Estratégias e Inteligência em Segurança da Informação*1

Todos nossos cursos são preparados por mestres e profissionais reconhecidos no mercado de Segurança da Informação no Brasil e exterior.

Os cursos são ministrados em português, espanhol ou inglês, atendendo suas necessidades locais de formação.

Os cursos são oferecidos em turmas abertas compostas no máximo por 9 alunos, podendo também ser oferecido na modalidade In Company.

A formação em segurança da informação destina-se ao seguinte público:

- Gestores, consultores e técnicos nas áreas de Segurança e Tecnologia da Informação , Auditoria , Sistemas e Compliance.

- Profissionais em geral com interesse em conhecer e aprimorar as boas práticas em segurança da informação.

A nossa formação apresenta um diferencial no mercado, onde você pode se especializar na área de seu interesse, possibilitando forte reconhecimento no mercado de trabalho.

A crescente sofisticação e barateamento da tecnologia, bem como o acesso fácil a informação propiciam situações convergentes que ameaçam de forma crescente o individuo, a empresa e a sociedade em geral, pois é cada vez mais possível que um pequeno grupo resoluto, ou até uma pessoa de forma isolada, bem financiada e bem informada poder atacar centros nervosos de nossa existência, sejam escolas, sejam hospitais, sejam empresas; por outro lado, a ínfra-estrutura de nossa vida diária – de energia a transportes e até o fornecimento de água, por exemplo – ficou tão complexa e interligada, que sua vulnerabilidade aumentou de forma exponencial. Daí a necessidade crescente de se alinhar a Estratégia com as ações de Inteligência, notadamente em relação a informação e ao conhecimento, que são as bases de sustentação do poder atualmente.

Embora melhorem os sistemas de segurança, as novas tecnologias também promovem uma exposição maior de nossa vida diária. O preço do aumento da proteção será conviver com sistemas de sensores automáticos, cameras de segurança, senhas eletrônicas, alarmes e patrulhas policiais *on-line*. Trata-se também de uma medida da relatividade do progresso humano.

A promessa da Era da Informação representa o desencadeamento de uma capacidade produtiva jamais vista, mediante o poder do capital intelectual o sonho dos pensadores Iluministas está se tornando cada vez mais possível de ser realizado. Por outro lado, há enorme defasagem entre nosso excesso de desenvolvimento tecnológico e subdesenvolvimento social, dado que os índices de desenvolvimento humano mostram uma diversidade crescente entre os países mais ricos e os mais pobres de uma forma geral e também se pode observar esta tendência na distriibuição da população dos centros urbanos mais populosos. O que pode fomentar de forma potencial a possibilidade de conflitos onde a tecnologia é usada de forma ilícita.

Diante deste cenário a Segurança da Informação é estratégica pois tende a ampliar a sua aplicabilidade na medida que os ativos ditos intangíveis se tornam cada vez mais essências para a sobrevivência das organizações.

Assim, vale relembrar que hoje a necessidade não é somente proteger os dados puros, mas também as informações e o conhecimento do negócio como um todo. Hoje é necessário manter os dados e as informações sempre disponíveis. A informação deverá estar acessível somente para pessoas autorizadas e não pode sofrer nenhuma alteração desde a sua criação até o seu armazenamento.

Para quem quer dar os primeiros passos antes de implementar a segurança da informação na empresa, precisa saber o porque e para que proteger as informações e os sistemas computacionais e aí observar os seguintes conceitos fundamentais:

- Confidencialidade: a informação estará acessível somente para pessoas autorizadas.

- Integridade: as informações e os métodos de processamento somente podem ser alterados através de ações planejadas e autorizadas.

- Disponibilidade: os usuários autorizados devem ter acesso à informação e aos ativos correspondentes, sempre que necessário para o desenvolvimento de suas atividades.

- Autenticidade: para evitar o não-repúdio, ou não recusa, deverá ser garantida a autenticidade da fonte. Esta é a garantia que o emissor de uma mensagem é quem realmente diz ser.

- Legalidade: é a situação de conformidade com as leis vigentes*2.

- Conformidade: é a situação de conformidade com as normas*3

Objetivo

Este curso permite compreender a Segurança da Informação como uma vantagem estratégica aos seus negócios, utilizando-se de técnicas de inteligência e contra-inteligência para fortalecer a sua organização e proteger suas informações sensíveis. Aprenda também os métodos utilizados na engenharia social e suas formas de proteção. Para ampliar ainda mais a proteção sobre sua empresa, entenda como ocorrem e como prevenir fraudes que podem comprometer a sua organização.

Público alvo

Gestores, consultores e técnicos nas áreas de Segurança e Tecnologia da Informação, Auditoria, Sistemas e Compliance.

Profissionais em geral com interesse em conhecer boas práticas em segurança da informação.

Benefícios

Fornecer subsídios para os alunos entenderem como funcionam os aspectos estratégicos da segurança da informação, notadamente sobre o relacionamento com iniciativas de inteligência e contra-inteligência e investigação de fraudes, permitindo que os processos internos sejam reavaliados e revisados ‘a luz de sua relevância e os riscos concernentes.

Metodologia de ensino

Exposição interativa com apresentação de estudo de casos e exercícios práticos. O curso tem como proposta preparar o participante para estar apto a estruturar e modificar processos e procedimentos da empresa alinhando as iniciativas de segurança da informação com a iniciativas de inteligência estratégica. Através de abordagem teórica e prática, com a aplicação de exemplos e debates, propicia um suporte para elucidação de dúvidas durante e após o término imediato do curso.

Pré requisitos

Não há pré-requisito específico, mas, recomenda-se que o participante tenha conhecimentos básicos sobre Processos de Negócios, Segurança da Informação e Gestão de Riscos, Tecnologia da Informação e Gestão Empresarial.

Material Didático

Apostila fornecida com os slides do curso e espaço para anotações.

Conteúdo Programático

1. Segurança como valor estratégico

    - Conceitos
    - Segurança das informações
    - CSO X CISO
    - Estratégias de redução de risco

- PCN e gerenciamento de crises
- Monitoramento de segurança
- Auditoria de Segurança

2. Inteligência e Contra-Inteligência

- Conceitos de Inteligência e Contra-Inteligência
- Espionagem e Contra-espionagem
- Coleta de informações e Sistema de Vantagem Competitiva

3. Engenharia Social

- Técnicas de Argumentação
- Técnicas de Convencimento
- Neurolinguística
- Proteções contra a engenharia social
- Estudo de Caso

4. Investigação e prevenção a Fraudes

- Conceitos sobre fraudes
- Áreas de risco para fraudes
- Fases da investigação
- Técnicas investigativas
- Investigação de Fraudes

- Apropriação indébita
- Fraudes financeiras e contábeis
- Corrupção
- Investimentos
- Seguros
- Digitais (inclui Forense Computacional)

- Prevenção a fraudes

*1 O significado da segurança da informação

Item 0 da ISO 17799:2005

Garantir a continuidade do negócio e minimizar os danos causados à empresa através da prevenção e redução dos impactos gerados por incidentes de segurança. A mesma existe para minimizar os prejuízos para a empresa.

O método PDCA - (Plan, Do, Check e Action)

É hoje o principal método da administração pela qualidade total e garantir da segurança.
Neste sentido a análise e medição dos processos são relevantes para a manutenção e melhoria dos mesmos, contemplando inclusive o planejamento, padronização e a documentação destes.

O uso dos mesmos pode ser assim descrito:

- Plan: o profissional responsável deverá definir o que quer. Deverá planejar o que será feito e estabelecer metas. Deverá definir os métodos que permitirão atingir as metas propostas.

- Do: o profissional responsável deverá tomar iniciativas como: educar e treinar as pessoas envolvidas, implementar e executar o planejado conforme as metas e métodos definidos.

- Check: o profissional responsável deverá observar os resultados obtidos e verificar continuamente os trabalhos afim de ver se estes estão sendo executados da forma definida.

- Action: o profissional responsável deverá fazer correções de rotas e tomar ações corretivas ou melhorias, caso tenham sido constatadas na fase anterior a necessidade de corrigir ou melhorar processos.

*2 Leis que aumentam a necessidade de Segurança & Controle

Sarbanes-Oxley (SOX)

É uma legislação criada após os problemas apresentados nas contabilidades das empresas Enron e WorldCom e que afeta as empresas de comércio público dos Estados Unidos.

A mesma foi criada para tentar restaurar a confiança dos investidores nos relatórios financeiros de empresas públicas. Responsabiliza pessoalmente os funcionários de uma empresa pelo fornecimento de informações financeiras públicas precisas aos investidores.
Elaborada pelos membros do congresso americano S. SARBANES e Michael OXLEY, em 2002.

Basel II Accord (Basiléia II)

Fornece diretrizes para o cálculo dos riscos (de crédito, do mercado e operacionais) de um banco. Ela visa deixar mais eficiente os esforços de um banco para o gerenciamento dos seus riscos. Porém, para conseguir isso é importante implementar com sucesso um programa de proteção das informações.

California Senate Bill (Lei das violações das informações)

Determina que as empresas que possuam negócios dentro do estado da Califórnia, informem aos seus clientes sempre que qualquer informação pessoal dos mesmos, forem expostas a terceiros de forma não sigilosa. A lei direciona as empresas a aprimorar o sigilo das informações pessoais. Além de criptografia, as empresas devem criar um programa de proteção às informações para obter o sigilo necessário.

Instrução CVM n. 358 - Art. 8

Cumpre aos acionistas, controladores, diretores, membros do conselho administrativo, membros do conselho fiscal e de quaisquer órgãos com funções técnicas ou consultivas, criados por disposição estatutária, e empregados da companhia, guardar sigilo das informações relativas a ato ou fato relevante às quais tenham acesso privilegiado em razão do cargo ou posição que ocupam, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo solidariamente com estes na hipótese de descumprimento.

O decreto GLBA (Gramm-Leachy Bliley Act)

Define o que as empresas de serviços financeiros podem fazer com as informações pessoais e confidenciais que coletam durante suas atividades.

O GLBA responsabiliza os CEOs e diretores das empresas como as pessoas responsáveis pelo mau uso das informações de identificação pessoal. A falha na conformidade com o GLBA pode incorrer em multas normativas para a instituição financeira.

*3 Normas e padrões nacionais e internacionais para a segurança da informação

Conceito: O que é Normalização

Atividade que estabelece, em relação a problemas existentes ou potenciais, prescrições destinadas à utilização comum e repetitiva com vistas à obtenção do grau ótimo de ordem em um dado contexto.
http://www.abnt.org.br

No passado não existiam normas nem procedimentos pré-estabelecidos que regulassem os procedimentos de segurança dentro das corporações. Os primeiros padrões de segurança física em informática foram definidos pelas normas:

NBR 1333 - Controle de acesso físico a CPDs.
NBR 1334 atual ABNT 11515 - Critérios de segurança física para armazenamento de dados.
NBR 1335 - Segurança de microcomputadores, terminais e estações de trabalho.
NBR 10842 - Equipamentos para tecnologia da Informação e requisitos de segurança.
NBR 12896 - Gerenciamento de senhas.

O que são as Normas BS7799, ISO .....?

Norma é um documento estabelecido por consenso e aprovado por um organismo reconhecido que fornece regras diretrizes ou características para atividades de uso comum e repetitivo e que visa à obtenção de ordenação em um dado contexto.

O departamento de comércio e indústria do Reino Unido (DTI) criou um centro de segurança de informações, que teve a tarefa de criar uma norma de segurança das informações para o Reino Unido. Desde 1989 vários documentos preliminares foram publicados.

Em 1995 surgiu a BS7799 (British Standart 7799) que é uma norma de segurança da informação.

Comitê da British Standard BS-7799

Relação de algumas das entidades que participaram do comitê da elaboração da British Standard - BS 7799:

- British Computer Society
- British Telecommunications plc
- The Business Continuity Institute
- Department of Trade and Industry (Information Security Policy Group)
- Det Norske Veritas Quality Assurance
- HMG Protective Security Authority

- Institute of Internal Auditors
- KPMG plc
- L3 Network Security

A BS7799-1, a BS7799-2, a ISO/IEC 17799 e a NBR ISO/IEC 17799

BS7799-1: É a primeira parte da norma que está homologada desde 2000. É planejada como um documento de referência para implementar "boas práticas“ de segurança da informação na empresa. Disponibiliza 148 controles divididos em dez partes distintas.

BS7799- 2: É a segunda parte da norma. Seu objetivo é proporcionar uma base para gerenciar a segurança da informação nas empresas.

ISO/IEC 17799:2005: É a versão internacional da BS7799, homologada pela ISO.(International Standartization Organization), tendo como objetivo criar normas e padrões universalmente aceitos em diversas áreas. Ela cobre os mais diversos tópicos da área de segurança da informação, possuindo um grande número de controles e requerimentos que devem ser atendidos para garantir a segurança das informações de uma empresa.

NBR ISO/IEC 17799:2005: É a segunda versão brasileira da norma ISSO sendo que a primeira versão tinha sido homologada em 2001 e lançada em Agosto 2005.

International Engineering Consortium, é uma organização voltada para o aprimoramento da indústria da informação.

Série ISO 27000

Visando reunir diversas normas de segurança da informação, a ISO criou a série 27000, com normas específicas.

Veja nosso Curso relacionado ao tema:
http://www.grupotreinar.com.br/treinamentos/seguran%C3%A7a-da-informa%C3%A7%C3%A3o/iso-27000.aspx

A norma ISO 27001:2005 é a norma BS7799-2:2002 revisada, com melhorias e adaptações.

As mudanças mais relevantes na migração para norma ISO/IEC 27001 ocorreram na estrutura do SGSI (sistema de gestão de segurança da informação), onde são destacados aspectos de auditoria interna e indicadores de desempenho do sistema de gestão de segurança da informação.

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

Explodindo a 27000

ISO 27002: Trata-se do padrão que substituiu em 2006/2007 a norma ISO 17799:2005 (o código de boas práticas).
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

ISO 27003: Esta contém recomendações para a definição e implementação de um sistema de gestão de segurança da informação.
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42105

ISO 27004: Trata-se do padrão que aborda os mecanismos de mediação e de relatório de um sistema de gestão de segurança da informação.
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42106

ISO 27005: Trata-se de uma abordagem para gestão de risco das informações numa organização.
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42107

ISO 27006: Provê um guia geral para abordagem de certificação, auditoria e homologação do sistema de gestão de segurança da informação.
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42505

AS/NZS 4360:2004

A AS/NZS 4360 (Australian Standard for Risk Management)é uma norma Australiana e Neozelandesa para gerenciamento de riscos. Foi elaborada pela Standards Austrália e Standards New Zealand através do comitê de gestão de riscos (OB-007). É uma norma genérica que fornece orientações para gerenciamento de riscos de qualquer natureza. Sua principal característica é avaliar os riscos com resultados positivos (ganhos potencias) e os

riscos com resultados negativos para esta forma fornecer uma visão única no gerenciamento de riscos.

O HIPAA - (Health Insurance Portability and Accountability Act (1996 - Congresso dos EUA)

Estabelece regulamentações federais que obrigam médicos, hospitais e outros fornecedores de assistência médica a atender à alguns padrões ao manipular informações sigilosas, como registros médicos e contas de pacientes.

A HIPAA não afeta apenas os planos de saúde e as seguradoras, mas qualquer empresa que lide com informações de pacientes.

Os seguintes pontos devem possuir garantia:

- G1: este ponto trata as informações administrativas, onde são colocadas regras, diretivas e procedimentos visando a privacidade empresarial, bem como a existência de planos para recuperação e contingência de desastres.

- G2: trata os controles físicos e regras relacionadas ao acesso físico às instalações e máquinas.

- G3: trata os controles sobre as informações intangíveis armazenadas nos sistemas computacionais das organizações. Relaciona-se ao acesso destas informações.

O Padrão de Segurança de Dados da PCI (Payment Card Industry)

O PCI é um programa de segurança da informação que define os padrões de manuseio de dados de pagamentos, sejam eles efetuados manualmente ou através da utilização de sistemas eletrônico de dados.

Veja o nosso Curso relacionado ao tema:
http://www.grupotreinar.com.br/treinamentos/seguran%C3%A7a-da-informa%C3%A7%C3%A3o/curso-pci-dss.aspx

Engloba todos os comerciantes e fornecedores de serviços que lidam com armazenamento, transmissão ou processamento de dados de cartões de crédito.

Esta é uma ação conjunta com o objetivo de reduzir as fraudes de cartões de crédito em transações on-line.

Em caso de falha ao cumprimento dos requerimentos do programa PCI ou a falta de correção das vulnerabilidades existentes, a empresa poderá ser penalizada com:

- Pagamento de multa;
- Restrições ao estabelecimento;
- Proibição permanente do estabelecimento de aceitar cartões de crédito.

The Orange Book (Truster Computer Security Evaluation Criteria)

O departamento de Defesa dos Estados Unidos (DoD 5200.28-STD) especificou um conjunto de regras a serem utilizadas no processo para classificação dos sistemas operacionais seguros. Este conjunto de regras ficou conhecido informalmente como (TCSEC) ou "The Orange Book (O Livro Laranja), devido a capa do documento ser da cor laranja.

Os níveis de segurança utilizados neste livro servem para avaliar a proteção para hardware, software e informações armazenadas nos sistemas de computadores.

O "Red Book" (Livro Vermelho) foi uma adaptação do livro laranja para os aspectos relacionados a rede de computadores.

A partir da criação do Orange Book foi possível a produção de uma larga quantidade de documentos ditos "técnicos" que representaram o primeiro passo na formação de uma norma coesa e completa sobre a segurança da informação.


GRUPO
TREINAR