos para cobrir os últimos desenvolvimentos em gerenciamento de TI. Desenvolvedores de aplicativos, proprietários de produtos, mestres Agile Scrum, gerentes de projeto, gerentes de testes e gerentes de serviços de TI se beneficiariam desse curso.

Por que fazer este curso?

Este curso permitirá que um DevOps Master aumente as facilidades de sucesso do DevOps em uma equipe e, ainda consiga promover seus princípios na organização. Além disso, poderá:

- Avaliar, mensuras as diversas práticas atuais da TI, seus sintomas e causas raiz, para determinar ações que aumentem a eficácia dos processos
- Implantar e melhorar as práticas atuais da TI, considerando a velocidade e a segurança da organização como um todo
- Capacitar a organização para evoluir seus diferentes sistemas em ambientes altamente dinâmicos e seguros
- Identificar que práticas de banco de dados suportam evoluções dinâmicas, com rápidos rollbacks no trânsito entre versões

Objetivos deste curso

Preparar o aluno para familiarizar-se com as melhores práticas DevOps nas Três Maneiras: Fluxo, Feedback (retroalimentação) e Aprendizagem e Experimentação Contínuas, além de mostrar o impacto dessas mudanças organizacionais e técnicas em seu trabalho diário.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 20 horas de treinamento (online, ao vivo)

Pré-requisitos

- Recomenda-se familiaridade básica com os princípios Ágil, Scrum, Lean e ITSM

Público-alvo

- Proprietários de Produto
- Agile Scrum Master
- Gerentes de Projetos
- Gerentes de Testes
- Gerentes de Serviços de TI
- Gerentes de Processo
- Praticantes do Lean IT

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

Certificações do curso

Programa do curso

MÓDULO 01 | Adoção do DevOps
- Mentalidade (Mindset) DevOps e seus benefícios
- Cultura Organizacional
- Princípios e conceitos DevOps

MÓDULO 02 | Planejamento, requisitos e design
- Gerenciamento do Ciclo de Vida de Aplicativos ou Serviços
- Termo de Abertura do Projeto (Definição de escopo) e Controle Visual
- Desenho da Infraestrutura e Arquitetura
- Requisitos e acordos de nível de serviço
- Implementando uma Estratégia de Testes

MÓDULO 03 | Desenvolvimento e Implantação
- Entrega Contínua e Integração Contínua
- Pipeline de Implantação
- Implantação Contínua
- Ji-Kotei-Kanketsu, Ritmo, Trabalho em Adamento e Fluxo Único (Fluxo Contínuo)
- Automação, Ferramentas e Testes

MÓDULO 04 | Operação e Dimensionamento
- Gerenciamento de Dados; Infraestrutura e Ambientes; Componentes e Dependências
- Gerenciamento de Configuração e Controle de Versão
- Infraestrutura em Nuvens e Imutável
- Continuidade do Negócio
- Escala

MÓDULO 05 | Fim de vida
- Condições de Fim de Vida de um Produto ou Serviço

Python se tornou uma das linguagens de programação mais úteis no dia-a-dia, seja eliminando tarefas repetitivas ou solucionando problemas complexos essa ferramenta é o verdadeiro canivete suíço nas mãos do profissional de redes nos dias atuais.

O curso de Python para profissionais de rede mostrará desde o básico até a documentação de rede e muito mais.

Por que fazer este curso?

De forma simples, no formato de bootcamp, neste curso você, mesmo que nunca programou, aprenderá a criar scripts, APIs, dashboards, gráficos, documentar sua rede e muito mais. Além disso, você poderá:

- Melhorar o desempenho na operação e administração de rede
- Ter controle total sobre a rede
- Criar scripts de configuração em Python
- Criar scripts para automatizar redes de médio e grande porte

Objetivos deste curso

O Objetivo deste curso é colocar o Python na sua rotina de gerenciamento de rede, começando do zero, mesmo que você nunca tenha programado.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 35 horas (online, ao vivo) de treinamento

Pré-requisitos

- Não há

Público-alvo

- Profissionais de Suporte em TI
- DevOps
- Administradores de Sistema
- Engenheiros de Rede
- Administradores de Rede
- Arquitetos de Rede

Instrutores

MARCELO NUNES

INSTRUTOR

Engenheiro Eletrônico e de Telecomunicações

Certificações do curso

Não há certificações disponíveis para este curso

Programa do curso

MÓDULO 01 | Introdução ao Python
- Instalação
- Gerenciamento de pacotes
- Ambiente de desenvolvimento
- Laços
- Coleções
- Lidando com texto e arquivos
- Scripts
- Notebooks
- APIs

MÓDULO 02 | Gerenciamento de Redes
- Elementos de gerenciamento de redes
- Eventos
- SNMP
- Gerenciamento de nível de serviço

MÓDULO 03 | Python na administração de Redes
- Monitoração de ativos
- Configuração de ativos
- Automação de tarefas
- Net health e análise de performance
- Alarmes e logs

MÓDULO 04 | Dashboard
- Desenvolvendo um painel de controle personalizado para gestão e monitoramento de rede

O curso Ops Foundation é ideal para você que quer compreender o lado Ops do DevOps.

Ele te apresentará os fundamentos do lado Ops do DevOps, apresentando a cultura do DevOps através de ferramentas práticas.

Por que fazer este curso?

Este curso apresentará o lado Ops do DevOps com conceitos e recursos específicos da área. Além disso, você poderá:

- Automatizar gerenciamentos e configurações
- Colaborar entre equipes
- Agilizar os serviços de TI
- Utilizar sistemas de automação: Git, Docker, Linux, Vagrant

Objetivos deste curso

O Objetivo deste curso é apresentar o lado Ops do DevOps , mostrando seus fundamentos e cultura do DevOps, além de utilizar sistemas de automação, como: Git, Docker, etc.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 16 horas (online, ao vivo) de treinamento

Pré-requisitos

- Não há

Público-alvo

- Todo público com o conhecimento mínimo de computação e Sistemas Operacionais

Instrutores

BRUNO BOURA

INSTRUTOR

Administrador de redes | DevOps

Certificações do curso

Não há certificações disponíveis para este curso

Programa do curso

MÓDULO 01 | Fundamentos de DevOps
Entender o que é DevOps, suas origens e como se encaixa no cenário atual de tecnologia. Uma conversa descontraída para entender um pouco mais de DevOps.

- Origem do DevOps
- Definição de DevOps
- Razões para usar DevOps
- Erros comuns sobre o DevOps

MÓDULO 02 | A Primeira Maneira: Fluxo
Preparação do ambiente inicial para o treinamento.

- Conhecer Virtual Box
- Instalar as ferramentas necessárias

MÓDULO 03 | Administrando Vagrant
Criar ambientes completos em diversos provedores de forma simples através de um arquivo de texto.

- Provisionando VMs
- Configuração da Rede
- Comandos do Vagrant
- Provedores

MÓDULO 04 | Git
Git é um sistema open-source de controle de versões. Git hub é um grande provedor de Git.

- O que é Git
- Instalação Git
- Clonando Projetos
- Criando e Sincronizando Repositórios
- Salvando Alterações
- Vendo Histórico
- Ignorando Arquivos

MÓDULO 05 | Introdução ao Linux
É um treinamento indispensável para o DevOps. Grande parte dos nossos trabalhos serão nesta plataforma, logo, é uma ferramenta essencial para o nosso desenvolvimento.

- Comandos Básicos
- Editores de Texto
- Gerenciamento de Pacotes
- SSH

MÓDULO 06 | Docker
Docker é uma tecnologia que permite empacotar, entregar e executar aplicações em containers Linux leves e autossuficientes, facilitando o desenvolvimento, a implantação e a execução de aplicações em ambientes isolados.

- Introdução ao Docker
- Instalação do Docker
- Comandos Básicos
- Gerenciando Volumes
- Trabalhando com Imagens

GRC | GOVERNANÇA, RISCO E COMPLIANCE

O acrônimo GRC tem origem na união dos termos governança, riscos e compliance, ou em inglês, governance, risk and compliance. Uma tendência recente, de integração das áreas de conhecimento de Gestão de Riscos, Governança Corporativa e práticas de auditoria e controle que visa garantir a conformidade com leis, regulamentos, imposições de padrões consolidando-os dentro de um único modelo, integrado inteligentemente e tendo como um dos seus objetivos a unificação dos interesses comuns e conciliação de interesses opostos de cada uma destas funções.

GRC 204 – FAIR Risk Management Foundation

Descubra os desafios dos métodos convencionais de Gerenciamento de Risco Qualitativo.
No curso FAIR Risk Management Foundation, será apresentado ao estudante, o padrão e a metodologia FAIR, os processos associados e a terminologia. Também serão apresentados os principais conceitos de medição, métodos de estimativa calibrados necessários para realizar análises quantitativas de risco em sua agência ou departamento e as melhores práticas para comunicar análises às partes interessadas.

Por que fazer este curso?

Este curso apresentará os conceitos fundamentais de Gerenciamento de Riscos FAIR. Além disso, você poderá:

- Conhecer o padrão FAIR (variáveis, definições, relacionamentos, formas de perda, etc.)
- Explicar o processo de Análise de Risco FAIR
- Mapear os controles para o padrão FAIR para analisar a mitigação de riscos
- Interpretar os resultados de uma Análise FAIR e criar relatórios para as partes interessadas

Objetivos deste curso

O Objetivo deste curso é apresentar o padrão e a metodologia FAIR, os processos associados e a terminologia.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 18 horas de treinamento (online, ao vivo)

Pré-requisitos

- Não há

Público-alvo

- Diretores de Risco
- Diretores de Segurança da Informação
- Diretores de Informações
- Líderes e Analistas de Gerenciamento de Riscos Corporativos
- Líderes e Analistas de Gestão de Risco da Informação

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

Certificações do curso

Open FAIR™ Foundation

Programa do curso

MÓDULO 01 | Introdução e Fundamentos FAIR

Neste módulo, discutiremos sobre o que o gerenciamento de riscos deve permitir que uma organização faça. Quais são os objetivos da gestão de risco? Como funciona o processo de gerenciamento de riscos? Depois disso, exploraremos os métodos tradicionais/qualitativos de gerenciamento de risco e identificaremos por que eles são subótimos. A partir daí, começaremos nossa exploração do FAIR alinhando-nos a um léxico comum de risco, discutindo conceitos fundamentais de análise quantitativa e aprendendo sobre estimativa calibrada. Concluiremos o dia aprendendo os componentes do próprio modelo FAIR.

- Introdução
  - Gestão de Riscos: Processo e Objetivos
  - As falhas do gerenciamento de risco tradicional/qualitativo
  - O Léxico do Risco
  - Gerenciamento de risco eficaz usando FAIR
- Fundamentos FAIR
  - Conceitos Fundamentais
  - Fazendo estimativas calibradas
  - O Modelo FAIR

MÓDULO 02 | Aplicando FAIR

Neste módulo, ampliaremos seu conhecimento sobre o modelo FAIR e como usá-lo para realizar análises quantitativas de risco. Discutiremos a simulação de Monte Carlo, uma visão geral de alto nível do subprocesso de análise de risco e o papel que os controles desempenham em uma análise baseada em FAIR.

- Fundamentos de FAIR
  - Simulação de Monte Carlo
  - O Subprocesso de Análise de Risco
  - Considerando controles em análises FAIR

- Aplicando FAIR
  - Estudo de caso e discussão

MÓDULO 03 | Análises de escopo e coleta de dados e estimativas

Neste módulo, aprimoraremos suas habilidades como analista de risco. Você está familiarizado com o modelo FAIR e pode aplicá-lo a situações da vida real, mas como isso se traduz na realização de análises em suas organizações? Os próximos módulos dão a você as habilidades necessárias para definir o escopo adequado de um esforço de análise, coletar dados e estimativas para as variáveis do modelo FAIR, realizar garantia de qualidade em seus resultados e apresentá-los aos tomadores de decisão.

- Análises de escopo
    - Elementos e Importância do Escopo
    - Escopo de vários cenários
    - Priorizando Cenários para Análise
- Coletas de dados e estimativas
    - Espectro de Coleta de Dados
    - Perguntas específicas do contexto
    - Identificação de PMEs
    - Conduzindo Sessões de Estimativa Calibrada

MÓDULO 04 | Apresentando e executando a garantia de qualidade nos resultados da análise

Neste módulo, mostraremos as habilidades necessárias para realizar uma análise de risco com competência. Vamos encerrar o curso com uma revisão abrangente do material coberto no Exame de Certificação OpenFAIR usando um guia de estudo do exame e perguntas de avaliação simuladas.

- Executando a garantia de qualidade nos resultados da análise
    - Lista de verificação de garantia de qualidade
    - Validando resultados e justificativa
    - Validando o Propósito da Análise
    - Conduzindo Análises Comparativas
- Apresentando resultados
    - Planejamento e entrega de apresentações de resultados
    - Preparando Relatórios Escritos
- Revisão do Curso/Preparação para Exame
    - Certificação OpenFAIR
    - Guia de Estudo do Exame/Perguntas Práticas
    - Avaliação do curso

O curso de Governança Corporativa, Risco e Compliance (GRC) apresenta o conhecimento necessário para o planejamento e o aprimoramento dos sistemas de governança, gestão de riscos e compliance, além de abordar as principais práticas e papéis dos agentes envolvidos, provocando a reflexão sobre como integrar as várias atividades do GRC em sua organização.

Por que fazer este curso?

Este curso irá contribuir para uma mentalidade nova na governança corporativa e nas práticas de gestão de compliance e riscos, buscando facilitar o entendimento desse assunto através de metodologias de gestão de riscos, de compliance e de controles internos para possibilitar uma conduta corporativa com ética e caráter. Além disso, você poderá:

- Aplicar as melhores práticas de Governança e Gestão
- Realizar a Gestão de Riscos
- Desenvolver planos e mapas com base nos riscos existentes
- Elaborar Matriz de Risco (Probabilidade e Impacto)

Objetivos deste curso

O Objetivo deste curso é apresentar o conhecimento necessário para o planejamento e aprimoramento dos sistemas de Governança, Gestão de Riscos e Compliance.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 16 horas (online, ao vivo) de treinamento

Pré-requisitos

- Conhecimentos básicos de Gestão Comercial, Riscos e Conformidades

Público-alvo

- Bachareis em Direito
- Executivos
- Gestores de equipes
- Gerentes de Controladoria (Controllers)
- Analistas de Riscos
- Profissionais que atuam com orgãos governamentais
- Profissionais que desejam atuar na área de Governança, Risco e Compliance

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

Certificações do curso

Não há certificações disponíveis para este curso

Programa do curso

MÓDULO 01 | Introdução ao GRC

Este módulo demostra como incidentes ligados a falhas nas áreas de Governança, Gestão de Riscos e Conformidade podem comprometer o valor de mercado e o lucro das empresas, além de apresentar alguns conceitos importantes para a compreensão da integração de GRC.

- A necessidade do GRC
- Cases de empresas afetadas por problemas de GRC
- Definições
- Stakeholder
- Sociedades Anônimas
- Shareholders
- Bolsa de Valores

MÓDULO 02 | A história do GRC

Este módulo explica, através de eventos históricos, como as pessoas se comportavam em relação ao risco e como a matemática e estatística criaram uma nova visão sobre a causa dos eventos. Paralelamente, a história da Governança Corporativa é contada em uma linha do tempo que começa com a primeira sociedade de ações do mundo, em 1250, e avança até a crise da Enron, que culminou na Lei Sarbanes-Oxley.

A linha histórica da conformidade aparece como uma resposta a eventos como a quebra da bolsa de NY em 1929 e a quebra da Enron. Por esse motivo, esses eventos são apontados como marcos de governança e conformidade.

- Risco
    - A Vontade dos Deuses dita as regras, Algarismos Indo-Arábicos
    - 1654 – Luca Paccioli e o desafio da renascença
    - 1703 a 1760 – Jabob Bernoulli e a lei dos grandes números
    - 1875 – Regressão a média
    - 1952 – Ovos em cestas separadas
    - 1992 – O Cubo COSO
    - 2004 – Coso II

- Governança
    - 1250 – Societe des Moulins bu Bazacle
    - 1600 – Companhia das Índias Orientais
    - 1602 – Amsterdam Stock Exchange
    - 1915 a 1929 – A Economia Liberal
    - 1929 – Euforia na Bolsa de NY
    - 1929 – O Crash da Bolsa de NY

- 1930 – A Grande Depressão
- 1961 – A Criação da OECD
- 1980 – O Ativismo de Robert Monks
- 1992 – O Relatório Cadbury
- 1999 – Os Princípios de Governança da OECD
- Enron

- Compliance
  - 1934 – New Deal e a SEC
  - 1969 – A Criação da ISACA
  - 1976 – A CVM no Brasil
  - 1973 – A Criação da IASC
  - 1977 – A FCPA
  - 1985 – COSO
  - 1992 – A Convença o anti-suborno da OECD
  - 1996 – HIPAA
  - 1996 – Cobit 1.0
  - 1998 – The Anti-Bribery Act
  - 1998 – O Acordo de Basileia
  - 1999 – Gramm-Leach-Bliley Act
  - 2002 – A Lei Sarbanes-Oxley
  - 2004 – Basileia II
  - 2004 – IFRS
  - 2005 – O Roubo de dados de Cartões de Crédito na TJX
  - 2006 – O PCI Council
  - 2010 – Basileia III

MÓDULO 03 | Governança
Este módulo apresenta os conceitos de governança (corporativa e de TI), visando criar um melhor entendimento das necessidades das empresas, facilitando o entendimento de quais devem ser os objetivos de Tecnologia da Informação e Segurança da Informação para que estas áreas estejam alinhadas aos objetivos da alta gestão.

Governança Corporativa – Definições do IBGC (Instituto Brasileiro de Governança Corporativa), níveis de governança e o novo mercado da Bovespa, transparência, equidade, prestação de Contas, responsabilidade corporativa, conselho de administração, relações com os investidores, gestão de riscos, relatório anual, código de conduta. Governança de TI – Estrutura de governança de TI, estudo da norma ABNT ISO/IEC 38500.

MÓDULO 04 | Gestão de Riscos
Este módulo demonstra os conceitos de risco positivo e negativo, que juntos com os conceitos de apetite e tolerância a riscos demonstram a necessidade do risco para a o crescimento e sucesso das organizações. O módulo aborda também todos os conceitos e as principais normas e frameworks para a avaliação e tratamento de riscos.

Definições de risco – Riscos positivos e negativos, fontes de risco, nível de risco e probabilidade, consequência, análise quantitativa , qualitativa e semi-quantitativa, matriz de riscos, percepção de riscos, responsabilidade pelo risco, apetite e tolerância a riscos.

Gestão de Riscos – Princípios de Gestão de Riscos, estudo da norma ABNT ISO 31000, critérios de Risco (ALARP – As Low as Reasonable Practicable), processo de avaliação de riscos, tratamento de riscos, monitoração do risco, reporte de riscos, gestão de riscos através da ABNT ISO 27005, comparação do Coso ERM (Coso II) com a ISO 31000.

MÓDULO 05 | Conformidade

Este módulo apresenta os principais conceitos relacionados à conformidade, assim como as mais importantes regulamentações a s quais as empresas nacionais estão sujeitas. Ao final dos estudos é apresentada a norma Australiana de Compliance e os principais pontos abordados por esta.

Conceitos e definições, sistema normativo (Leis e Regulamentações), tipos de conformidade, CVM, CVM 358/2002 – Fato Relevante, CVM 456/2007 – IFRS, decreto 11.638 – Contabilidade das Sociedades por Ações, Basileia II e III, Banco Central, resolução 2554, resolução 3380, SUSEP 249/2004, culpa e dolo, responsabilidades dos Administradores, lei das S.A.'s, business judgement rule, conflito de Interesses, dever de qualificar-se e informar-se, dever de informar, dever de sigilo, insider trading, concorrência desleal, dever de vigiar, investigar e punir , código de ética, política de propriedade intelectual, política de segurança da informação, sustentabilidade, a norma AS 3806/2006, o papel do CCO/CECO.

MÓDULO 06 | IT GRC utilizando o Cobit

Este módulo complementa os três anteriores ao mostrar o Conjunto Cobit+Vai IT+Risk IT, delimitando o seu relacionamento com as áreas de Governança, Gestão de Riscos e Compliance.

Em uma segunda etapa, apresentamos o Cobit 5, o framework de GRC da ISACA que integrou o Val IT e RisK IT ao CobiT e tem a proposta de ser um framework de GRC para qualquer área da organização.

Governança de TI segundo o Cobit – Áreas de foco na Governança de TI, produtos do CobiT, objetivos e Arquitetura de TI, ciclo de vida de TI, domínios do CobiT, objetivos de Controle, tabela RACI, modelo de maturidade, objetivos de negócio, objetivos de negócio transformados em objetivos de TI, objetivos de TI transformados em objetivos de processo.

VAL IT – Definição e Objetivos, os quatro "Estamos?", Val IT x CobiT, domínios e Processos, quadro de atividades, entradas e saídas.

Risk IT – Posicionando Cobit, ValIT e RiskIT, hierarquia dos riscos, resposta e priorização de riscos, governança de riscos, avaliação de riscos, articulação de riscos.

Cobit 5 – Princípios e aspectos gerais, arquitetura e objetivos em cascata, objetivos de governança, modelo de “Enablers” integrados, objetivos de governança, objetivos de TI, governança e gestão, governança corporativa de TI, novo modelo de maturidade (ISO 15504), ciclo de implementação.

MÓDULO 07 | Considerações Finais

Neste módulo trazemos uma reflexão sobre os desafios para a implantação do GRC desde uma definição do termo e de sua real função até o perfil do profissional de GRC.

O que esperar do GRC, visão do modelo de negócio (OCEG), colaboração, stakeholders internos do GRC, stakeholders externos do GRC, sistemas eficientes, eficazes e responsivos, implantação do GRC na organização, vencendo resistências, perfil do profissional de GRC.

GCN | GESTÃO DA CONTINUIDADE DE NEGÓCIOS

A Gestão de Continuidade de Negócios (GCN) oferece às organizações capacidade de responder e lidar com interrupções em seus negócios. Nossos cursos fornecem todo o conteúdo para as disciplinas de GCN (BCM), além de serem totalmente orientados paras as normas ISO 22301, 27031 etc., dedicadas à continuidade de negócios.

Reduza perdas financeiras e evite que o negócio pare!

Com o curso de Fundamentos de Continuidade de Negócios, você poderá criar um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre indo até o retorno à situação normal de funcionamento da organização.

Por que fazer este curso?

Além de te preparar para a Certificação ECES (EC-Council Certified Encryption Specialist) do EC-Council, você também poderá:

- Realizar uma Análise de Impacto de Negócios (BIA)
- Definir estratégias de continuidade
- Desenvolver planos de continuidade, restauração e recuperação
- Implementar a GCN (Gestão de Continuidade de Negócios)

Objetivos deste curso

O Objetivo deste curso é apresentar o conhecimento necessário para que o profissional consiga implementar a GCN em sua organização, além de criar planos de ação para garantir que os serviços essenciais sejam identificados e preservados após a ocorrência de um desastre.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 16 horas (online, ao vivo) de treinamento

Pré-requisitos

- Conhecimentos básicos de TI (Tecnologia da Informação)

Público-alvo

Todo o pessoal técnico envolvido com o manuseio de dados críticos, mais especificamente os custodiantes das informações, normalmente pertencentes a área de tecnologia da informação. Dentre esses profissionais destacamos:

- Desenvolvedores, Integradores e arquitetos de sistemas
- Engenheiros e especialistas de rede
- Profissionais de segurança da Informação

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

Certificações do curso

Programa do curso

MÓDULO 01 | Histórico da disciplina
Apresenta uma visão geral das disciplinas relacionadas com a continuidade aplicadas em cenários diversos ao longo da História, sua evolução como instrumento estratégico e a aplicabilidade como prática de adequação da resiliência organizacional em diferentes abordagens.

MÓDULO 02 | Conceitos Fundamentais
Apresentação dos conceitos que estruturam as práticas de continuidade, onde é abordada a definição de incidente, a composição e uso das estratégias de resposta e os critérios que devem ser empregados para definir a composição e uso de uma Estratégia para a Continuidade dos Negócios.

Apresenta as teorias que fundamentam a necessidade de resposta e manutenção da continuidade são ainda explicadas, através da conceituação e entendimento dos valores estabelecidos para o Recovery PointObjective e a composição do Maximum Tolerable Downtime pelo uso do Recovery Time Objective e Work Recovery Time.

MÓDULO 03 | O ciclo da continuidade
Abordando os componentes da Estratégia e seus relacionamentos e apresentado o uso do processo de resposta a incidentes e compartilhadas experiências práticas de como fundamentar a tomada de decisão para o acionamento da contingência.

Após o entendimento deste processo, o uso e relacionamentos entre os diversos planos que compõem a Estratégia são apresentados e fundamentados: o papel dos planos de recuperação de desastres e continuidade operacional, o entendimento do processo de retorno ao Modo Regular e a prática de Lições Aprendidas para a melhoria contínua da estratégia.

MÓDULO 04 | Normas e regulamentações
O papel das normas e regulamentações como direcionadores da Continuidade de Negócios, abrangendo a aderência em determinados setores, a aplicabilidade da responsabilidade compartilhada e o entendimento no Código Civil, Sarbanes-Oxley, Basile ia, Resolução 3380 do Banco Central do Brasil e nos programas de qualidade da Bolsa de Mercadorias e Futuros.

ICS | INDUSTRIAL CONTROL SYSTEMS

O Industrial Control Systems (ICS) é um termo geral que abrange vários tipos de sistemas de controle e instrumentação associada utilizada para o controle de processos industriais. Os sistemas de controle podem variar em tamanho, desde alguns controladores modulares montados em painéis até grandes sistemas de controle distribuídos interconectados e interativos (DCSs) com milhares de conexões de campo.

Os padrões e estruturas de segurança cibernética mais populares são hoje voltados principalmente para ambientes de TI. A ISA, uma organização estabelecida que desenvolve padrões para automação há muitos anos, desenvolveu os padrões ISA/IEC 62443. Eles são desenvolvidos especificamente para resolver problemas de segurança exclusivos dos sistemas de automação e controle industrial (IACS) e da tecnologia operacional (OT).

Por que fazer este curso?

Além de fornecer uma visão detalhada de como a estrutura de padrões ISA/IEC 62443 pode ser usada para proteger sistemas de controle críticos, você estará pronto para:

- Discutir os princípios por trás da criação de uma segurança eficaz de programas de longo prazo
- Interpretar o quadro de segurança industrial ISA/IEC 62443 e aplica-lo à sua operação
- Analisar as tendências atuais em incidentes de segurança industrial e métodos que os hackers usam para atacar um sistema
- Definir os princípios por trás das principais técnicas de mitigação de riscos, incluindo gerenciamento antivírus e patches, firewalls e redes privadas virtuais

Objetivos deste curso

Este curso abrange o ciclo completo de vida da avaliação, projeto, implementação, operações e manutenção do sistema de automação industrial (IACS).

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.
- Laboratórios práticos: Laboratórios práticos para desenvolver e testar suas habilidades examinando centenas de capturas que irão fortalecer os conceitos que você aprendeu.

Carga-horária

- 24 horas de treinamento (online, ao vivo)

Pré-requisitos

- Não há

Público-alvo

- Engenheiros de Sistemas de Controles
- Gerentes de Sistemas de Controles
- Profissionais de Automação
- Engenheiros de TI—Instalações Industriais
- Gerentes de TI—Instalações Industriais
- Gerentes de fábrica
- Segurança da Planta e Gerenciamento de Riscos

Instrutores

PAULO COELHO

INSTRUTOR

AWS | CCDA | CCNA | CCNP | CNE | CNI | CWNA | MCSA | VMware

Certificações do curso

Programa do curso

MÓDULO 01 | Introdução à Cyber Segurança

MÓDULO 02 | Entendendo o ecossistema de Cyber Segurança

MÓDULO 03 | Noções básicas de rede industrial L1-L7

MÓDULO 04 | Protocolos Industriais

MÓDULO 05 | Entendendo os principais ataques

MÓDULO 06 | Frameworks de segurança

MÓDULO 07 | Análise de Risco

MÓDULO 08 | Normas ISA/IEC 62443-1-1

MÓDULO 09 | Introdução ao ciclo de vida de Cyber Segurança do ambiente IAC

MÓDULO 10 | Estabelecendo um Programa de Segurança de Sistemas de Automação e Controle Industrial

MÓDULO 11 | Gerenciamento e Auditoria

MÓDULO 12 | Aplicando a Norma ISA/IEC 62443

MÓDULO 13 | IACS e Cloud Computing

LABORATÓRIO 01 | Utilizando o Kali Linux

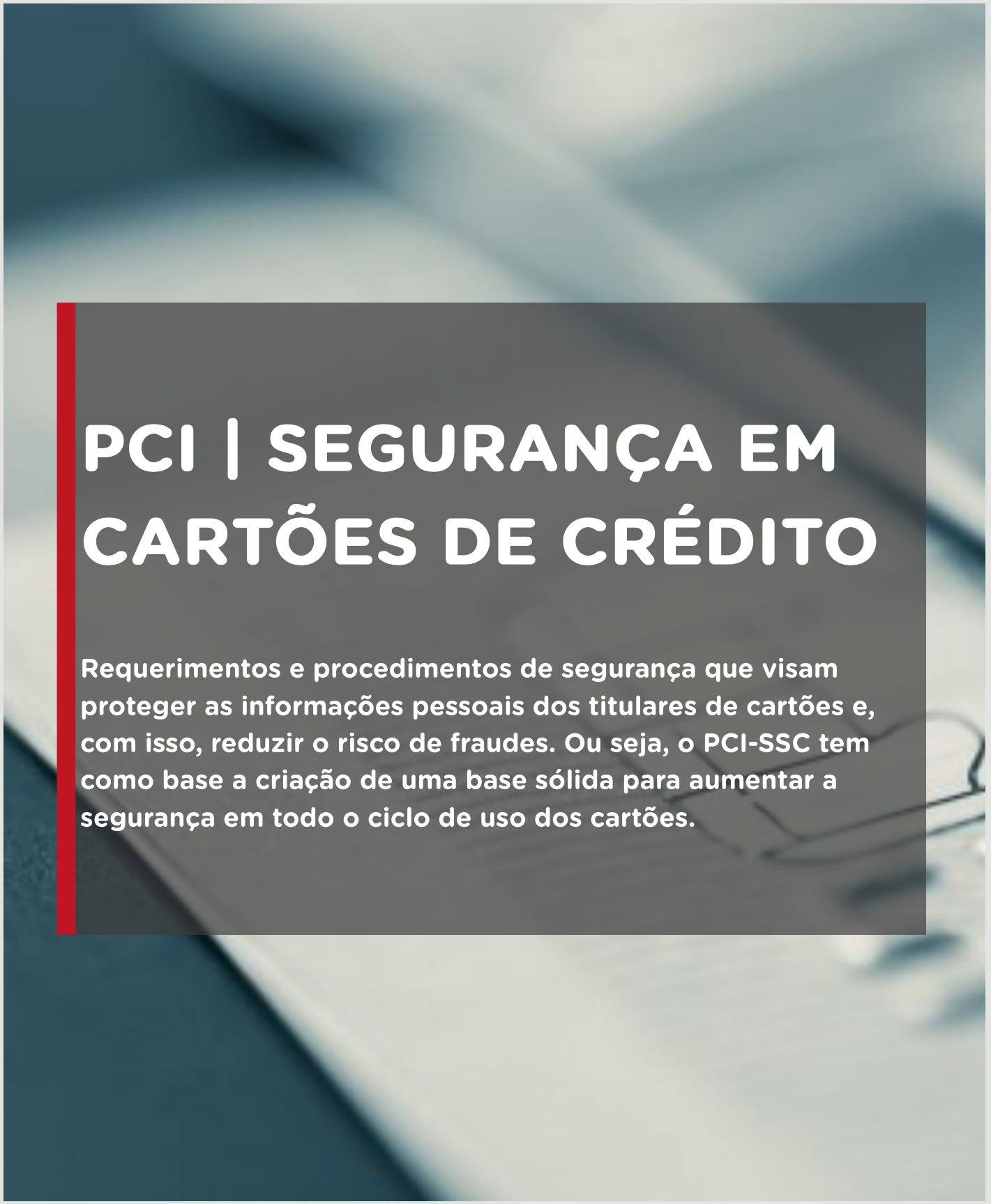
LABORATÓRIO 02 | Praticando os ataques

LABORATÓRIO 03 | Utilizando o analisador de protocolos

LABORATÓRIO 04 | Praticando uma metodologia de Análise de Risco

LABORATÓRIO 05 | Plataforma de monitoramento

LABORATÓRIO 06 | Aplicando a Norma ISA/IEC 62443



PCI | SEGURANÇA EM CARTÕES DE CRÉDITO

Requerimentos e procedimentos de segurança que visam proteger as informações pessoais dos titulares de cartões e, com isso, reduzir o risco de fraudes. Ou seja, o PCI-SSC tem como base a criação de uma base sólida para aumentar a segurança em todo o ciclo de uso dos cartões.

PCI 501 – Implementando o PCI DSS 3.2 e 4.0

Existe o momento certo para cada capacitação e este é o momento de sair na frente e se capacitar para implementar todos os controles do PCI DSS 4.0

O PCI DSS é um padrão de segurança para cartões de crédito, que acaba sendo um tipo de dado pessoal. Se você quiser conhecer como a indústria de cartões de pagamento protege estes dados tão cobiçados pelos criminosos, inscreva-se em nosso treinamento e conheça as centenas de controles, dos mais organizacionais aos mais técnicos, que vem sendo aperfeiçoados há décadas pelo PCI Council.

Por que fazer este curso?

Este curso aumentará a expertise nos padrões de segurança da PCI Council e a eficiência de sua empresa na implementação dos controles necessários para atender aos requisitos e alcançar a conformidade com o PCI DSS. Além disso, você poderá

- Entender e implementar os vários requisitos do PCI DSS, reduzindo o risco de qualquer possível violação de dados
- Compreender os diferentes níveis de conformidade exigidos pelos comerciantes e prestadores de serviços
- Compreender os controles necessários para que sua organização possa lidar com segurança com os dados do titular do cartão
- Relatar a conformidade (autoavaliação e auditoria)

Objetivos deste curso

O objetivo deste curso é capacitar os colaboradores envolvidos na conformidade com o PCI DSS, abordando desde a definição de escopo até a entrega de relatórios de conformidade.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 20 horas (online, ao vivo) de treinamento

Pré-requisitos

- Conhecimentos básicos de TI (Tecnologia da Informação)

Público-alvo

- Gestores
- Consultores
- Pessoal de suporte
- Gerentes de Projeto de serviços de TI
- Desenvolvedores
- Integradores e arquitetos de sistemas
- Engenheiros e especialistas de rede
- Profissionais de Segurança da Informação

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

Certificações do curso

Não há certificações disponíveis para este curso

Programa do curso

MÓDULO 01 | Identificando e isolando dados sensíveis
A Evolveris e o grupo de colaboradores mais envolvido com a segurança da informação é apresentado aos alunos.

Hilda solicita que o CIO da empresa (Willian) faça um levantamento de todos os tipos de dados que a empresa processa, armazena, e em seguida pede que Olívia (Jurídico) identifique as leis, normas e regulamentações relacionadas às atividades da empresa e a esses tipos de dados. Juntos, Olívia e Wallace (CISO) desenham as políticas de retenção de dados e diretrizes para comunicação com portadores de cartão de pagamento para atenderem ao PCI DSS.

Capítulo 1: A Evolveris e o PCI Council

Allan, o CSO da Evolveris posiciona a segurança da informação no organograma da empresa, explana sobre o enquadramento dá Evolveris nos programas de conformidades das bandeiras de cartões de pagamento e apresenta o PCI Council e seus padrões de segurança para os outros gestores da empresa.

Wallace, o CISO, apresenta os componentes de SI (processos, pessoas e tecnologia), os conceitos de defesa em profundidade, o processo de criação de controles de segurança e os tipos e funções das medidas de segurança existentes.

Capítulo 2: Análise de Riscos

Allan inicia um processo de análise de riscos baseado nas melhores metodologias de mercado, como a ISO 27005 e NIST SP 800-30 revision1.

Para atender ao requisito 12.2, Allan estabelece sistemas de gestão de riscos com um processo de revisão anual dos riscos.

Capítulo 3: Localização de Dados

Wallace desenha um diagrama de rede que identifica todos as conexões entre o ambiente de dados de portadores de cartão, ou CDE (Cardholder Data Environment), e demonstra o fluxo de dados de cartões dentro dos sistemas e redes.

Adicionalmente, Willian se utiliza de ferramentas para identificar dados de cartões que possam estar em outras localidades além das documentadas.

Capítulo 4: Retenção de Dados

Apresenta os critérios utilizados para armazenamento de dados de cartões de pagamento na Evolveris.

Capítulo 5: Descarte de Dados

Wallace apresenta os controles utilizados para a destruição de dados que não possuem mais uma necessidade legal ou de negócio para serem armazenados.

MÓDULO 02 | Protegendo sistemas e redes e preparando-se para responder às falhas

Capítulo 6: Definição de Escopo

Wallace apresenta a Hilda as estratégias de segurança relacionadas à identificação do fluxo de dados de portadores de cartão dentro da Evolveris e de todos os componentes por onde estes dados trafegam, são armazenados ou processados.

Capítulo 7: Configuração dos Ativos de Rede

Alex apresenta as políticas de configuração dos ativos de rede, incluindo as regras de firewall, NAT, técnicas anti-spoofing e sincronização dos arquivos de configuração.

Alex especifica também os protocolos em uso e apresenta os mecanismos de detecção de intrusos nos diferentes segmentos de rede criados através de perímetros que separam diferentes zonas com diferentes níveis de confiança através de firewalls, switches e roteadores.

Capítulo 8: Configuração Padrão

Alex apresenta as políticas definidas para a substituição de senhas dos ativos de rede e dos softwares instalados na Evolveris antes da implantação dos mesmos na rede corporativa.

Capítulo 9: Configuração de Endpoint

Wallace apresenta as políticas e configurações utilizadas pela Evolveris para a configuração do (s) software (s) em execução nos hosts. Que incluem o antivírus, firewall pessoal e monitor de integridade nos equipamentos dentro do ambiente de dados do portador de cartão.

Capítulo 10: Criptografia Assimétrica

Samuel, o coordenador de infraestrutura apresenta os fundamentos da criptografia assimétrica, certificados digitais, autoridades certificadoras, infraestrutura de chaves públicas e assinatura digital.

Capítulo 11: Criptografia aplicada a transmissão de Dados

Samuel continua sua explicação, demonstrando como a Evolveris utiliza a criptografia para atingir os objetivos de conformidade e aumentar a segurança ao transmitir dados de cartões de pagamentos de forma segura, utilizando VPN, SSL/TLS e WPA.

Capítulo 12: Acesso Remoto

Samuel apresenta as políticas de acesso remoto, que incluem autenticação forte, baseada em mais de um fator, as características criptográficas para acesso administrativo.

Capítulo 13: Controles Físicos

Allan apresenta os controles de segurança física como a proteção do perímetro físico, áreas sensíveis, controles de acesso ao ambiente, CFTV, pontos de rede, estações desbloqueadas, informações nas estações de trabalho, além das políticas de controle de dispositivos de pagamento com lista de dispositivos, e inspeção periódica dos mesmos.

Capítulo 14: Teste de Vulnerabilidades

Samuel apresenta as políticas e as metodologias utilizadas para realizar os testes trimestrais de vulnerabilidades e os testes anuais de invasão no ambiente de dados do portador de cartão.

Capítulo 15: Provedores de Serviço e Plano de Resposta a Incidentes

Wallace apresenta as políticas para controle de provedores de serviço, os controles para resposta a incidentes de segurança e apresenta o plano de resposta a incidentes da Evolveris para o caso de vazamento de dados.

MÓDULO 03 | Segurança em aplicação de pagamento

Willian apresenta os estudos relacionados a vulnerabilidades de softwares, o processo de criação de exploits, zero-days, os procedimentos a serem adotados pelas empresas para mitigar essas ameaças e as melhores práticas de atualização, além das políticas de atualização, hardening e privilégio mínimo da Evolveris.

Capítulo 16: Configuração

Samuel descreve os procedimentos para criação e manutenção de padrões de instalação e configuração segura (hardening) dos componentes do sistema, assim como os procedimentos criados para que estes sistemas permanecem sempre atualizados e com uma configuração segura em qualquer tipo de componente, incluindo sistemas operacionais, páginas WEB, e firmware de ativos como roteadores e firewalls.

Capítulo 17: Desenvolvimento

Gabriel, o "Lenda", explica como os princípios de segurança no design e segurança por default são aplicados nos desenvolvimentos internos da Evolveris. Apresenta também a separação entre os ambientes de desenvolvimento, teste e produção, os procedimentos para gestão de mudanças em software, treinamento de desenvolvedores e os cuidados tomados na validação das entradas dos sistemas para evitar falhas de Buffer overflow, SQL Injection.

MÓDULO 04 | Controle de acesso

Capítulo 18: Controle de Acesso

Willian apresenta a política de controle de acesso da Evolveris, as regras para criação e manutenção de senhas seguras e os conceitos de gestão e identidades, identificação única, Need to Know, privilégio mínimo, segregação de funções.

Capítulo 19: Reference Monitor

Wallace apresenta os conceitos de Reference Monitor, Trile A, DACL's, SACL's, Auditoria de eventos (Logs), assim como o processo e a política de auditoria e os cuidados para sincronização de hosts (NTP).

Capítulo 20: Autenticação

Willian analisa as diferenças entre os processos de autenticação mais utilizados em sistemas operacionais, como o passwd, SAM, domínios e Kerberos. Discute também, as políticas de acesso a banco de dados e autenticação com Smatcards.

Capítulo 21: Monitoramento

Alex apresenta as políticas e recursos de monitoramento do ambiente utilizados para detectar alterações e arquivos críticos, redes wireless não autorizadas. O Capítulo aborda tecnologias como Scanners de Vulnerabilidades, IDS, IPS e NAC.

MÓDULO 05 | Proteção de dados armazenados

Capítulo 22: Proteção dos Dados Armazenados

Wallace apresenta as bases da criptografia simétrica, truncagem e hash de dados através da teoria e da demonstração da criptografia de arquivos, bancos de dados, discos e backups utilizada na Evolveris para a proteção dos dados armazenados.

Capítulo 23: Gerenciamento de Chaves

Samuel apresenta as políticas para geração, transmissão, custódia de chaves criptográficas, conhecimento compartilhado, duplo controle e destruição das chaves.

Capítulo 24: Tokenização

Samuel apresenta os conceitos de Tokenização e como essa metodologia vem sendo aplicada dentro da Evolveris para diminuir o impacto de um eventual vazamento de dados.

MÓDULO 06 | Controles adicionais

Capítulo 25: Gestão de Mudanças

Wallace apresenta os controles utilizados para garantir uma gestão adequada das alterações realizadas nos componentes dos sistemas da Evolveris, dentre eles a documentação de impacto, aprovação da mudança, teste de funcionalidade e procedimentos de retorno.

Capítulo 26: Política de Segurança

Allan apresenta o processo de criação e aprovação da política de segurança da Evolveris, assim como a sua divulgação e a capacitação da equipe nos assuntos referentes à segurança da informação.

MÓDULO 07 | Documentação do PCI Council

Capítulo 27: Os documentos de Apoio

Allan apresenta os documentos disponibilizados pelo PCI Council para auxiliar as empresas na obtenção da conformidade com os padrões vigentes.

Capítulo 28: SAQ's, ROC's, AOC's e planilha de controles compensatórios

Allan explica as diferenças entre os Questionários de Auto-Avaliação (SAQ's) e Relatórios de Conformidade (ROC's), e Atestados de Conformidade (AoC), além de demonstrar os requisitos e passos para preenchimento da planilha de controles compensatórios.

PRIVACIDADE E PROTEÇÃO DE DADOS

O cuidado com as informações pessoais e como elas são manuseadas nunca foi uma preocupação como nos dias de hoje. Num mundo globalizado, proteger os dados pessoais e empresariais, é essencial. Por isso, oferecemos cursos que mostrarão ao profissional como lidar com estes percalços de acordo com as Leis de Privacidade Nacionais e Internacionais.

Adquira conhecimentos e habilidades para aplicar estratégias técnicas para mitigar o risco de Privacidade em todos os ciclos de vida de desenvolvimento de software e sistemas.

Por que fazer este curso?

Com a certificação CIPT – emitida pela IAPP (International Association of Privacy Professional), você será capaz de aplicar estratégias, políticas, processos e técnicas para gerenciar riscos de cibersegurança, ao mesmo tempo em que permitem o uso prudente de dados para fins comerciais, além disso, você também poderá:

- Criar produtos, serviços e processos amigáveis à privacidade
- Proteger os dados de várias formas de interferência
- Projetar softwares e sistemas para garantir melhor a privacidade
- Auditar e produzir soluções para problemas de privacidade

Objetivos deste curso

O objetivo deste curso é capacitar o profissional a aplicar estratégias, políticas, processos e técnicas para gerenciar riscos de cibersegurança, além de permitir o uso prudente de dados para fins comerciais.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 20 horas (online, ao vivo) de treinamento

Pré-requisitos

- Compreensão da língua inglesa (material e prova em inglês)

Público-alvo

- Profissionais de Dados
- Desenvolvedores de Software
- Auditores de TI
- Gerentes de Riscos
- Analistas de Segurança
- DPO's ou qualquer outra pessoa responsável pela proteção tecnológica nas empresas

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

Certificações do curso

Programa do curso

MÓDULO 01 | Princípios fundamentais de Privacidade em Tecnologia
- Resumo dos elementos fundamentais para incorporar privacidade em tecnologia por meio de privacidade by design e design sensível ao valor
- Análise do ciclo de vida dos dados os modelos e frameworks comuns no contexto de risco à privacidade

MÓDULO 02 | O papel do profissional de Tecnologia na Privacidade
- Revisar os fundamentos da privacidade no que se refere as questões tecnológicas
- Descrever a função do tecnólogo de privacidade para garantir a conformidade com os requisitos de privacidade e atender às expectativas de privacidade dos stakeholders
- Explorar a relação entre privacidade e segurança

MÓDULO 03 | Ameaças e violações à Privacidade
- Identificar os riscos inerentes ao longo dos estágios do ciclo de vida dos dados e explorar como a segurança do software ajuda a mitigar ameaças à privacidade
- Examinar os impactos que a publicidade comportamental, o cyberbullying e a engenharia social têm na privacidade no ambiente tecnológico

MÓDULO 04 | Medidas técnicas e tecnologias para aumentar a Privacidade
- Descrever as estratégias e técnicas para aumentar a privacidade ao longo do ciclo de vida dos dados, incluindo gerenciamento de identidade e acesso, autenticação, criptografia e agregação
- Coleta e uso de informações pessoais

MÓDULO 05 | Engenharia de Privacidade
- Explorar o papel da Engenharia de Privacidade em uma organização, incluindo os objetivos de Engenharia de Privacidade, padrões de design de privacidade e riscos de privacidade de software

MÓDULO 06 | Metodologia de Privacy by design
- Ilustrar o processo e a metodologia do privacy by design
- Explorar práticas para garantir vigilância contínua ao implementar privacy by design

MÓDULO 07 | Desafios de Tecnologia para Privacidade

- Examinar os desafios únicos que vêm de questões de privacidade on-line, incluindo tomada de decisão automatizada, tecnologias de rastreamento e vigilância, antropomorfismo, computação ubíqua e computação social móvel

Faça a diferença na sua organização e na sua carreira. Seja um líder em administração de programas de privacidade e tenha os bens para estabelecer, manter e gerenciar um programa de privacidade em todos os estágios de seu ciclo de vida.

Por que fazer este curso?

Com a certificação CIPM – emitida pela IAPP (International Association of Privacy Professional), você será capaz de criar um programa de gerenciamento de privacidade, e também poderá:

- Avaliar riscos
- Realizar operações de Privacidade e análise de dados
- Realizar auditorias
- Acessar a maior comunidade de profissionais de privacidade do mundo

Objetivos deste curso

O objetivo deste curso é capacitar o profissional a entender as regulamentações de Privacidade de dados e fazê-las funcionarem dentro de uma organização, além de criar uma visão da empresa, estruturar uma equipe de Proteção de Dados, desenvolver e implementar estruturas de sistema, medir o desempenho, etc.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 16 horas (online, ao vivo) de treinamento

Pré-requisitos

- É recomendável que você tenha conhecimento nas Leis de Privacidade

Público-alvo

- Profissionais que desejam alcançar posições como a de DPO (Data Protection Officer)

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

Certificações do curso

Programa do curso

MÓDULO 01 | Desenvolvendo um Programa de Privacidade
- Criar uma visão da empresa
- Estabelecer um modelo de governança de dados
- Estabelecer um programa de privacidade
- Estruturar a equipe de privacidade
- Comunicar-se

MÓDULO 02 | Estruturando um Programa de Privacidade
- Desenvolver a Estrutura do Programa de Privacidade
- Implementar a Estrutura do Programa de Privacidade
- Desenvolver Métricas Apropriadas

MÓDULO 03 | Ciclo de vida operacional de Privacidade: Avaliação
- Documentação da linha de base atual do seu programa de privacidade
- Avaliação de processadores e fornecedores terceirizados
- Avaliações Físicas
- Fusões, aquisições e alienações
- Avaliações de impacto de privacidade e avaliações de impacto de proteção de dados

MÓDULO 04 | Ciclo de vida operacional de Privacidade: Proteger
- Práticas de segurança da informação
- Privacidade por Design
- Integrar requisitos de privacidade e representação em áreas funcionais em toda a organização
- Outras medidas organizacionais

MÓDULO 05 | Ciclo de vida operacional de Privacidade: Sustentar
- Monitorar
- Auditar

MÓDULO 06 | Ciclo de vida operacional de Privacidade: Resposta
- Solicitações de informações do titular dos dados e direitos de privacidade
- Resposta a incidentes de privacidade

Mostre ao mundo que você conhece as leis e regulamentos de privacidade de dados e como aplicá-los. Demonstre seu domínio das leis, regulamentos e modelos de execução jurisdicionais, além de requisitos legais para manuseio e transferência de dados.

Por que fazer este curso?

Ao fazer este curso, você terá o conhecimento, perspectiva e compreensão abrangentes da GDPR para garantir o sucesso de conformidade e Proteção de Dados na Europa. Além disso, você poderá:

- Conhecer a Proteção de Dados Europeia
- Compreender o cumprimento da Lei e Regulação Europeia de Proteção de Dados
- Entender as transferências internacionais de dados
- Aprender mais sobre as Instituições Reguladoras Europeias

Objetivos deste curso

O objetivo deste curso é capacitar o profissional a conhecer e compreender a perspectiva abrangente na GDPR Europeia a fim de garantir o sucesso da conformidade e da Proteção de Dados na Europa.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 20 horas (online, ao vivo) de treinamento

Pré-requisitos

- Não há

Público-alvo

- Advogados
- Profissionais de TI e Segurança da Informação
- Encarregados de Proteção de Dados (DPO)
- Compliance Officers
- Cientistas de Dados
- Qualquer profissional que utilize dados pessoais em suas atividades

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

Certificações do curso

Programa do curso

MÓDULO 01 | Introdução à Proteção de Dados Europeia
- Origens e Contexto Histórico da Lei de Proteção de Dados
- Instituições da União Europeia
- Quadro Legislativo

MÓDULO 02 | Lei e Regulamentação Europeia de Proteção de Dados
- Conceitos de proteção de dados
- Âmbito Territorial e Material do Regulamento Geral de Proteção de Dados
- Princípios de Processamento de Dados
- Critérios de Processamento Legal
- Obrigações de Prestação de Informações
- Direitos dos Titulares dos Dados
- Segurança de Dados Pessoais
- Requisitos de responsabilidade
- Transferências Internacionais de Dados
- Supervisão e execução
- Consequências das violações do GDPR

MÓDULO 03 | Conformidade com a Lei e Regulamentação Europeia de Proteção de Dados
- Relação de emprego
- Atividades de Vigilância
- Marketing direto
- Tecnologia e Comunicações da Internet

Seja um profissional de destaque para o cargo de Encarregado de Proteção de Dados e conquiste a certificação CDPO/BR, fornecida pela IAPP – reconhecida mundialmente como referência em Privacidade e Proteção de Dados.

Por que fazer este curso?

Os profissionais certificados com a CDPO Brasil desempenharão todas as funções de um DPO (Data Protection Officer) exigidas pela LGPD (Lei Geral de Proteção de Dados), como:

- Atender solicitações de titulares de dados
- Adotar medidas de Proteção de Dados
- Treinar equipes
- E mais...

Objetivos deste curso

O objetivo deste curso é capacitar o profissional a conhecer e compreender a Lei Geral de Proteção de Dados (LGPD) e princípios de gestão de programas de Proteção de Dados.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 24 horas (online, ao vivo) de treinamento

Pré-requisitos

- É recomendável que você tenha conhecimento nas Leis de Privacidade.

Público-alvo

- Data Protection Officer (Encarregado)
- Especialistas em privacidade e proteção de dados
- Advogados
- Profissionais da área de Compliance, Tecnologia ou Segurança da Informação
- Profissionais que trabalhem dentro do programa de conformidade em privacidade e proteção de dados de uma organização
- Profissionais que desejam iniciar uma carreira de DPO

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

RENATA AVELAR

INSTRUTORA

Advogada | Enfermeira | Gestão de Serviços de Saúde | Professora de Pós-Graduação e MBA | PDPF | ISFS

ULYSSES MACHADO

INSTRUTOR

Sócio de Aires e Levy Machado Advogados Associados; MsC (UFPE) | Esp.SI (UnB) | DPO (Exin) | Lead Implementer (ABNT/ISO)

Certificações do curso

CIPM + LGPD = CDPO BR

Programa do curso

MÓDULO 01 | LGPD - Introdução à Privacidade de Dados no Brasil

- Panorama Legislativo

MÓDULO 02 | LGPD - A Lei Geral de Proteção de Dados Brasileira

- Princípio de Processamento de Dados
- Conceitos de Proteção de Dados
- Escopo de Aplicação
- Bases Legais para o Tratamento de Dados Pessoais
- Direitos do Titular de Dados
- Transferência Internacional de Dados
- Prestação de Contas
- Supervisão e Fiscalização

MÓDULO 03 | LGPD - Legislação setorial e conformidade com a LGPD
- Governo
- Criminal
- Aplicações de Internet (Aplicativos) e Marketing Eletrônico
- Proteção à Criança
- Relação de Emprego
- Saúde
- Bancos e Instituições Financeiras
- Sigilo Profissional

MÓDULO 04 | CIPM - Desenvolvendo um Programa de Privacidade
- Criar uma visão da empresa
- Estabelecer um modelo de governança de dados
- Estabelecer um programa de privacidade
- Estruturar a equipe de privacidade
- Comunicar-se

MÓDULO 05 | CIPM - Estruturando um Programa de Privacidade
- Desenvolver a Estrutura do Programa de Privacidade
- Implementar a Estrutura do Programa de Privacidade
- Desenvolver Métricas Apropriadas

MÓDULO 06 | CIPM - Ciclo de vida operacional de Privacidade: Avaliação
- Documentação da linha de base atual do seu programa de privacidade
- Avaliação de processadores e fornecedores terceirizados
- Avaliações Físicas
- Fusões, aquisições e alienações
- Avaliações de impacto de privacidade e avaliações de impacto de proteção de dados

MÓDULO 07 | CIPM - Ciclo de vida operacional de Privacidade: Proteger
- Práticas de segurança da informação
- Privacidade por Design
- Integrar requisitos de privacidade e representação em áreas funcionais em toda a organização
- Outras medidas organizacionais

MÓDULO 08 | CIPM - Ciclo de vida operacional de Privacidade: Sustentar
- Monitorar
- Auditar

MÓDULO 09 | CIPM - Ciclo de vida operacional de Privacidade: Resposta
- Solicitações de informações do titular dos dados e direitos de privacidade
- Resposta a incidentes de privacidade

A LGPD (Lei Geral de Proteção de Dados) exige que os profissionais das empresas estejam bem capacitados e preparados para o adequado tratamento dos dados pessoais, "dados sensíveis", clientes, usuários, etc., dos mais diversos estabelecimentos que lidam com a área.

- E mais...

Por que fazer este curso?

Este curso tem o objetivo garantir ao profissional os conhecimentos sobre proteção de dados e os principais pontos da LGPD, buscando validar os seus conhecimentos acerca da organização e proteção das informações, bem como os regulamentos vigentes sobre as mesmas. Além disso, o profissional poderá

- Atender solicitações de titulares de dados
- Adotar medidas de Proteção de Dados
- Treinar equipes

Objetivos deste curso

O objetivo deste curso é capacitar o profissional a conhecer e compreender a Lei Geral de Proteção de Dados (LGPD) buscando validar seus conhecimentos acerca da organização de Proteção de informações, bem como os regulamentos vigentes sobre as mesmas.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 08 horas (online, ao vivo) de treinamento

Pré-requisitos

- Não há

Público-alvo

- Todos os profissionais que precisam conhecer ou estar atualizados quanto à privacidade e proteção de dados e dos requisitos legais brasileiros, conforme definido na LGPD

Instrutores

RENATA AVELAR

INSTRUTORA

Advogada | Enfermeira | Gestão de Serviços de Saúde | Professora de Pós-Graduação e MBA | PDPF | ISFS

Certificações do curso

Programa do curso

MÓDULO 01 | Fundamentos e regulamentações de Privacidade e Proteção de Dados

- Definições de privacidade: A LGPD (Lei Geral de Proteção de Dados Pessoais), privacidade e proteção de dados.
- Dados pessoais: Definição de dados segundo a LGPD, descrever os direitos do titular dos dados com relação aos dados pessoais, listar papeis, responsabilidades e stakeholders.
- Motivos legítimos e limitação da finalidade: Os seis motivos legítimos, especificações de propósito, proporcionalidade e a subsidiariedade.
- Outros requisitos para o tratamento legítimo de dados pessoais: Requisitos para processamento/tratamento de dados, finalidade do tratamento de dados pessoais, princípios relativos ao tratamento de dados pessoais.
- Direitos do titular dos dados: Descrever os direitos relativos ao direito de ser esquecido.
- Violação de dados e procedimentos relacionados: Violação de dados, procedimentos em uma violação de dados, diferença entre uma violação de segurança (incidente) e uma violação de dados, stakeholders que devem ser informados.

MÓDULO 02 | Organizando a Proteção de Dados

- A Importância da proteção de dados para a organização: Os diferentes tipos de administração, as atividades necessárias para o cumprimento da LGPD, dar uma definição de proteção de dados desde a concepção e por padrão, a obrigação de notificação de violação de dados estabelecida na LGPD.
- Autoridade Nacional de Proteção de Dados (ANPD): Responsabilidades Gerais de uma Autoridade de Proteção de Dados.
- Normas Corporativas Globais e proteção de dados em contratos: Descrever o conceito de Normas Corporativas Globais, formalização da privacidade em contratos escritos entre o controlador e o operador.

MÓDULO 03 | A prática da Proteção de Dados

- Privacidade por design e privacidade por padrão relacionadas à Segurança da Informação: Os benefícios da aplicação dos princípios da privacidade desde a concepção e por padrão, os sete princípios da privacidade por design e a relação entre privacidade e segurança da informação.
- Relatório de impacto sobre a proteção de dados (RIPD): Descrever o que é um RIPD e quando aplicar um RIPD.
- Aplicações relacionadas ao uso de dados, marketing e mídias sociais: Gerenciamento do ciclo de vida de dados (GCVD), definição de cookie e o que ele faz, informações de mídia social são usadas para atividades de Marketing.

Você pretende no futuro tornar-se um Data Protection Officer (DPO)? Essa certificação EXIN Privacy & Data Protection Foundation (PDPF) é um dos cursos para se obter o título de DPO da EXIN.

Por que fazer este curso?

Este curso tem o objetivo garantir ao profissional os conhecimentos necessários para garantir a conformidade com a regulamentação GDPR (General Data Protection Regulation). Além disso, o profissional poderá:

- Listar os direitos, papeis, responsabilidades e partes interessadas definidas na GDPR
- Descrever o que é um Relatório de Impacto sobre a Proteção de Dados (RIPD) e quando aplicar
- Conhecer as definições válidas de Privacidade
- Relacionar Privacidade com dados pessoais, ao conceito de Proteção de Dados

Objetivos deste curso

O objetivo deste curso é capacitar o profissional a conhecer e compreender a Lei Geral de Proteção de Dados (LGPD) buscando validar seus conhecimentos acerca da organização de Proteção de informações, bem como os regulamentos vigentes sobre as mesmas.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 16 horas (online, ao vivo) de treinamento

Pré-requisitos

- Não há

Público-alvo

- Data Protection Officers (DPO)
- Compliance Officers
- Security Officers
- Funcionários de RH
- Gerentes de Processos e de Projetos

Instrutores

RENATA AVELAR

INSTRUTORA

Advogada | Enfermeira | Gestão de Serviços de Saúde | Professora de Pós-Graduação e MBA | PDPF | ISFS

Certificações do curso

Programa do curso

MÓDULO 01 | Fundamentos de Privacidade e regulamentações

- Definições de privacidade: A GDPR (General Data Protection Regulation), Privacidade e Proteção de Dados.
- Dados pessoais: Definição de Dados segundo a GDPR, distinção entre dados pessoais e categorias especiais como dados pessoais sensíveis, processamento de dados pessoais, papeis, responsabilidades e stakeholders.
- Motivos legítimos e limitação da finalidade: Os seis motivos legítimos, especificações de propósito, proporcionalidade e a subsidiariedade.
- Outros requisitos para o tratamento legítimo de dados pessoais: Requisitos para processamento de dados, finalidade do tratamento de dados pessoais, princípios relativos ao tratamento de dados pessoais.
- Direitos dos proprietários dos dados: Descrever os direitos relativos a portabilidade dos dados e a inspeção, direito de ser esquecido e proteção de dados por design e por padrão.
- Violação de dados e procedimentos relacionados: Violação de dados, procedimentos em uma violação de dados, exemplos de violações de dados, diferença entre uma violação de segurança (incidente) e uma violação de dados, stakeholders que devem ser informados.

MÓDULO 02 | Proteção de dados da organização

- A Importância da Proteção de Dados para a organização, Os diferentes tipos de administração, as atividades necessárias para o cumprimento do GDPR, exemplos de violações de dados, a obrigação de notificação de violação de dados estabelecida no GDPR, a aplicação das regras mediante a emissão de sanções, incluindo multas administrativas.
- Autoridades de Proteção de Dados: Responsabilidades gerais de uma Autoridade de Proteção de Dados, o papel e a responsabilidade de uma Autoridade de Proteção de Dados relacionadas com violações de dados, Autoridade de Proteção de Dados.
- Dados pessoais transferidos a outros países: Transferência de dados dentro da União Europeia, fora da União Europeia e entre a União Europeia e os Estados Unidos.
- Vinculando regras corporativas e privacidade aos contratos: Descrever o conceito de regras corporativas vinculativas (BCR), formalização da privacidade em contratos escritos entre o controlador e o processador, cláusulas do contrato escrito.

MÓDULO 03 | A prática da Proteção de Dados

- Privacidade por design e Privacidade por padrão relacionadas a Segurança da Informação: Os benefícios da aplicação dos princípios da privacidade, design e privacidade por padrão, os sete princípios da privacidade por design e a relação entre Privacidade e Segurança da Informação.
- Avaliação do impacto sobre a privacidade (PIA) e auditoria de privacidade: Definição de PIA (Privacy impact assessment) e quando aplicar um PIA, os oito objetivos de um PIA, os tópicos de um relatório PIA, o objetivo de uma auditoria e o conteúdo de um plano de auditoria.
- Aplicações relacionadas ao uso de dados, marketing e mídias sociais, gerenciamento do ciclo de vida de dados (DLC), retenção de dados e minimização, definição de cookie e o que ele faz, informações de mídias sociais são usadas para atividades de Marketing.

Dê o último passo para se tornar DPO (Data Protection Officer) e conquistar a Certificação EXIN em Privacy and Data Protection Practitioner (PDPP). Este curso desenvolve conhecimento detalhado para fazer implementações a fim de atender aos requisitos do escopo da GDPR e da LGPD.

Por que fazer este curso?

Além de você se tornar apto para realizar a prova da Certificação Privacy and Data Protection Practitioner (PDPP) – emitida pela EXIN e ser uma das certificações que compõem a formação DPO (Data Protection Officer), você será capaz de compreender noções práticas da Lei, além disso, você também poderá:

- Realizar Avaliação de Impacto de Proteção de Dados (DPIA)
- Trabalhar com DPO (Data Protection Officer) no Brasil e na Europa
- Gerenciar e organizar a Proteção de Dados
- Analisar violações de dados, notificação e resposta a incidentes

Objetivos deste curso

O objetivo deste curso é capacitar o profissional a conhecer e compreender a legislação de Privacidade e Proteção de Dados Europeia e sua relevância internacional, aplicando-a à sua prática profissional diária.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 24 horas (online, ao vivo) de treinamento

Pré-requisitos

- Conhecer os fundamentos da GDPR ou ter realizado o curso de Privacy and Data Protection Foundation (PDPF)

Público-alvo

- Data Protection Officers (DPO's)
- Privacy Officers
- Legal / Compliance Officers
- Security Officers
- Gerentes de Continuidade de Negócios
- Controladores de Dados
- Auditores de Proteção de Dados
- Analista de Privacidade
- Gerentes de RH

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

AFONSO COELHO

INSTRUTOR

ISF Country Manager | CDPSE | CHFI | CISA | DPO

Certificações do curso

EXIN Privacy & Data Protection PRACTITIONER Certified by EXIN

Programa do curso

MÓDULO 01 | Políticas de Proteção de Dados

- O aluno compreende o objetivo da Proteção de Dados / políticas de privacidade dentro de uma organização, as políticas e procedimentos necessários dentro de uma organização para cumprir a legislação de proteção de dados e o conteúdo das políticas
- O aluno compreende a proteção de dados por design e, por padrão, o conceito de proteção de dados por design e por padrão, os sete princípios para proteção de dados por design e por padrão e como os princípios de privacidade por projeto e por padrão podem ser implementados

MÓDULO 02 | Gerenciando e organizando a Proteção de Dados

- O aluno aprende a aplicar as fases do Data Protection Management System (DPMS), ilustram como aplicar a fase 1 a 4 (preparação, organização, Desenvolvimento e Implementação, Governança, avaliação e aprimoramento) do DPMS
- O aluno aprende a aplicar a teoria de um plano de ação para conscientização de proteção de dados e compor um plano de ação para conscientização da proteção de dados em uma situação específica

MÓDULO 03 | Funções do Controlador, Processador e Data Protection Officer (DPO)

- O Aluno compreenderá as funções do Controlador e do Processador, compreenderá as responsabilidades do Controlador e do Processador e explicará a relação entre o Controlador e o Processador em uma situação específica
- O aluno compreenderá o papel e as responsabilidades de um DPO, entenderá quando um DPO e obrigatório sob o GDPR, entenderá o papel do DPO e a posição do DPO em relação a autoridade supervisora

MÓDULO 04 | Avaliação de Impacto de Proteção de Dados (DPIA)

- O Aluno compreenderá os critérios para uma DPIA, aprenderá a realizar um DPIA e compreenderá os objetivos e resultados de uma DPIA
- O aluno compreenderá as etapas de um DPIA e será capaz de descrever os passos de um DPIA e executar um DPIA em uma situações específicas

MÓDULO 05 | Violações de Dados, notificação e resposta a incidentes

- O aluno compreenderá os requisitos relacionados a vazamentos de dados pessoais e avaliar se uma violação de dados ocorreu nos termos da GDPR
- O aluno compreenderá os requisitos para notificação da autoridade supervisora e os titulares dos dados sobre uma violação de dados pessoais e compreenderá os elementos da obrigação de documentação da GDPR

Se você já é ou pretende ser DPO (Data Protection Officer), este é o curso ideal para você – ele te fornecerá os conhecimentos mais amplos da GDPR (General Data Protection Regulation), além das competências para assumir o papel e desempenhar as atividades adequadas de implementação e manutenção em uma organização.

Por que fazer este curso?

Além de você se tornar apto para realizar as provas das Certificações Privacy and Data Protection Foundation (PDPF) e Privacy and Data Protection Practitioner (PDPP) – emitidas pela EXIN , você será um DPO (Data Protection Officer), além disso, você estará pronto para:

- Garantir que a organização esteja consciente e treinada sobre todas as obrigações da GDPR e LGPD
- Realizar auditoria para garantir compliance
- Receber comunicações de órgãos reguladores e adotar as providências cabíveis
- Auxiliar no desenvolvimento de produtos, serviços e práticas por meio da adoção de metodologias como: Privacy by design e Data Protection by design

Objetivos deste curso

O objetivo deste curso é capacitar o profissional a conhecer os conceitos e princípios fundamentais da Proteção de Dados e os principais requisitos do Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e da Lei Geral de Proteção de Dados (LGPD) no Brasil.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 32 horas (online, ao vivo) de treinamento

Pré-requisitos

- Para realizar a prova de certificação Privacy and Data Protection Practitioner (PDPP), é necessário participar do treinamento e fazer atividades complementares. Requisito exigido pela EXIN.

Público-alvo

- Todos os profissionais que estarão à frente dos projetos de adequação à privacidade e proteção de dados

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

RENATA AVELAR

INSTRUTORA

Advogada | Enfermeira | Gestão de Serviços de Saúde | Professora de Pós-Graduação e MBA | PDPF | ISFS

AFONSO COELHO

INSTRUTOR

ISF Country Manager | CDPSE | CHFI | CISA | DPO

Certificações do curso

EXIN Privacy & Data Protection FOUNDATION Certified by EXIN

EXIN Privacy & Data Protection PRACTITIONER Certified by EXIN

Programa do curso

MÓDULO 01 | PDPF - Fundamentos de Privacidade e regulamentações

- Definições de privacidade: A GDPR (General Data Protection Regulation), Privacidade e Proteção de Dados.
- Dados pessoais: Definição de Dados segundo a GDPR, distinção entre dados pessoais e categorias especiais como dados pessoais sensíveis, processamento de dados pessoais, papeis, responsabilidades e stakeholders.

- Motivos legítimos e limitação da finalidade: Os seis motivos legítimos, especificações de propósito, proporcionalidade e a subsidiariedade.
- Outros requisitos para o tratamento legítimo de dados pessoais: Requisitos para processamento de dados, finalidade do tratamento de dados pessoais, princípios relativos ao tratamento de dados pessoais.
- Direitos dos proprietários dos dados: Descrever os direitos relativos a portabilidade dos dados e a inspeção, direito de ser esquecido e proteção de dados por design e por padrão.
- Violação de dados e procedimentos relacionados: Violação de dados, procedimentos em uma violação de dados, exemplos de violações de dados, diferença entre uma violação de segurança (incidente) e uma violação de dados, stakeholders que devem ser informados.

MÓDULO 02 | PDPF - Proteção de dados da organização

- A Importância da Proteção de Dados para a organização, Os diferentes tipos de administração, as atividades necessárias para o cumprimento do GDPR, exemplos de violações de dados, a obrigação de notificação de violação de dados estabelecida no GDPR, a aplicação das regras mediante a emissão de sanções, incluindo multas administrativas.
- Autoridades de Proteção de Dados: Responsabilidades gerais de uma Autoridade de Proteção de Dados, o papel e a responsabilidade de uma Autoridade de Proteção de Dados relacionadas com violações de dados, Autoridade de Proteção de Dados.
- Dados pessoais transferidos a outros países: Transferência de dados dentro da União Europeia, fora da União Europeia e entre a União Europeia e os Estados Unidos.
- Vinculando regras corporativas e privacidade aos contratos: Descrever o conceito de regras corporativas vinculativas (BCR), formalização da privacidade em contratos escritos entre o controlador e o processador, cláusulas do contrato escrito.

MÓDULO 03 | PDPF - A prática da Proteção de Dados

- Privacidade por design e Privacidade por padrão relacionadas a Segurança da Informação: Os benefícios da aplicação dos princípios da privacidade, design e privacidade por padrão, os sete princípios da privacidade por design e a relação entre Privacidade e Segurança da Informação.
- Avaliação do impacto sobre a privacidade (PIA) e auditoria de privacidade: Definição de PIA (Privacy impact assessment) e quando aplicar um PIA, os oito objetivos de um PIA, os tópicos de um relatório PIA, o objetivo de uma auditoria e o conteúdo de um plano de auditoria.
- Aplicações relacionadas ao uso de dados, marketing e mídias sociais, gerenciamento do ciclo de vida de dados (DLC), retenção de dados e minimização, definição de cookie e o que ele faz, informações de mídias sociais são usadas para atividades de Marketing.

MÓDULO 04 | PDPP - Políticas de Proteção de Dados

- O aluno compreende o objetivo da Proteção de Dados / políticas de privacidade dentro de uma organização, as políticas e procedimentos necessários dentro de uma organização para cumprir a legislação de proteção de dados e o conteúdo das políticas
- O aluno compreende a proteção de dados por design e, por padrão, o conceito de proteção de dados por design e por padrão, os sete princípios para proteção de dados por design e por padrão e como os princípios de privacidade por projeto e por padrão podem ser implementados

MÓDULO 05 | PDPP - Gerenciando e organizando a Proteção de Dados

- O aluno aprende a aplicar as fases do Data Protection Management System (DPMS), ilustram como aplicar a fase 1 a 4 (preparação, organização, Desenvolvimento e Implementação, Governança, avaliação e aprimoramento) do DPMS
- O aluno aprende a aplicar a teoria de um plano de ação para conscientização de proteção de dados e compor um plano de ação para conscientização da proteção de dados em uma situação específica

MÓDULO 06 | PDPP - Funções do Controlador, Processador e Data Protection Officer (DPO)

- O Aluno compreenderá as funções do Controlador e do Processador, compreenderá as responsabilidades do Controlador e do Processador e explicará a relação entre o Controlador e o Processador em uma situação específica
- O aluno compreenderá o papel e as responsabilidades de um DPO, entenderá quando um DPO e obrigatório sob o GDPR, entenderá o papel do DPO e a posição do DPO em relação a autoridade supervisora

MÓDULO 07 | PDPP - Avaliação de Impacto de Proteção de Dados (DPIA)

- O Aluno compreenderá os critérios para uma DPIA, aprenderá a realizar um DPIA e compreenderá os objetivos e resultados de uma DPIA
- O aluno compreenderá as etapas de um DPIA e será capaz de descrever os passos de um DPIA e executar um DPIA em uma situações específicas

MÓDULO 08 | PDPP - Violações de Dados, notificação e resposta a incidentes

- O aluno compreenderá os requisitos relacionados a vazamentos de dados pessoais e avaliar se uma violação de dados ocorreu nos termos da GDPR
- O aluno compreenderá os requisitos para notificação da autoridade supervisora e os titulares dos dados sobre uma violação de dados pessoais e compreenderá os elementos da obrigação de documentação da GDPR

A BRA Certificadora em parceria com o IBRASPD (Instituto Brasileiro de Segurança, Proteção e Privacidade de Dados) criou um modelo de certificação inovador e efetivo em processos de Segurança, Proteção e Privacidade de Dados: CPDATASEC®.

A Antebellum, uma empresa que é referência em formação de profissionais de Segurança da Informação e Proteção e Privacidade de Dados, juntamente com a BRA Certificadora, desenvolveu um curso completamente voltado para a formação de auditores da Certificação CPDATASEC®.

Por que fazer este curso?

Além de você se tornar apto para realizar a prova da Certificação CPDATASEC® Auditor (Data Security Management System Premium Certification), você estará pronto para:

- Analisar os documentos essenciais que devem compor o sistema de Gestão da Proteção e Privacidade de Dados
- Analisar os processos e cultura da organização
- Compreender e verificar os controles de Segurança da Informação
- Compreender e verificar os controles de Proteção e Privacidade de Dados

Objetivos deste curso

O objetivo deste curso é capacitar o profissional a realizar a prova da Certificação CPDATASEC® Auditor (Data Security Management System Premium Certification), juntamente com os conceitos de Privacidade e Proteção de Dados, Segurança da Informação e Auditoria.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 40 horas de treinamento híbrido (com aulas presenciais em Belo Horizonte, MG)

Pré-requisitos

- Certificação em Segurança da Informação e/ou Privacidade e Proteção de Dados

Público-alvo

- Profissionais da área de Privacidade e Proteção de Dados com as certificações: DPO EXIN, CIPM, CDPO/BR, CIPP/E IAPP ou semelhantes
- Profissionais da área de Segurança da Informação com as certificações: CISSP, CISM, Security+ ou semelhantes

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

RENATA AVELAR

INSTRUTORA

Advogada | Enfermeira | Gestão de Serviços de Saúde | Professora de Pós-Graduação e MBA | PDPF | ISFS

ARTHUR DORIGO

INSTRUTOR

Gerente de Soluções em Compliance e Governança

Certificações do curso

Programa do curso

MÓDULO 01 | Auditor

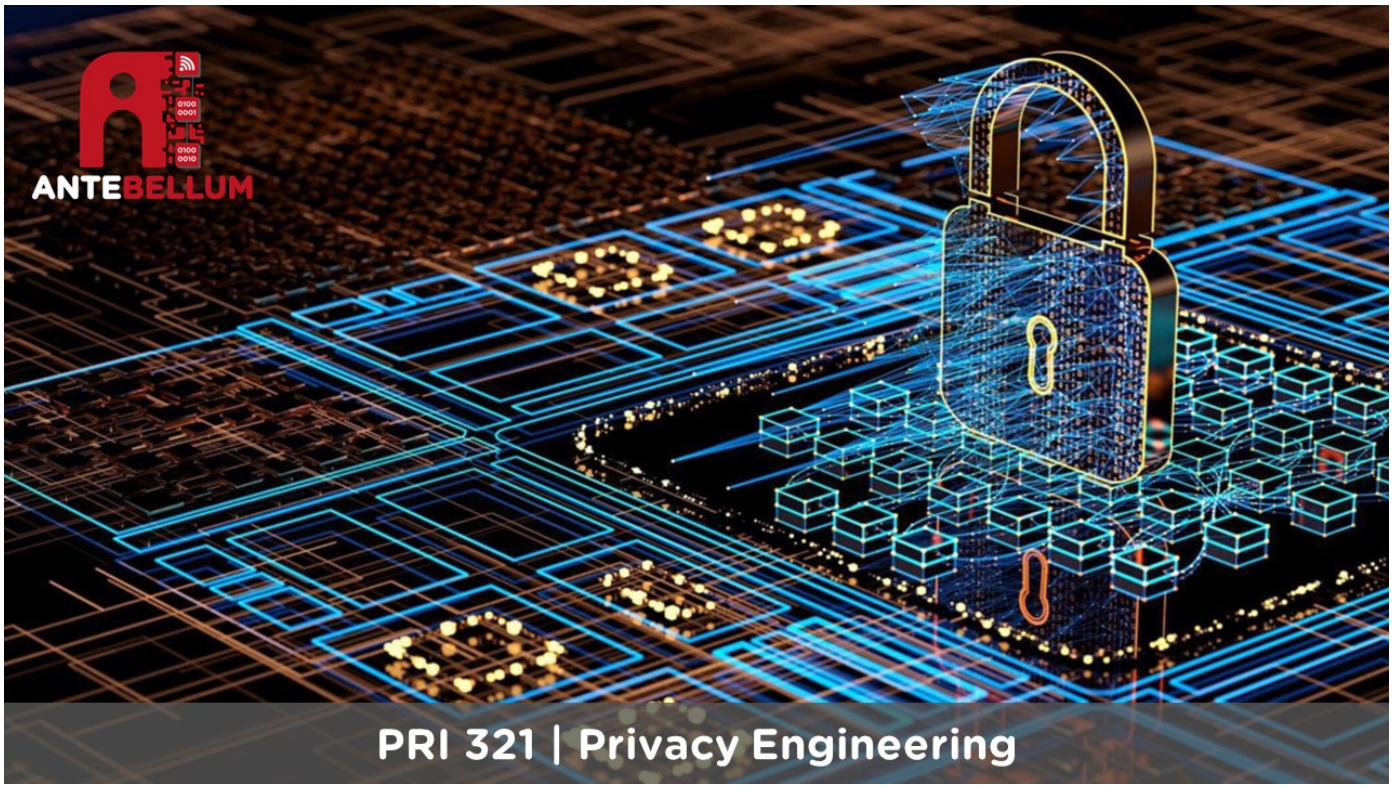
- Terminologia básica, baseados na ABNT NBR ISO 19011.2012, item 3
- Análise das informações iniciais do solicitante: Tamanho da Organização; Mercado de Atuação; Fronteiras de Atuação; Leis e Regulações Aplicáveis; Risco Reputacional; Relação com Ente Público
- Planejamento de análise da viabilidade inicial: A referência para realização do dimensionamento base será o documento IAF MD 5 2015 para auditoria de sistemas de gestão, considerando enfoque apenas na Auditoria de Processos o qual utiliza primordialmente o parâmetro de tamanho da organização como informação chave para sua aplicação
- Planejamento do tempo da auditoria presencial: O planejamento da realização da Auditoria da Cultura de proteção segurança e privacidade de dados está diretamente relacionada ao tamanho da organização mercado de atuação número de colaboradores e número de colaboradores alocados em áreas consideradas críticas (alta exposição)
- Plano de auditoria / relatório de avaliação: Trata se da Organização do tempo e Requisitos que serão avaliados e sua comunicação com os auditados. Caso seja necessário, durante a reunião de abertura os horários podem ser alterados.
- Competência e postura do auditor
- Condução da auditoria
- Registrando evidências
- Relatório de auditoria

MÓDULO 02 | Segurança da Informação

- Informação e Segurança
- Conceitos Fundamentais
- Governança e organização corporativa
- Gestão de Riscos
- Controles de Segurança da Informação (Norma ABNT NBR ISO IEC 27002:2022)
- Templates relacionados a Segurança da Informação

MÓDULO 03 | Proteção e Privacidade de Dados

- Fundamentos de Privacidade e regulamentações
- Governança e organização da privacidade e proteção de dados
- Templates relacionados a privacidade e proteção de dados



Com o crescente desenvolvimento de Projetos de Tecnologia da Informação que lidam com dados pessoais, o futuro já espera um novo membro para garantir que as políticas de privacidade sejam corretamente implementadas conforme a legislação – o Engenheiro de Privacidade.

Se você deseja ser um dos primeiros Engenheiros e ganhar reconhecimento nacional, o curso Privacy Engineering será capaz de te ensinar todas as técnicas para respeitar a privacidade dos titulares, desde a coleta dos dados até a eliminação destes.

Por que fazer este curso?

Além de garantir que as políticas de privacidade sejam corretamente implementadas conforme a legislação, você estará pronto para:

- Colaborar com as equipes de desenvolvimento de produtos de dados, criando novos usos de dados que empregam recursos de privacidade
- Atuar como interface com a equipe de usabilidade para garantir que os controles de privacidade voltados para o usuário sejam fáceis de utilizar
- Interagir com gerentes internos de programas de privacidade, equipes de desenvolvimento de produtos, equipes jurídicas de conformidade, governança e proteção de dados
- Identificar áreas de melhoria nas práticas locais relacionadas ao gerenciamento de privacidade de

Objetivos deste curso

O objetivo deste curso é preparar o estudante para desenhar os processos e sistemas dentro de uma organização garantindo a Privacidade e Proteção de Dados desde o momento de sua criação e durante todo seu ciclo de vida.

Metodologia de ensino

- Modalidade híbrida: O aluno assiste as aulas quando elas acontecem ou participa presencialmente das aulas em Belo Horizonte / MG, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 18 horas de treinamento (online, ao vivo)

Pré-requisitos

- Não há

Público-alvo

- Arquitetos de dados
- Engenheiros de dados
- Cientistas de dados
- Arquitetos de sistemas
- Desenvolvedores e UX designers
- Profissionais de Segurança da Informação
- Profissionais de Tecnologia da Informação
- Advogados de Direito Digital e Proteção de Dados

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

Certificações do curso

Não há certificações disponíveis para este curso

Programa do curso

MÓDULO 01 | Definição da Política de Privacidade
- Princípios e práticas informacionais justos (FIPPs)
- Generally Accepted Privacy Principles (GAPP)
- Taxonomia de Privacidade de Daniel Solove

MÓDULO 02 | Estratégia de Privacy by Design
- Estratégias voltadas a processos
- Estratégias voltadas a Dados
- Frameworks (ISO, NIST, Etc.)
- NIST Privacy Framework
- O design sensível ao valor (VSD)
- Privacy-Enhancing Technologies (PETs)

MÓDULO 03 | Análise de Riscos
- Incorporando Privacidade na Análise de Riscos
- Dimensões de danos de Ryan Calo
- Integridade contextual da Helen Nissenbaum
- FAIR – Factor Analisys for Information Risk

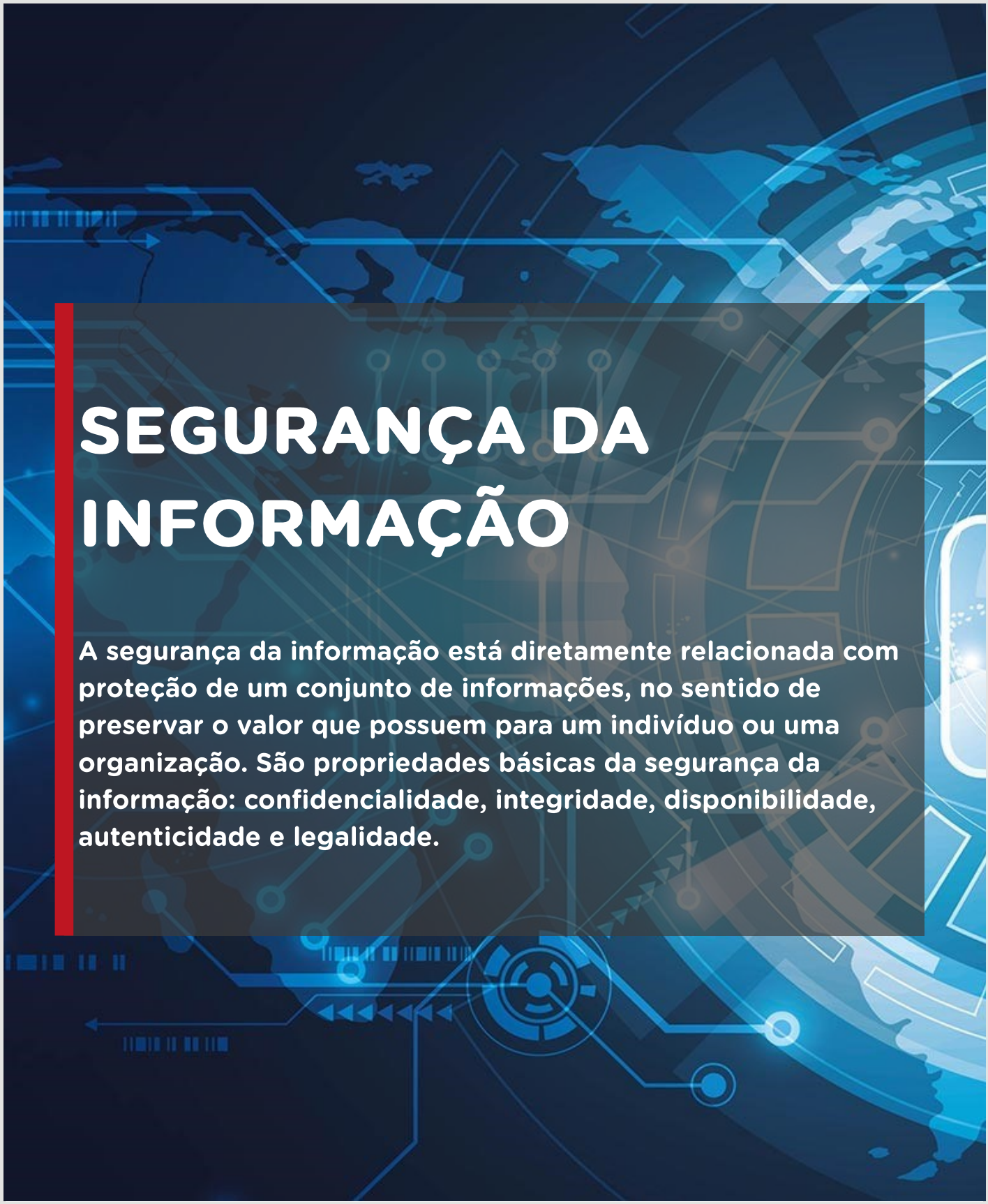
MÓDULO 04 | O Ciclo de Vida dos Dados—Coleta
- Formas de coleta de Dados
    - Coleta direta x Vigilância (ativa e passiva)
    - Consentimento explícito e implícito
- Desenho da UX para aviso e consentimento
- Dark Patterns
- Avisos de Privacidade
    - Contract Design Pattern
    - ISO 29184:2021
- Global Privacy Control
- Self-Sovereign Identity)

MÓDULO 05 | O Ciclo de Vida dos Dados—Uso/Retenção/Divulgação
- Análise dos tipos de tratamentos realizados dentro de uma organização
- O papel do Engenheiro e do Cientista de Dados extraindo informações.
- Interfaces de Privacidade
- Criptografia Segura de dados
- Criptografia Homomórfica
- Secure multiparty computation (SMPC)
- Desidentificação: Pseudonimização Segura
- Desidentificação: Anonimização efetiva
- Privacidade Diferencial
- Trusted execution environments
- Private set intersection (PSI)
- Federated learning
- Zero-knowledge proofs
- Synthetic data
- Não-repúdio

MÓDULO 06 | O Ciclo de Vida dos Dados—Destruição
- Deleção segura
- Destruição física

MÓDULO 07 | Privacidade no Desenvolvimento Seguro de Software
- Secure Development Lifecycle
- Linguagem FIDES

MÓDULO 08 | Tecnologias que impactam a privacidade
- Inteligência Artificial
- Biometria
- Computação Quântica



SEGURANÇA DA INFORMAÇÃO

A segurança da informação está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da informação: confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

Você busca um carreira em Segurança de Tecnologia da Informação? O curso Security+ é ideal para você! Ele tratará do conhecimento básico e as habilidades necessárias para avaliar o nível da segurança em um ambiente corporativo.

Por que fazer este curso?

Este curso abordará os princípios fundamentais da instalação e configuração de controles de segurança virtual e participação na resposta a incidentes e atenuação de riscos. . Além disso, você poderá:

- Identificar estratégias desenvolvidas por adversários para atacar redes e hosts e medidas utilizadas para defende-las
- Compreender o princípios da segurança organizacional e os elementos de uma política de segurança efetiva
- Instalar e configurar tecnologias de segurança de rede e de host
- Identificar estratégias para garantir a continuidade de funcionamento da empresa e recuperação de desastres

Objetivos deste curso

O objetivo deste curso é capacitar o profissional a entender as habilidades básicas necessárias para desempenhar as funções básicas de segurança e buscar uma carreira em segurança de Tecnologia da Informação (TI).

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 40 horas (online, ao vivo) de treinamento

Pré-requisitos

- Recomenda-se conhecimentos básicos em TI

Público-alvo

- Profissionais de TI
- Consultores de tecnologia
- Auditores de sistemas
- Administradores de redes
- Profissionais de Segurança em TI

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

Certificações do curso

Programa do curso

MÓDULO 01 | Ataques, ameaças e vulnerabilidades

- Engenharia Social
- Tipos de Ataque
- Tipos de Ataque as Aplicações
- Tipos de Ataque em Rede
- Atores de Ameaça, Vetores e Inteligência
- Tipos de Vulnerabilidades
- Técnicas para Security Assesment
- Teste de Invasão

MÓDULO 02 | Design e arquitetura de segurança

- Conceitos de Segurança
- Virtualização e Computação em Nuvem
- Conceitos de Desenvolvimento Seguro
- Conceitos de Autenticação e Autorização
- Resiliência Cibernética
- Segurança em Sistemas Embarcados
- Segurança Física
- Conceitos de Criptografias

MÓDULO 03 | Implementação de controles de segurança

- Protocolos
- Segurança de host e Aplicações
- Segurança de Rede
- Segurança em Redes sem Fio
- Segurança em dispositivos móveis
- Segurança em Cloud Computing
- Controles de identidade
- Controles de autenticação e autorização
- PKI

MÓDULO 04 | Operações e respostas a incidentes

- Ferramentas de Segurança
- Respostas a incidentes
- Investigação de incidentes
- Mitigação de Incidentes
- Forense

MÓDULO 05 | Governança, risco e conformidade

- Tipos de controles
- Postura de Segurança
- Políticas de Segurança

Seja o profissional de destaque em Segurança da Informação. Sendo um CISEF, você entenderá o lado técnico da segurança da informação, infraestrutura de segurança, vulnerabilidades, riscos e medidas necessárias.

Por que fazer este curso?

Além de você se tornar apto para realizar a prova da Certificação Cyber and IT Security Foundation (CISEF) – emitida pela EXIN, você será capaz de compreender o lado técnico da Segurança da Informação, além disso, você também poderá:

- Compreender a arquitetura de redes TCP/IP
- Entender algoritmos e protocolos criptográficos e quando utilizá-los
- Identificar as tecnologias de acesso e autorização
- Entender as vulnerabilidades e como explorá-las

Objetivos deste curso

O objetivo deste curso é capacitar o profissional a entender o lado técnico da Segurança da Informação, desde o contexto teórico, informações detalhadas sobre infraestrutura de segurança até vulnerabilidades, riscos e medidas necessárias.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 16 horas (online, ao vivo) de treinamento

Pré-requisitos

- Conhecimentos básicos sobre redes e desenvolvimento de aplicativos

Público-alvo

- Profissionais de Segurança da Informação
- Profissionais de TI
- Desenvolvedores
- Coordenadores
- Gerentes
- Administradores de rede
- Auditores

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

PAULO COELHO

INSTRUTOR

AWS | CCDA | CCNA | CCNP | CNE | CNI | CWNA | MCSA | VMware

Certificações do curso

EXIN Cyber & IT Security FOUNDATION Certified by EXIN

Programa do curso

MÓDULO 01 | Cybersecurity e Segurança da Informação

Apresenta as diferenças entre a tradicional Segurança da Informação e a Segurança Cibernética (Cybersecurity)

- Cibernética, Cyberspace, Cybercrime e Cyberwar
- ISO 27001 x ISO 27032
- Red Team x Blue Team

MÓDULO 02 | TCP/IP

Este módulo faz um estudo completo sobre as características do protocolo e endereçamento TCP/IP

- Nós, conexões, endereçamento TCP/IP V4 e V6
- Modelos OSI, TCP/IP e outros protocolos

MÓDULO 03 | Sistemas de computador

Capacita o estudante a explicar os componentes de diferentes sistemas operacionais e listar seus componentes, vulnerabilidades e controles de segurança.

- Arquitetura de computadores, sistemas operacionais
- Vulnerabilidades de sistemas de computador
- Medidas de segurança de sistemas de computador

MÓDULO 04 | Aplicações e bancos de dados

Apresenta ao estudante as metodologias para bordar a segurança durante o ciclo de vida de desenvolvimento de sistemas.

- Desenvolvimento seguro de aplicações (SDLC)
- Bancos de dados e suas vulnerabilidades
- Problemas de segurança e contramedidas

MÓDULO 05 | Criptografia

Os participante são apresentados aos princípios de criptografia de Bloco e Fluxo, Simétricas e Assimétricas, RSA e Curva Elíptica, estudando e diferenciando os algoritmos inseguros e seguros.

- O Princípio de Kerckoff, gerenciamento de chaves e aleatoriedade
- Performance comparada de algoritmos (Custo e tempo de processamento)
- Criptografia simétrica de Substituição e Transposição, Bloco e Fluxo (DES/3DES, RC4, AES, etc.)
- Criptografia Assimétrica (Diffie-Helman, RSA, Curva Eliptica, Assinatura de Código)
- 3 Infraestrutura de chave pública (PKI)
- Criptografia Híbrida (HTTPS, VPN, SSL/TLS, Ipsec, Etc.)

MÓDULO 06 | Gerenciamento de identidade e acesso

O módulo descreve as principais tecnologias de autenticação e autenticação, seus fatores (MFA), biometria, Single sign-on (SSO), gerenciamento de senhas e seus casos de uso.

- Identificação, autenticação, biometria, Single sign-on (SSO), gerenciamento de senhas
- Autorização, Need to Know, Menor Privilégio, Separação de Deveres (SoD), RBAC, ABAC, OpenID, OAuth.

MÓDULO 07 | Computação em nuvem

O estudante aprende a diferenciar entre os modelos de implantação, nuvem pública, privada e híbrida, os modelos de serviço SaaS, PaaS, IaaS, SECaaS e IDaaS e os riscos associados

- Nuvem pública, privada e híbrida
- Modelos SaaS, PaaS, IaaS, SECaaS e IDaaS
- Riscos de computação em nuvem

MÓDULO 08 | Exploração de Vulnerabilidades

- O estudante diferencia Black, White e Grey hat hackers, script kiddies e hackativistas, assim como as ferramentas e métodos que os cibercriminosos usam para explorar vulnerabilidades.
- Categorias de ataque & tipos de ameaças
- Atores: Black, White e Grey hat hackers, script kiddies e hackativistas)
- Ferramentas: Nmap, Metasploit, etc.

Deseja ser reconhecido pela sua empresa ou mercado, ou começar sua carreira na área de Segurança da Informação?

O curso Information Security Management Foundation (ISFS) é o curso certo para você!

O conteúdo dele foi cuidadosamente criado para fornecer todos os fundamentos de Segurança da Informação.

Por que fazer este curso?

Esta Certificação abrange os fundamentos de Segurança da Informação. Além disso, você poderá:

- Ter a compreensão de diversos aspectos importantes em Segurança da Informação
- Aumentar sua conscientização de que as informações são valiosas e vulneráveis
- Prover o entendimento das medidas de segurança que precisam ser adotadas para protege-las
- Compreender legislação e regulamentação aplicáveis a Segurança da Informação: a importância e funcionamento

Objetivos deste curso

Capacitar o estudante a conhecer os conceitos, valores, importância e confiabilidade da informação, a política de segurança e a organização de segurança, a importância das medidas de segurança, a importância e o impacto da legislação e das regulamentações.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 16 horas (online, ao vivo) de treinamento

Pré-requisitos

- Recomenda-se conhecimentos básicos de Tecnologia da Informação

Público-alvo

- Gestores, consultores, pessoal de suporte e gerentes de projetos de serviços de TI
- Analistas e gerentes de áreas de negócio (financeiro, RH, engenharia, etc)
- Desenvolvedores, integradores e arquitetos de sistemas
- Engenheiros e especialistas de rede
- Profissionais de Segurança da Informação

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

Certificações do curso

Programa do curso

MÓDULO 01 | Informação e Segurança

Apresenta os conceitos fundamentais e de construção da informação e das formas de garantir sua segurança.

- Conceitos Fundamentais – Explica os conceitos de informação em seus diversos formatos, seu ciclo de vida, as diferenças entre dados e informação e a infraestrutura básica para armazenamento e proteção damesma.
- Valor da Informação – Discorre sobre o valor estratégico da informação para as organizações, como a informação pode influenciar no desempenho da organização e como as práticas de segurança da informação protegem esse bem da organização.
- Aspectos de confiabilidade – Apresenta os aspectos da segurança da informação: Confidencialidade, Integridade e Disponibilidade (CID), detalhando seus requisitos de avaliação.

MÓDULO 02 | Alinhamento estratégico

Este módulo introduz alguns conceitos fundamentais para estabelecer a conexão entre os objetivos da área de Segurança da Informação e os objetivos de negócio das empresas.

- Governança – Apresenta um modelo de governança corporativa, a diferenciação entre governança e gerenciamento, o funcionamento e as áreas de foco da governança de TI, um exemplo de Balanced Scorecard (BSC), a relação do BSC com os objetivos de negócio, o alinhamento dos objetivos de TI/SI com o BSC e os objetivos de negócio e os processos que levam a realização dos objetivos de TI.
- Modelagem de Processos – Mostra como o processo de modelagem pode ajudar a encontrar os ativos da informação que suportam os processos mais críticos, facilitando sua classificação e uma posterior proteção proporcional à sua importância para a organização.
- Classificação da Informação – Mostra como os ativos de informação devem ser classificados por categorias, de acordo com seu valor para a organização, para que recebam uma proteção proporcional às suas necessidades de confidencialidade, disponibilidade e integridade.

MÓDULO 03 | Gestão de riscos

Este módulo apresenta os conceitos básicos de risco, gestão de riscos e análise e avaliação de riscos.

- Ameaças – Apresenta os conceitos de ameaça, vulnerabilidade e agente de ameaça.
- Tipos de Ameaça – Apresenta aos alunos os tipos mais comuns de ameaças a segurança da informação como: Código Malicioso, Vírus, Worm, Spyware, Trojan, Rootkit, Backdoor, Engenharia Social, Hacking, Hoax, Phishing Scam, Bots, Botnets, Spam e Scam.
- Dano – Discute o incidente de segurança, a probabilidade, consequência, impacto e danos diretos e indiretos à organização.
- Análise de Riscos – Explica os processos de análise (quantitativa e qualitativa) e avaliação de riscos, a relação entre uma ameaça e um risco, assim como as estratégias para tratamento dos riscos e aceitação de riscos residuais.

MÓDULO 04 | Abordagem e organização

Este módulo fornece uma visão da construção das políticas de segurança e a organização da segurança da informação.

- Políticas de Segurança – Descreve os objetivos e a composição de uma política de segurança, assim como a organização da segurança da informação.
- Organização da segurança – Apresenta fatores fundamentais para o bom funcionamento da política de segurança como: Código de Conduta, propriedade de ativos e papeis principais na Segurança da Informação.
- Gestão de Incidentes e escalação – Descreve a importância de uma rotina de gesta o de incidentes, apresentando um ciclo onde os mesmos devem ser reportados de forma correta, analisados e escalados funcional ou hierarquicamente. Descreve também os efeitos negativos de eventuais falhas neste processo.

Você deseja ser ISO (Information Security Officer)?

Então o curso Information Security Management Professional (ISMP) é ideal para você!

Ele aborda os principais assuntos relacionados à Segurança da Informação, seus riscos e possíveis formas de controle.

Por que fazer este curso?

Este curso apresentará os aspectos organizacionais e gerenciais da Segurança da Informação. Além disso, você poderá:

- Compreender os conceitos básicos de Segurança da Informação
- Gerenciar riscos e ameaças à Segurança da Informação
- Compreender os controles de Segurança da Informação: organizacionais, técnicos, físicos
- Ter perspectiva da Segurança da Informação, considerando o ponto de vista dos negócios, clientes e fornecedores

Objetivos deste curso

Capacitar o estudante a conhecer os aspectos organizacionais e gerenciais da Segurança da Informação, bem como: perspectivas em Segurança da Informação, gerenciamento de risco, controles de Segurança da Informação.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 16 horas (online, ao vivo) de treinamento

Pré-requisitos

- Recomenda-se um conhecimento prévio da norma ISO/IEC 27001 e ISO/IEC 27002

Público-alvo

- Profissionais de Segurança da Informação
- Profissionais de Tecnologia da Informação
- Profissionais de Privacidade e Proteção de Dados
- Advogados

Instrutores

FERNANDO FONSECA

INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

Certificações do curso

Programa do curso

MÓDULO 01 | Perspectiva em Segurança da Informação

Este módulo apresenta os conceitos básicos de governança (corporativa e de TI), visando criar um melhor entendimento das necessidades das empresas, facilitando o entendimento de quais devem ser os objetivos de Tecnologia da Informação e Segurança da Informação para que estas áreas estejam alinhadas às metas, missão e objetivos da alta gestão.

- Perspectiva do Negócio – Trata o papel da Segurança da Informação no negócio, e e capaz de distinguir os tipos de informação com base em seu valor para o negócio e explicar as características de um sistema de gerenciamento para segurança da informação.
    - Processos organizacionais
    - Conformidade legal e regulatória
    - Requisitos de privacidade
    - Arquitetura de segurança corporativa
    - due care

- Gestão do ciclo de vida da informação – Mostra o ciclo de vida da informação desde a criação, passando por sua classificação, categorização, propriedade, etc.
    - Tipos e classificação da informação
    - Papeis e responsabilidades de cada colaborador

- Perspectiva do Cliente – Aborda o ponto de vista do cliente sobre o controle da informação e a importância do controle da informação no processo de terceirização.
- Perspectiva do provedor de serviços / fornecedor – Aborda as responsabilidades do provedor de serviços de informação em garantir a segurança, os aspectos da segurança em processos de gerenciamento de serviços e atividades para conformidade do mesmo
    - Alinhamento dos requisitos de segurança
    - Afirmação de gestão da segurança
    - Certificação em segurança da informação
    - Auditoria de clientes

MÓDULO 02 | Gerenciamento de risco

Este módulo demonstra os conceitos de análise de riscos, apetite e tolerância a riscos e todos os conceitos e as principais normas e frameworks para a avaliação e tratamento de riscos.

- Análise e avaliação de riscos – Apresenta os princípios de gerenciamento de risco, de acordo com a classificação de cada ativo.
    - Análise dos riscos (ameaças e vulnerabilidades)
    - Avaliação dos riscos (ativos tangíveis e intangíveis)
    - Análise quantitativa
    - Análise qualitativa
    - Análise semi-quantitativa

- Controles para tratamento do risco – Foca na escolha dos controles dos riscos com base nos requisitos de Confidencialidade, Integridade e Disponibilidade (CIA) de cada ativo e nos estágios do ciclo de vida do incidente além de escolher diretrizes relevantes para a aplicação dos controles.
    - Estudo da norma ISO IEC/27005
    - Seleção de medidas de tratamento
    - Retenção do risco
    - Redução de riscos
    - Compartilhamento/transferência de riscos
    - Eliminação do risco

- Riscos residuais – Aborda os riscos residuais e as estratégias para lidar com este risco através da:
    - produção de casos de negócios para controles
    - produção de relatórios sobre as análises de risco

- Comunicação do risco – Aborda a tradução dos riscos de segurança da informação em uma linguagem gerencial para atender os requisitos da gestão e governança da empresa
    - Risk Scorecard
    - Aceitação do risco

MÓDULO 03 | Controles de Segurança da Informação

Este módulo aborda a criação de controles diversos para diminuir e monitorar o risco na organização, de acordo com o resultado da avaliação de riscos da empresa.

- O Sistema de Gestão da Segurança da Informação (SGSI) – Aborda a criação de um sistema de gestão contínua da segurança da informação, visando identificar e manter os riscos nos patamares desejáveis pela gestão e governança da organização.
    - Sistemas de gerenciamento para segurança da informação
    - O ciclo PDCA
    - Padrões de mercado (família ISO 27000, Cobit, etc)
    - Gestão de incidentes de segurança
    - Métricas de segurança
    - Conscientização dos colaboradores

- Controles Organizacionais – O aluno adquire conhecimento sobre controles organizacionais, e é capaz de redigir políticas e procedimentos de segurança da informação, implementar estratégias para gerenciamento de incidentes de segurança da informação, realizar uma campanha de conscientização na organização, implementar papeis e responsabilidades para segurança da informação:
    - Código de conduta
    - Política de Segurança da Informação
    - Procedimentos
    - Guias
    - Documentação

- Controles Técnicos – O aluno adquire conhecimento sobre controles técnicos e é capaz de explicar as arquiteturas de segurança, a finalidade dos serviços de segurança, e a importância dos elementos de segurança na infraestrutura.
    - Elementos da arquitetura de segurança
    - Princípios de desenho para serviços seguros (performance, gestão de capacidade, resiliência, funcionalidade, gerenciamento, etc)
    - Princípios de desenho para ambientes seguros (isolamento, mediação completa, resiliência, redundância, diversidade, etc)
    - Principais serviços de segurança (identificação, Autorização, Controle de acesso, hardening, etc)

- Controles Adicionais – Aborda os controles relacionados a segurança física, gestão de pessoas e desenvolvimento e teste de planos de continuidade de negócios. Dentre eles destacamos:
    - Código de conduta
    - Política de segurança da informação
    - Procedimentos de contratação
    - Conscientização e monitoração
    - Desligamento de colaboradores.

Os ISO's (Information Security Officers) são responsáveis por levar a visão de sua organização sobre segurança, incluindo processos, governança e treinamento de pessoal. Isso torna uma posição emocionante e desafiadora para qualquer profissional de segurança aspirar.

Devido à natureza em constante mudança das empresas digitalmente orientadas, o mundo da segurança da informação está se tornando cada vez mais complexo.

Por que fazer este curso?

Além de você se tornar apto para realizar as provas das Certificações Information Security Foundation (ISFS) e Information Security Management Professional (ISMP) – emitidas pela EXIN , você será um ISO (Information Security Officer), além disso, você estará pronto para:

- Gerenciar os riscos de Segurança da Informação
- Coordenar todo o processo de análise / avaliação de riscos
- Receber informações e coordenar a resposta a incidentes de segurança
- Aprovar métodos apropriados para a proteção de dispositivos móveis, redes de computadores e outros canais de comunicação

Objetivos deste curso

Capacitar o estudante a desenvolver seus conhecimentos sobre os aspectos organizacionais e gerenciais da Segurança da Informação juntamente com perspectivas em Segurança da Informação, gerenciamento de riscos, controles de Segurança da Informação.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.

Carga-horária

- 24 horas (online, ao vivo) de treinamento

Pré-requisitos

- Para realizar a prova de certificação Information Security Management Professional (ISMP), é necessário participar do treinamento e fazer atividades complementares. Requisito exigido pela EXIN.

Público-alvo

- Profissionais de Tecnologia e Segurança da Informação
- Profissionais que estarão à frente dos projetos de adequação à privacidade e proteção de dados
- Profissionais que queiram ingressar nessa área de atuação

Instrutores

FERNANDO FONSECA
INSTRUTOR

CIPM | CIPT | CDPSE | DPO | ISO | CISSP-ISSAP | CISM | ISO 27001 Lead Auditor | MCSE Security 2003 | ISFS | ISMAS and others

PAULO COELHO
INSTRUTOR

AWS | CCDA | CCNA | CCNP | CNE | CNI | CWNA | MCSA | VMware

PAULO FURIATI
INSTRUTOR

Consultor Cybersec | Diretor Capítulo ISACA-BH | Professor Universitário | LGPD | Privacidade | DPO

Certificações do curso

EXIN Information Security Management ISO/IEC 27001 FOUNDATION Certified by EXIN

EXIN Information Security Management ISO/IEC 27001 PROFESSIONAL Certified by EXIN

Programa do curso

MÓDULO 01 | Introdução

Informação e Segurança: Apresenta os conceitos fundamentais e de construção da informação e das formas de garantir sua segurança.

- Conceitos Fundamentais, Valor da Informação e Aspectos da Confiabilidade.
- Alinhamento Estratégico: Introduz alguns conceitos fundamentais para estabelecer a conexão entre os objetivos da área de Segurança da Informação e os objetivos de negócio das empresas.
- Governança, Modelagem de Processos e Classificação da Informação.

MÓDULO 02 | Perspectivas em Segurança da Informação

- Apresenta os conceitos básicos de governança (Corporativa e de TI), visando criar um melhor entendimento das necessidades das empresas, facilitando o entendimento de quais devem ser os objetivos de Tecnologia da Informação e Segurança da Informação para que estas áreas estejam alinhadas as metas, missão e objetivos da alta gestão.
- Perspectiva do Negócio; Gestão do Ciclo de Vida da Informação; Perspectiva do Cliente e Perspectiva do Provedor de Serviços/Fornecedor.

MÓDULO 03 | Gerenciamento de Riscos

- Demonstra os conceitos de análise de riscos, apetite e tolerância a riscos e todos os conceitos e as principais normas e frameworks para a avaliação e tratamento de riscos.
- Ameaças; Tipos de Ameaça; Dano e Impacto; Análise e Avaliação de Riscos; Controles para Tratamento do Risco; Riscos Residuais e Comunicação do Risco.

MÓDULO 04 | Abordagem e organização

- Fornece uma visão da construção das Políticas de Segurança e a Organização da Segurança da Informação.
- Políticas de Segurança; Organização da Segurança; Gestão de Incidentes e Escalação e Sistema de Gestão da Segurança da Informação (SGSI).

MÓDULO 05 | Controles de Segurança da Informação

- Aborda a criação de controles diversos para diminuir e monitorar o risco na organização de acordo com o resultado da avaliação de riscos e a forma como são estruturadas de acordo com sua classificação e possível impacto à organização.
- Importância das Medidas de Segurança; Segurança Física; Controles de Acesso; Controles Tecnológicos; Segurança de Software; Controles Organizacionais; Controles para Gestão de Colaboradores e Continuidade de Negócios.

MÓDULO 06 | Conformidade

- Legislação; Regulamentação e Avaliação.

“Jamais destrua seus sonhos
Destrua seus limites”

(autor desconhecido)

/cursosantebellum

/cursos.antebellum

@cursosantebellum

cursos@antebellum.com.br