TI.exames Com êxito

EDUCAÇÃO E TREINAMENTO
PARA ALAVANCAR A SUA CARREIRA

Fundamentos da Segurança da Informação com base na ISO/IEC 27002

Curso e-learning completo

Preparatório para o exame EXIN ISO 27002 Foundation

Módulo 4

Ativos da informação e incidentes de segurança

Este módulo cobre:

- O que são estes ativos e como gerenciá-los, sua classificação, papéis
- Gestão de incidentes de segurança da informação

Slide 2

O que são ativos da informação

Ativos do negócio custam dinheiro e tem valor. Parte destes ativos são ativos da informação – veja exemplos a seguir:

- Documentos, banco de dados, contratos, sistemas de documentação, procedimentos, manuais, sistemas de acesso, etc.
- Programas de computadores, em uso ou em desenvolvimento
- Equipamentos como servidores, computadores, componentes e cabos, etc.
- Ativos não tangíveis como imagem e reputação da organização
- Mídias diversas
- Serviços
- Pessoas e seu conhecimento

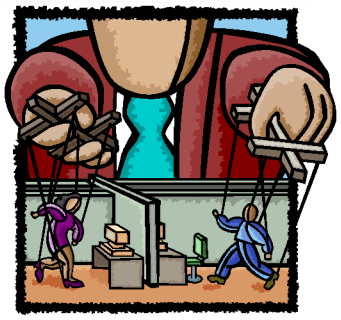
Cada ativo deve ser listado, deve ter um dono e deve ser classificado para que seja estabelecido o nível de segurança necessário.

Devem ser documentadas as seguintes informações: tipo do ativo, dono do ativo, localização, formato, classificação e valor para o negócio.

Slide 3

Gestão dos riscos para os ativos do negócio

Uma forma de controlar ou gerenciar riscos é controlar as mudanças que causam os diversos riscos. Pode-se usar modelos como COBIT®, ITIL® e ISO 20000-1, que são referências para gestão dos processos. Cada um destes modelos tem elementos que ajudam no controle dos processos. Esses elementos são:



- Métodos de lidar com os ativos do negócio. Por exemplo: como usar notebooks fora da organização, regras sobre o que se pode deixar e o que não se pode deixar sobre a mesa de trabalho.
- Métodos sobre como realizar mudanças.
- Métodos sobre quem pode iniciar e executar mudanças e como essas mudanças serão verificadas.

Slide 4

Definições

- **Classificação:** define os diferentes níveis de sensibilidade nos quais as diversas informações podem ser estruturadas.
- **Grau (grading):** é o ato de definir uma classificação correta como informação secreta, confidencial ou pública.
- **Designação:** é uma forma especial de categorizar uma informação. Por exemplo: de acordo com determinado assunto ou organização ou grupo de pessoas autorizadas.
- **Proprietário:** é a pessoa que tem a responsabilidade sobre determinada informação.

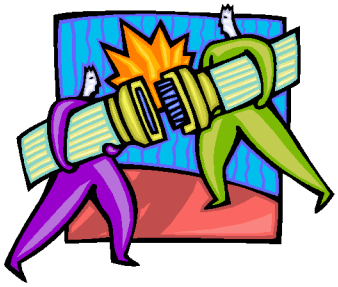
Slide 5

Gestão de incidentes de segurança da informação

Normalmente incidentes são informados à help desk, mas podem ser informados para um responsável específico ou para a chefia dentro da hierarquia da organização.

Exemplos de incidentes:

- Alguém deixou um documento confidencial na impressora.
- Um arquivo com informações pessoais de um funcionário desapareceu.
- Uma porta que deveria ser mantida trancada estava aberta.
- Um colega não está se portando corretamente.
- O monitor do PC mostra informações estranhas.
- Etc.



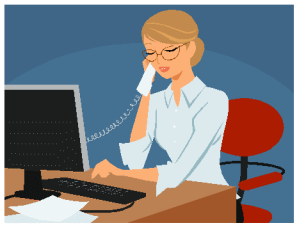
O propósito de um processo de gestão de incidentes é aprender com o erro e usar este aprendizado para não errar novamente no futuro.

Slide 6

Reportando incidentes de segurança da informação

- Nem todos os incidentes registrados em help desks são incidentes de segurança da informação. Por exemplo:
  - → Não é incidente de segurança da informação: um usuário liga para a help desk para solicitar suporte porque o programa que ele utiliza não está iniciando.
  - → É incidente de segurança da informação: um funcionário do RH reporta para a direção que a folha salarial impressa está circulando pela organização.

- O propósito do processo de gestão de incidentes é garantir que incidentes e fraquezas de segurança da informação sejam identificados, registrados e analisados, e que medidas apropriadas sejam tomadas a tempo – sendo que 2 pontos devem ficar claros:



1) **A gestão de incidentes deve ser realizada para que possamos aprender com eles.**
2) **Não estamos buscando um culpado.**

- Devemos sempre informar os resultados do processo para a pessoa que informou o incidente e atualizar o sistema a partir das lições aprendidas.
- No processo de gestão de incidentes deve ficar claro que caso um funcionário esteja deliberadamente roubando informação, a polícia será acionada.

Slide 7

Formulário de registro de incidentes

Dados necessários para um bom formulário de registro de incidentes:

- Data e hora
- Nome da pessoa que está reportando o incidente
- Local de ocorrência do incidente
- Descrição do incidente (vírus, roubo, perda de dados, etc.)
- Consequências do incidente
- Tipo de sistema (desktop, impressora, servidor, servidor de e-mail, etc.)
- Número/nome do sistema
- Quem mais foi informado

Slide 8

Procedimento para gestão de incidentes

Informações que devem ser contidas em um procedimento para gestão de incidentes:

- Qual formulário deve ser utilizado para documentação do incidente, e se necessário como preenchê-lo.
- Que passos devem ser realizados para minimizar as consequências de um incidente.
- Como analisar o incidente e identificar a causa do incidente ou de um conjunto de incidentes.
- Que passos devem ser realizados para determinar as medidas corretivas necessárias para prevenir que o incidente não ocorra novamente.
- Quem deve ser informado da ocorrência do incidente (partes afetadas e partes capazes de ajudar na solução do problema).

Slide 9

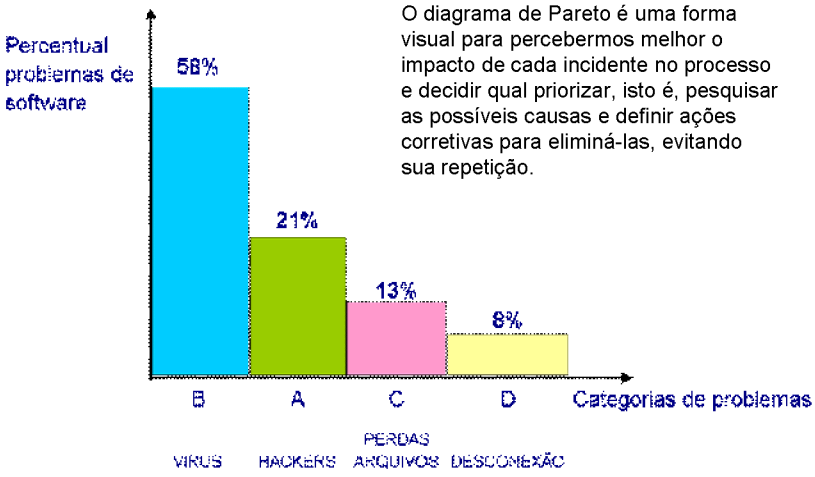
Exemplo de tabulação de dados de incidentes

	A	B	C	D
Número problemas por período	Invasões hackers pela Internet	Virus detectados	Perdas de arquivos	Desconexões do Servidor
Janeiro	5	10	5	1
Fevereiro	3	14	2	3
Março	8	11	3	2
Abril	4	19	2	1
Total de problemas	20	54	12	7
% por categoria	22%	58%	13%	8%

Slide 10

Análise de incidentes

Exemplo de análise de dados de incidentes utilizando o diagrama de Pareto:



O diagrama de Pareto é uma forma visual para percebermos melhor o impacto de cada incidente no processo e decidir qual priorizar, isto é, pesquisar as possíveis causas e definir ações corretivas para eliminá-las, evitando sua repetição.

Slide 11

Monitoramento e revisão do SGSI em função dos incidentes

A organização deve:

Revisar as análises de risco a intervalos planejados e analisar criticamente os riscos residuais e os níveis de risco aceitáveis identificados, levando em consideração mudanças relativas a:

1) Organização
2) Tecnologias
3) Objetivos e processos do negócio
4) Ameaças identificadas
5) Eficácia dos controles implementados
6) Eventos externos, tais como mudanças nos ambientes legais ou regulamentares, alterações das obrigações contratuais e mudanças na conjuntura social

Sempre que uma mudança ocorre poderemos ter alteração dos ativos, das ameaças e das vulnerabilidades – e portanto dos riscos.

Slide 12

Informando fraquezas de segurança

- Incidentes só podem ser evitados se fraquezas no Sistema de Gestão de Segurança da Informação forem identificadas, reportadas ao pessoal responsável e tratadas.
- Todos são responsáveis por relatar tais fraquezas: funcionários, subcontratados, usuários internos e externos, pessoal temporário, etc.
- Quando uma fraqueza é reportada não significa necessariamente que ela não seja conhecida e que não hajam medidas definidas. Se houverem, ótimo – se se não houverer é preciso realizar a análise de riscos e definir que medidas de controle devem ser aplicadas, se cabível.
- Outro ponto importante é a questão de informar ou não à polícia. O incidente deve ser analisado, mas cuidados devem ser tomados para que pistas não sejam perdidas durante esse processo. Exemplo: alguém informa que um profissional mantém pornografia infantil em seu computador. A verificação do incidente deve ser realizada cuidadosamente para garantir que evidências não sejam perdidas.

Slide 13

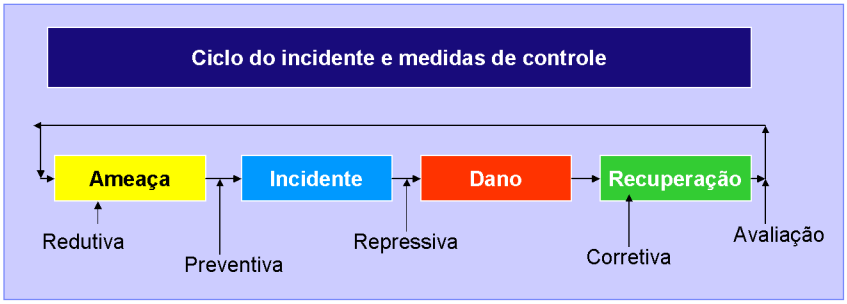
Registrando interrupções de serviço

- Em grandes organizações as interrupções de serviço são normalmente informadas à help desk. Ela normalmente tem procedimentos para lidar com estas situações, e se necessário retransmite o problema para a área que tem condições de resolvê-lo.
- Para analisar interrupções de serviço é importante que as informações relevantes sejam levantadas. Estas informações frequentemente são armazenadas em arquivos de log.
- Quando há uma interrupção de serviço pode-se realizar os registros dos incidentes de segurança em papel.

Slide 14

Ciclo de incidente

- O ciclo de incidente tem as seguintes etapas: ameaça, incidente, dano e recuperação.
- Medidas de segurança são destinadas a etapas especificas do ciclo do incidente. As medidas são: prevenir incidentes (medidas preventivas), reduzir as ameaças (medidas detectivas), responder aos incidentes, parar ameaças (medidas repressivas) e corrigir os danos (medidas corretivas).
- Essas medidas são tomadas para garantir confidencialidade, integridade e disponibilidade da informação.



Slide 15

Papéis

Dependendo do tamanho da organização existem vários papéis ou posições abrangendo as diversas responsabilidades dentro da organização:

- Superintendente de Segurança da informação (Chief Information Security Officer – CISO)
- Diretor de Segurança da informação (Information Security Officer – ISO)
- Gerente de Segurança da Informação (Information Security Manager– ISM)
- Responsável pela Proteção dos Dados (Data Protection Officer)

Slide 16

Estudo de caso

Em uma grande organização com filiais em todo país, incidentes de segurança são ocorrências comuns. Há pouco tempo um funcionário deixou seu laptop na capota do seu carro. O laptop foi encontrado, mas a informação nele contida era importante e não devia ser divulgada para as pessoas em geral. Pen drives também são frequentemente perdidos e os profissionais não sabem com certeza que arquivos estavam armazenados. O departamento de marketing ficou surpreso ao descobrir, durante uma auditoria, o grande número de funcionários no departamento que tinham informações confidenciais sobre ações estratégicas da organização.

Você como funcionário da empresa teve a honra de ser escolhido o primeiro "Information Security Officer – ISO" e sua primeira tarefa foi garantir que a administração fosse conscientizada da necessidade da segurança da informação, e que os incidentes acima fossem analisados e ações fossem tomadas para que não voltassem a ocorrer.

Indique quais ações você tomaria para garantir que seus objetivos acima indicados fossem atingidos.

Resposta do estudo de caso

Ações possíveis:

Laptop:

1) Passar a criptografar as informações armazenadas no HD do laptop
2) Não armazenar dados no HD do laptop (armazenar no sistema online da empresa)
3) Fazer um back up ao menos semanal caso armazene dados no HD do laptop

Pen drive:

1) Passar a criptografar as informações armazenadas em pen drives
2) Não permitir unidade de disquete, cd ou pen drive
3) Usar softwares para impedir a entrada e saída de dados do computador, impedindo desta forma o uso de dispositivos como o pen drive

Informações estratégicas:

1) Definir quem pode ter acesso a informações estratégicas no departamento de marketing e passar a realizar as estratégias dentro de grupos de identidade (perfil de acesso)
2) Realizar processo de conscientização para todos os funcionários do departamento a fim de reduzir o compartilhamento das informações. Por exemplo: senhas não devem ser compartilhadas, introduzir a política da mesa limpa, não imprimir e-mail, não deixar a tela do computador aberta, etc.

Conscientização da administração sobre a necessidade de segurança da informação:

1) Identificar os maiores riscos de segurança da informação e suas consequências, principalmente as perdas, e realizar palestras com todo pessoal da administração apresentando estas informações