Curso Governança em Segurança da Informação

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.

Os investimentos em Segurança da Informação já estão na lista de prioridades dos CIOs de grandes corporações há tempos, todavia esta preocupação já começa a ser questionada do ponto de vista estratégico, notadamente sob a ótica do gerenciamento de risco. Organizar a TI para crescer de forma sustentável é um objetivo comum das organizações, no entanto ao dar

os primeiros passos as questões de governança da sua segurança se tornam cada vez mais prioritárias, tornando cada vez mais claro que há um GAP entre o que existe hoje de real na maioria delas e a distância que tais empresas ainda precisam percorrer para sua governança sob os aspectos e enfoques de um sistema efetivo de gestão da segurança da informação - SGSI com a Gestão de Riscos. Enquanto a Gestão da Segurança da Informação atende as demandas pontuais (visão de curto prazo ou operacional) para garantir confidencialidade, integridade e disponibilidade dos ativos, a Governança da Segurança da Informação alinha as ações de Governança aos objetivos estratégicos da organização, o que permite a área de Segurança da Informação venha agregar valor ao negócio e esteja apta para atender não somente as demandas atuais mais também as futuras.

Nesse contexto fica evidente que governar a Segurança da Informação é uma tarefa complexa, que exige o apoio da alta direção e que é mais facilmente atendida quanto maior for o nível de maturidade do processo de gestão da segurança da informação.

Esta visão deve partir desde a criação de plano formal de negócios e preparar a organização para eventuais incertezas, desenvolver um modelo de governança compatível com o futuro planejado, que permite identificar e gerir os riscos associados ao negócio, levando-se em conta que na avaliação dos riscos potenciais não passará despercebido os temas ligados a ações de hackers e vírus, eventuais perda de informações dos clientes, indisponibilidade operacional, falha de conduta e falta ética de parceiros e colaboradores, roubo de propriedade intelectual, espionagem, vazamento de informações e até fraude.

Neste esforço, a experiência nos diz que ainda há uma enorme dificuldade em demonstrar para a alta direção das organizações, o valor real da Segurança da Informação e o retorno do investimento necessário nessa área quando ainda não ocorreu um incidente grave de segurança. O mesmo se passa frequentemente na implementação de um sistema de gestão de continuidade de negócio, por exemplo.

Para os dirigentes de uma organização o número de vulnerabilidades corrigidas em determinada aplicação ou a quantidade de ataques sofridos no último mês não são informações relevantes se não forem relacionadas com as principais interrupções nos principais processos de negócio, ou prejuízos de ordem financeira. Daí a importância em direcionar as ações e o planejamento da gestão de maneira que “falem a mesma língua” da direção do negócio.

Esta capacitação que propomos habilita o participante a ampliar o conhecimento sobre a Governança da Segurança da Informação, sua importância estratégica e descreve detalhadamente os seus principais componentes. Por outro lado, dá subsídios para que a Governança Corporativa possa interagir e controlar a Governança de TI nos seus aspectos relativos ‘a segurança da informação permitindo que a organização estabeleça seus objetivos, determine os meios necessários para alcançá-los e monitore seu desempenho com elementos garantidores suportados por um SGSI.

Sempre é bom lembrar que a visão integrada da segurança da informação e as novas quatro “ondas” (mobilidade, social network, cloud e Big data) que estão se “quebrando” sobre as empresas e a própria indústria de TI vão provocar uma descontinuidade na maneira de como se adquire e usa tecnologia garantindo a confiabilidade, disponibilidade e integridade das informações que a partir desta nova visão será distribuída e gerenciada por toda a cadeia produtiva, indo desde a indústria até o ponto de venda. Mas para “surfar estas ondas” de forma segura temos que ir além das tecnologias que as suportam, e para isso precisamos dar muita atenção à preparação, contratação e reciclagem dos profissionais de TI, processos e todos os componentes envolvidos com a segurança de forma ampla e de todo risco relacionado.

Este conteúdo aborda várias metodologias, modelos de boas práticas, frameworks e normas ISO, partindo-se de um tópico muito comum da administração baseado na ferramenta da qualidade, o enfoque PDCA. Esta ferramenta visa garantir o alcance das metas necessárias à sobrevivência dos negócios e, embora simples, representa um avanço sem limite para o planejamento eficaz e também é a base do planejamento para a Governança com foco na segurança da informação.

Este ciclo é necessário para que todas as experiências sejam constantemente revisadas, para que os ajustes sejam realizados e para que o aprendizado com os erros seja possível. Desta forma é possível sempre identificar necessidades de melhoria, principalmente nas áreas suportadas por processos de apoio onde os recursos em todos os sentidos são mais escassos, devendo dessa forma alcançar a melhor produtividade possível nos processos implantados.

Diversos fatores influenciam a implantação de uma Governança de Segurança da Informação, começando pela nomenclatura, *dialeto* um tanto estranho à realidade dos principais executivos das empresas. O Perfil do profissional gestor de TI é outro fator que é decisivo para o sucesso de um projeto desse nível. Além das habilidades técnicas, tornam-se necessárias outras características, como um perfil de negociador e de liderança transformacional independente da hierarquia que ocupa. O gestor deve buscar obter alinhamento estratégico da segurança da informação. A organização precisa, por exemplo, desenvolver e divulgar de forma conjunta com

a Governança em geral uma politica de segurança da informação de acordo com um plano de continuidade de negócio, se possível.

Já no que diz respeito a gestão de riscos as diretrizes gerais devem focar em uma análise sistemática e avaliação dos riscos, identificar, monitorar e reportar incidentes de segurança, estimar e reduzir a probabilidade e o impacto dos riscos.

A Governança em Segurança da informação deve ter como diretrizes mestras o Alinhamento Estratégico, a Gestão de Riscos, Gestão de Infraestrutura (incluindo todos os recursos de forma eficaz), Gestão de Indicadores de Desempenho de Segurança da Informação e principalmente estar alinhada a entrega de Valor do negócio como um todo.

Sobre a gestão de desempenho através de indicadores é bom frisar que não basta criar e implementar controles, é preciso checar a eficácia dos mesmos. Exemplos de metas para monitorar esse objetivo: número de incidentes e quantidade de sistemas que não atendem aos requisitos de segurança.

Minimizar o impacto de incidentes e reduzir a probabilidade de interrupção dos serviços são exemplos de metas que podem ser utilizadas para verificar se a organização está alcançando seu objetivo principal, a entrega de valor.

Objetivo

A capacitação em Governança da Segurança da Informação tem como objetivo qualificar profissionais para conduzir ou coordenar as áreas de segurança da informação de uma organização, de maneira objetiva e eficaz, alinhando-a aos objetivos de negócio da organização e tornando-a uma área estratégica para o sucesso da empresa.

Este curso tem como objetivo prover conhecimentos Gerenciais da aplicabilidade das Normas ISO 27000, ISO 27004, ISO 27005, NBR ISO 31000, se aprofundando em sua contextualização de acordo com os objetivos estratégicos da organização e o relacionamento com gerenciamento de Risco, com grande enfoque em Gestão de Continuidade de Negócios através de uma proposta que inclui conceitos de gestão de projetos para a implantação de Governança da Segurança da Informação.

Público alvo

Gestores e coordenadores da área de Segurança da Informação, Tecnologia da Informação, Controles Internos, Prevenção à Fraude e Gestão de Risco que buscam conhecer e implantar as melhorias nos processos e nas áreas de Segurança da Informação de suas organizações. Dentre os quais podemos destacar:

- Analistas das mais diversas áreas que tem como objetivo implementar, do ponto de vista estratégico, melhorias nos processos de Segurança da Informação;
- Profissionais responsáveis pela implementação e gestão da ISO/IEC 27001 e ISO/IEC 20000-1 em cujas organizações há uma preocupação de alinhamento estratégico entre todas as áreas envolvidas com segurança e gestão do risco;
- Gestores e coordenadores da área de Segurança da Informação, Gestão de Risco e Controles Internos;
- Executivos e Gerentes responsáveis pelo Planejamento Estratégico de TI e Segurança da Informação.

Benefícios

Conhecer mais profundamente Governança de Segurança da Informação visa:

- Reduzir o custo operacional, pois mitiga os fatores de risco que podem comprometer e interromper os processos;
- Reduzir a probabilidade de vazamento de informações identificando e priorizando os principais processos que a segurança da informação necessita implantar;
- Proteger da imagem da organização;
- Aumentar o grau de confiança no relacionamento com a cadeia de valor (funcionários, clientes, fornecedores e parceiros);
- Aprimorar a Segurança da informação de forma geral, permitindo:
  - Saber como desenvolver e implantar os principais documentos reguladores da segurança da informação;
  - Conhecer os principais indicadores de gestão para segurança da informação;
  - Avaliar um modelo para evolução e governança de segurança da

informação tendo como base as ISO 27000, ISO 31000 e o COBIT;

- Decidir sobre os riscos e controles necessários para que a segurança da informação apresente os resultados desejados.

Metodologia de ensino

Exposição interativa com apresentação de estudo de casos e exercícios práticos.

Pré-requisitos

Não existem pré-requisitos mandatórios para este treinamento; no entanto, experiência de trabalho em segurança de TI, melhoria de processos ou Serviços de TI é recomendada, bem como conhecimentos básicos da língua inglesa, na parte de leitura especificamente, dado que muitos materiais e referencias ainda se encontram neste idioma.

Carga Horária:

40 horas (08:30h às 17:30h) – 5 dias

Conteúdo Programático

1. **Governança em Segurança da Informação**

- O que é governança?
- COSO.
- Governança Corporativa.
- A importância da Gestão de Pessoas na Governança.
- Objetivos de Governança.
- Governança de TI e Fundamentos de COBIT.
- Governança em Segurança da Informação.
- Benefícios e Resultados da Governança em Segurança.
- Características de uma Governança em Segurança eficaz.
- Responsabilidades na Governança em Segurança.
- Plano de Segurança Empresarial (PES).
- Segurança Orgânica.
- Arquitetura de Segurança.

- Framework SABSA.
- Eficiência e maturidade da Governança em Segurança.

2. Segurança da Informação como Valor Estratégico

- Papel estratégico da Segurança da Informação.
- Visão executiva da área de segurança.
- Papéis e responsabilidades de Segurança da Informação.
- Organograma da área de Segurança da Informação.
- Estratégias de redução de risco.
- Monitoramento e Auditoria de Segurança.
- Gestão Executiva e Gestão da Segurança.

3. ISO 27001 - Sistema de Gestão de Segurança da informação

- Sistema de Gestão de Segurança da Informação.
- Modelo PDCA.
- Estabelecimento, Implementação e Operação do SGSI.
- Monitoramento e Análise Crítica do SGSI.
- Manutenção e Melhoria do SGSI.
- Requisitos de Documentação e Controle de Registros.
- Requisitos Adicionais do SGSI.
- Responsabilidades da Direção.
- Auditorias Internas do SGSI.
- Análise Crítica do SGSI pela Direção.

4. ISO 27004 - Métricas para a Gestão da Segurança da Informação

- Objetivos da Medição de Segurança da Informação.
- Programa de Medição de Segurança da Informação.
- Medida básica e medida derivada.
- Indicadores de Segurança.
- Resultado de medições e critérios de decisão.

- Monitoração, análise critica e avaliação.

5. ISO 27005 - Gestão de Risco da Segurança da informação

- Visão Geral da Gestão de Riscos.
- Processo de Gestão de Riscos.
- Alinhamento do SGSI com a Gestão de Riscos.
- Análise e Avaliação de Riscos.
- Estimativa de Riscos.
- Tratamento do Risco.
- Comunicação e Monitoramento do Risco.

6. NBR ISO 31000 - Gestão de Risco: Princípios e Diretrizes

- Visão Geral da Norma.
- Principais Termos de gestão de risco.
- Benefícios da Gestão de Risco.
- Princípios da Gestão de Risco.
- Estrutura da Gestão de Risco.
- Processo da Gestão de Risco.

7. Gestão de Projetos de Segurança da Informação- PMBOK

- Conceitos de Gestão de Projetos.
- Gerência de Escopo em Segurança da Informação.
- Gerência de Tempo em Segurança da Informação.
- Gerência de Custo em Segurança da Informação.
- Gerência de Qualidade em Segurança da Informação.
- Gerência de Pessoas em Segurança da Informação.
- Gerência de Comunicação em Segurança da Informação.
- Gerência de Aquisições em Segurança da Informação.
- Gerência de Integração em Segurança da Informação.

8. Gestão de Serviços de Segurança da Informação- ITILV3

- Introdução ao ITIL.
- Gerenciamento de Segurança da Informação.
- Gerenciamento de Incidentes.
- Gerenciamento de Mudanças.
- Gerenciamento da Continuidade dos Serviços de TI.