Segurança Informática - Ameaças, Riscos e Vulnerabilidades

OBJECTIVOS

A Segurança da informação passa por garantir que as informações, em qualquer formato: *media*, papel e até mesmo conversas pessoais ou por telefone, estejam protegidas contra o acesso por pessoas não autorizadas, estejam sempre disponíveis quando necessárias, e que sejam confiáveis.

Para que exista segurança da informação, deve ser feita em primeiro lugar uma Análise de Risco que identifique todos os riscos (vulnerabilidades e ameaças) que ameaçam as informações, considerando três categorias básicas: riscos administrativos, físicos e tecnológicos. Após a identificação dos riscos, o relatório da Análise de Risco deve apontar as soluções que eliminem, minimizem ou transfiram os riscos. Isto para que, caso ocorra um evento que ameace as informações, sejam tomadas as devidas medidas com o objectivo de garantir, a partir de procedimentos de contingência, a disponibilidade das informações e a continuidade dos processos críticos do negócio.

No final deste Curso os participantes deverão ser capazes de:

- **Compreender os riscos em que incorre o Sistema de Informação;**
- **Dominar os métodos e técnicas para tornar seguro o Sistema de Informação;**
- **Comunicar eficazmente junto dos utilizadores para prevenir os riscos;**
- **Assegurar a continuidade da actividade;**
- **Gerir as situações de crise;**
- **Integrar textos regulamentares.**

DESTINATÁRIOS

Este Curso destina-se a Directores e Gestores de sistemas informáticos. Responsáveis de Gestão de Informática e todos aqueles que estejam implicados na segurança dos sistemas informáticos.

DURAÇÃO

3 dias

Luanda Angola | Email:geral@okwin.biz

CONTEÚDO PROGRAMÁTICO

1. ANALISAR OS DIFERENTES RISCOS PARA O SISTEMA DE INFORMAÇÃO

- A tipologia dos riscos informáticos
- A análise das causas e das consequências
- Hierarquização dos riscos

2. PROCURAR SOLUÇÕES EFICAZES

- Em função das regras da prioridade, procurar soluções que sejam curativas ou preventivas
- Planificar a sua implementação
- Orçamentar o plano de segurança informática
- Introduzir indicadores de *performance* do plano de segurança

3. PREVENIR OS RISCOS ATRAVÉS DE ACÇÕES JUNTO DOS UTILIZADORES

- Regras simples podem evitar grandes problemas
- Comunicá-las aos utilizadores
- Fazer de um incidente uma oportunidade para enriquecer o conhecimento colectivo
- Evitar as sabotagens: saída de colaboradores / má-fé
- Comunicar sobre a segurança de maneira pedagógica
- Formar os novos colaboradores

4. ASSEGURAR A CONTINUIDADE DA ACTIVIDADE

- As principais situações da urgência
- Estabelecer um plano SOS informático, agir por prioridades
- Identificar os limites do exercício
- Gerir as situações de urgência
- A continuidade em termos de meios para satisfazer os clientes
- A segurança em caso de risco maior: incêndio, inundação

5. GERIR AS SITUAÇÕES DE CRISE

- Organizar a gestão de uma crise e assegurar a logística: Quem faz o quê? Onde? Como? Quando?
- Formalizar os processos de decisão
- Adoptar uma comunicação eficaz

6. A REGULAMENTAÇÃO

- Os aspectos legais
- A segurança e os dados
- A vigilância e os direitos dos trabalhadores
- Os seguros e as garantias em caso de sinistro

7. EXERCICIOS PRÁTICOS, SIMULAÇÕES E ANÁLISE DE CASE STUDIES