Curso Preparatório para Certificação
Em Gestão de Segurança da Informação Avançada – Baseada na ISO/IEC 27002:2013

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 1

Nível
Advanced

Prof. Adriano Martins Antonio

www.pmgacademy.com

Design: By Freepik

Módulo 1

Introdução

Sobre o EXIN

www.exin-exams.com

Sobre o Adriano

Adriano Martins Antonio

- Instrutor oficial credenciado aos institutos Axelos e ISACA;
- Consultor de Gestão de Serviços de TI, Governança de TI, Escritório de Projetos...;
- Mais de 20 anos de experiência;
- MBA em Gestão Empresarial pela FGV – SP;
- Possui diversas certificações.

Maior Aproveitamento

Assista no mínimo 2x

Contate o instrutor

Realize os exercícios

Leia o glossário

Execute os simulados

Visão Geral

Resumo

Segurança da Informação

Proteção das informações contra uma grande variedade de ameaças, que garante a continuidade do negócio, minimiza o risco e maximiza o retorno sobre investimentos e as oportunidades de negócios, segundo a definição da norma ISO/IEC 27002.

ERP - Sistemas de gerenciamento de planejamento de recursos empresariais.

- São cruciais para a continuidade e o funcionamento adequado tanto de organizações individuais quanto das economias que elas alimentam;
- Devem ser protegidas contra o acesso por pessoas não autorizadas;
- Protegidas contra a modificação ou destruição acidental ou mal intencionada;
- E devem estar disponíveis quando necessárias.

Globalização da economia

Esquema de Qualificação

- **Fundamento da Segurança da Informação** baseado na ISO/IEC 27002 (ISFS*); testa os conceitos básicos de segurança de informação e suas interrelações.
- **Gerenciamento de Segurança na Informação** baseado na ISO/IEC 27002 (ISMAS) que testa os aspectos de gerenciamento e organizacionais da segurança da informação:
- Gerente de Segurança da Informação (ISM – Information Security Manager);
- Administrador de Segurança da Informação, (ISO Information Security Officer);
- Gerente de Linha, o Gerente de Processo e o Gerente de Projeto.

*O termo S para: Baseado no padrão (standard)

Esquema de Qualificação

- A **Certificação do nível Advanced** em Gerenciamento de Segurança da Informação é baseado no Certificado do nível Foundation de Segurança da Informação, onde os conceitos básicos de segurança da informação são exigidos.

- O **Módulo de Expert (Especialista)** em Segurança da Informação baseado também na ISO/IEC 27002 (ISMES), testa o conhecimento especializado, entendimento e habilidades na estruturação, manutenção e otimização da segurança da informação dentro da organização.

*O termo S para: Baseado no padrão (standard)

Tendências

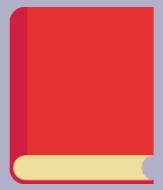
As exigências de conformidade estão aumentando:

A maioria dos países conta com múltiplas leis ou regulamentos que controlam o uso e exigem a proteção de vários tipos de dados.

Muitas indústrias, particularmente no mundo financeiro, têm regulamentos além daqueles impostos por um governo.

Normas de segurança estão sendo desenvolvidas e refinadas nos níveis industrial, nacional e internacional.

Certificações de segurança são provas passíveis de auditoria de que uma organização está seguindo as normas e/ou melhores práticas de segurança...



Código de Prática para Segurança da Informação ISO/IEC 27002:2013, é uma norma amplamente respeitada e citada e fornece uma estrutura para a organização e o gerenciamento de um programa de segurança da informação.

Tópicos do Curso

Testa seus conhecimentos sobre os aspectos organizacionais e gerenciais da segurança da informação.

A **Segurança da Informação** lida com a definição, a implementação, a manutenção, a conformidade e a avaliação de um conjunto coerente de controles que protegem a disponibilidade, a integridade e a confidencialidade do suprimento (manual e automatizado) de informações.

Os tópicos para este módulo Advanced são:

- **Perspectivas em segurança da informação:** Negócio, Cliente, Provedor de serviços/fornecedor (10%).
- **Gerenciamento de Risco:** Análise, Controles, Riscos residuais (30%).
- **Controles de segurança da informação:** Organizacionais, Técnicos, Outros. (60%).

Informações Sobre o Curso

Público-Alvo

- **Profissionais de nível intermediário;**
- **Gerente de Segurança da Informação (ISM);**
- **Executivo de Segurança da Informação (ISO) ou um Gerente de Linha;**
- **Gerente de Processo ou Gerente de Projeto com responsabilidades relevantes.**

Informações Sobre o Curso

Pré-requisitos

O certificado em Fundamentos da Segurança da Informação baseado na ISO/IEC 27002 ou seja, a ISO 27002 Foundation.

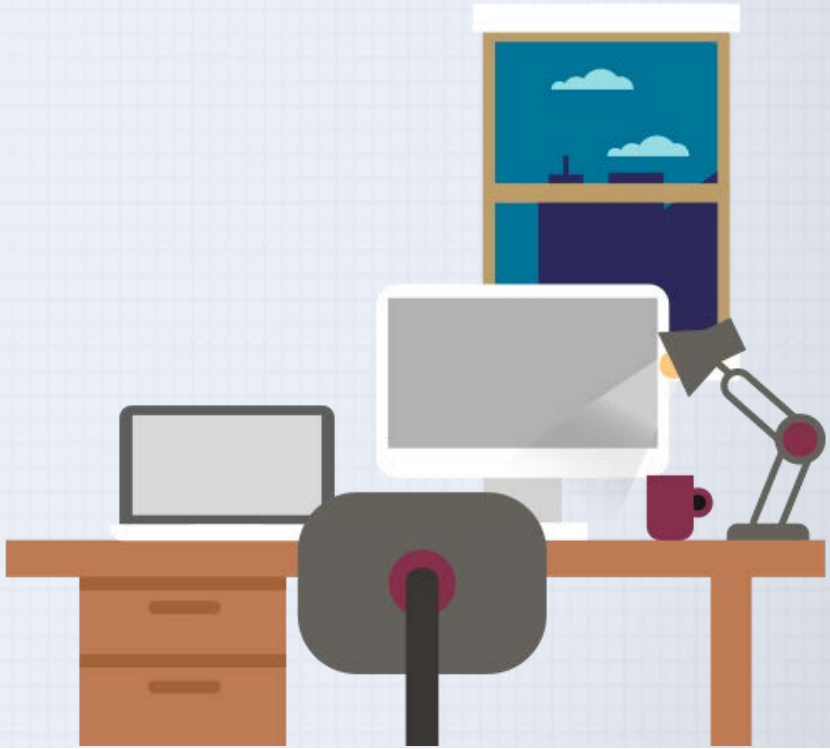
E as exigências para a certificação ISMAS:

- Curso de treinamento Advanced em Gerenciamento de Segurança da Informação com um provedor de treinamento credenciado pelo EXIN (ATP), incluindo a realização efetiva dos dois (2) exercícios práticos como parte do curso.

- Realização e aprovação no exame Avanced de Gerenciamento de Segurança da Informação baseado na ISO/IEC 27002 (ISMAS).

Formato do Exame

- Exame com questões de múltipla escolha;
- Tempo destinado ao exame: 90 minutos;
- Número de questões: 30;
- Mínimo para aprovação: 65 % (20 de 30);
- Com consulta: não;
- Estimativa de Tempo de Estudo:
- 120 horas, incluindo o tempo dedicado a este curso, simulado e exercício prático;
- Exercício prático:
- Exercícios práticos fazem parte do exame e serão avaliados por um provedor de treinamento credenciado pelo EXIN durante o curso de treinamento.



Desmistificando as Siglas

O dia a dia é cheio de pequenas siglas, isto porque acabam facilitando as coisas, algumas siglas são fáceis enquanto outras nem tanto, por isso vamos entender nas entrelinhas.

SGSI

- Sistema de Gestão da Segurança da Informação.

ISO

- International Organization for Standardization.

IEC

- **International** Electrotechnical Commission.

- Uma norma não é uma regra, ou uma lei;
- Servir como um excelente guia de melhores práticas também;
- Quem segue as normas, pode optar em obter um certificado **ISO** para os processos de gestão de Segurança da Informação da empresa, e quem tem este certificado, pode dizer que possui certo tipo de atestado de qualidade.

Definição de Segurança da Informação

Conforme a norma ISO 27002, a Segurança da Informação lida com…

- … a definição, implementação, manutenção, cumprimento e avaliação…
- … de um conjunto coerente de controles...
- ... que garante a disponibilidade, integridade e confidencialidade…
- ... do fornecimento de informações (manual e automático).

Definição de Segurança da Informação

E isso implica em:

- Um sistema de gestão, tal como ISO/IEC 27001;
- Um conjunto de controles, como a ISO/IEC 27002;
- Um foco sobre a disponibilidade e confidencialidade / integridade;
- Compreender os aspectos técnicos de segurança da informação exige que você conheça as definições de certos termos e conceitos de tecnologia da informação. Em geral, a segurança é definida como **"a qualidade ou estado de estar seguro ou estar livre do perigo.";**
- A segurança é muitas vezes atingida através de várias estratégias, geralmente conduzidas de forma simultânea ou utilizada em combinação.

Áreas da Segurança

Segurança Física

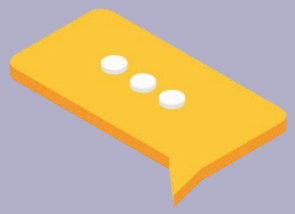
Segurança Pessoal

Segurança das Operações

Segurança das Comunicações

Conceito de Política

Segurança da Informação

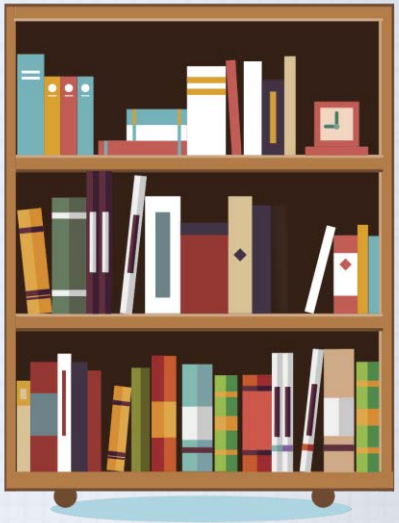


Segurança da Rede

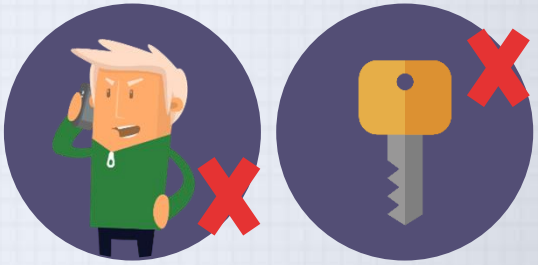
Segurança Envolve Toda a Empresa

ITIL® → COBIT 5 AN ISACA® FRAMEWORK → EXIN BUSINESS INFORMATION MANAGEMENT

No caso da Segurança da Informação, a norma mais usada é a ISO/IEC 27002. Ela foi publicada pela primeira vez em 2005, revisada em 2007 e revisada novamente em 2013. O que significa que na medida em que a tecnologia fica mais diversificada e complexa, pode ser preciso revisar novamente.



- É alcançada através de um conjunto de regras e modos de trabalhar;
- É necessário lidar com as políticas da empresa;
- Com os processos que ela adota;
- Com a estrutura organizacional;
- Com os programas de computador e os próprios computadores e outros hardwares envolvidos.



Segurança Envolve Toda a Empresa

Para que uma gestão seja eficiente, é preciso criar um modo operacional completo e sempre ficar monitorando, para ter certeza de que tudo segue conforme o combinado.

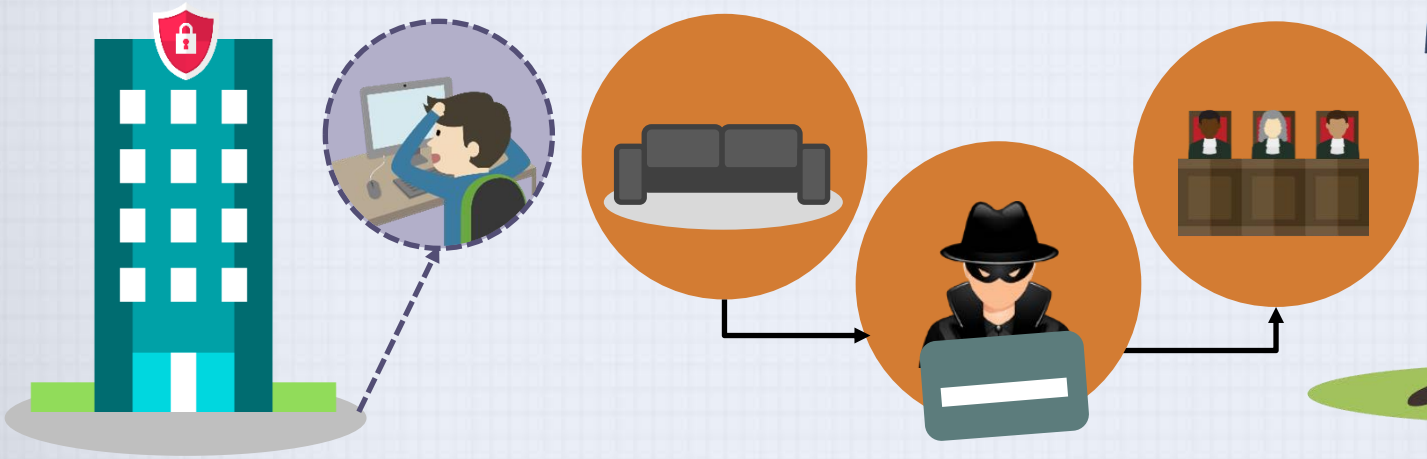
Este trabalho precisa ser feito em equipe, porque não há como cuidar de tudo sozinho.

Não há como criar um único escudo protetor, e sim, um conjunto de pequenos escudos, que são sustentados em áreas distintas.

Importância da Segurança da Informação

Segurança da informação é importante porque garante que uma informação não foi alterada, está completa e só pode ser vista por pessoas autorizadas, certo?

- É preciso adotar algumas medidas para que a segurança exista, assim como você tem ao travar a tela do seu celular ou colocar uma senha em seu e- mail.



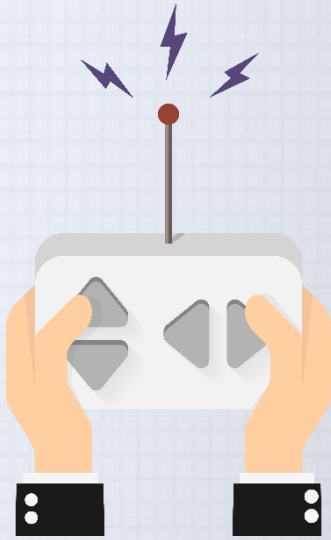
Importância da Segurança da Informação

Um site que recebe cadastro de seus usuários também teria um grande prejuízo caso deixasse vazar alguns dos dados sigilosos de quem o acessa, sem contar nos processos que teria que enfrentar.

Tanto para a empresa, quanto para o cliente – ou usuário – a segurança deve ser sempre uma prioridade.

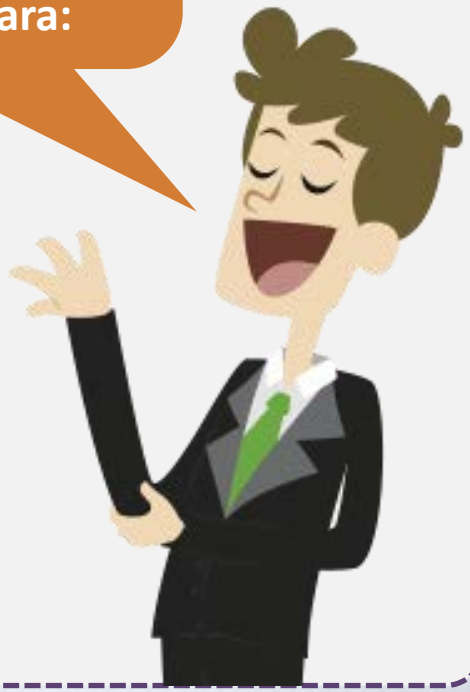
Medidas de Segurança: Controle

- Responsabilidades e tarefas passadas com clareza.
- Guias e documentação de referências.
- Procedimentos para emissão e encaminhamento de relatórios.
- Medidas que atendam às necessidades do negócio e do local da TI.
- Os processos e guias de referência devem dizer, por exemplo, em detalhes, como cada um dentro da equipe deve agir em casos particulares, determinando as ações, níveis de acesso, a quem se reportar, etc.



Medidas de Segurança: Controle

Não apenas membros da equipe de TI, mas todos dentro de uma empresa devem estar em linha com regras e normas para:

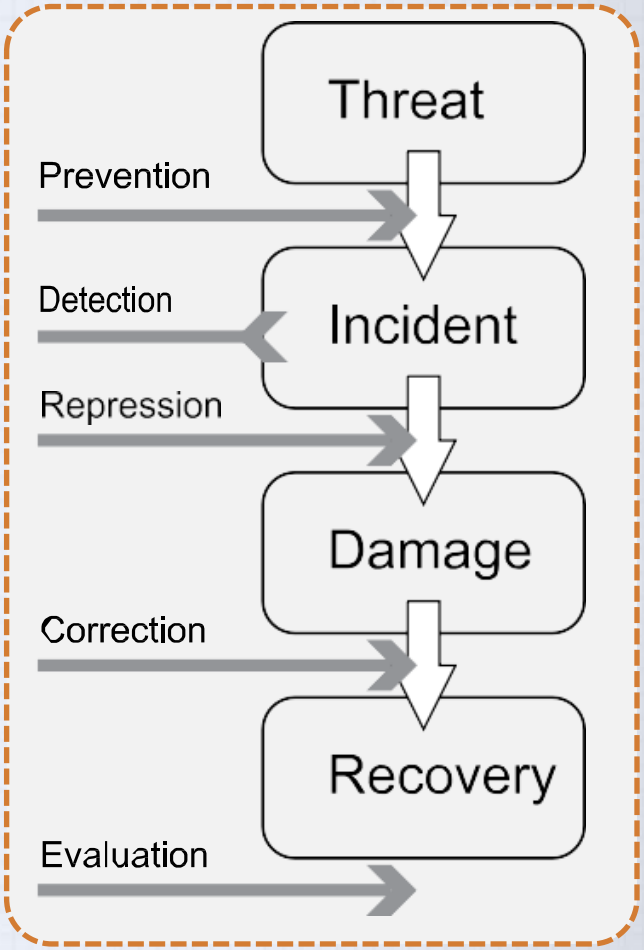


- Acessar arquivos confidenciais.
- Receber arquivos e material de terceiros.
- Realizar backups e cópias de segurança.
- Emitir relatórios de uso e monitoramento.

Medidas de Segurança: Contenção

Quando uma situação de risco se torna uma ameaça, procedimentos bem desenhados de segurança precisam ser postos em prática. Geralmente essas medidas de contenção possuem uma gradação, que começa com a prevenção, etapa na qual a ameaça ainda é evitada, terminando na avaliação e passando por diversas outras etapas, como mostram os itens e o gráfico.

- Para evitar uma AMEAÇA >> Faz-se a Prevenção;
- Para evitar um INCIDENTE >> Faz-se a Detecção >> e a Repressão;
- Para repara um DANO >> Faz-se a Correção;
- Após efetuar a RECUPERAÇÃO >> Faz-se a Avaliação.



Medidas de Segurança: Ameaças

- A primeira etapa de uma medida de contenção exige a identificação de possíveis ameaças, o que reflete o risco que essas ameaças geram caso se materializem.

- A ameaça é qualquer coisa que interrompa o funcionamento de um negócio baseado em informações, ou cause a ele prejuízos em termos de resultados.

Ameaça materializada = Incidente de Segurança

Esse incidente pode acarretar em danos e precisa ser imediatamente reparado ou corrigido. A cada minuto que você espera, um pequeno incidente vai se transformando em uma calamidade.

Medidas de Segurança: Incidentes

A escolha das medidas de contenção de incidentes...

Depende diretamente da importância da informação para o negócio.

- **Direitos de acesso**. Concessão, renovação e retirada de direitos.
- **Autorização**. Identificação das pessoas ou grupos cujo acesso é permitido e em que nível.
- **Autenticação**. Exigências de confirmações de identidade para garantia de acesso.
- **Controle de acesso**. Monitoramento constante de pessoas que acessam a informação, garantindo sua identidade e nível de permissões.

Medidas de Segurança: Incidentes

Detecção

Incidente de Segurança

Sistemas de monitoramento.

Sistemas de gestão de eventos.

Softwares de antivírus.

Softwares de diagnósticos e outros.

Medidas de Segurança: Incidentes

Entram em cena as medidas de repressão a ataques e ameaças. As medidas podem ser diversas:

Suspensão de acesso.

Reinício do sistema.

Atuação proativa de equipe de segurança.

Acionamento de um sistema de reserva ou contingência.

Bloqueio temporário.

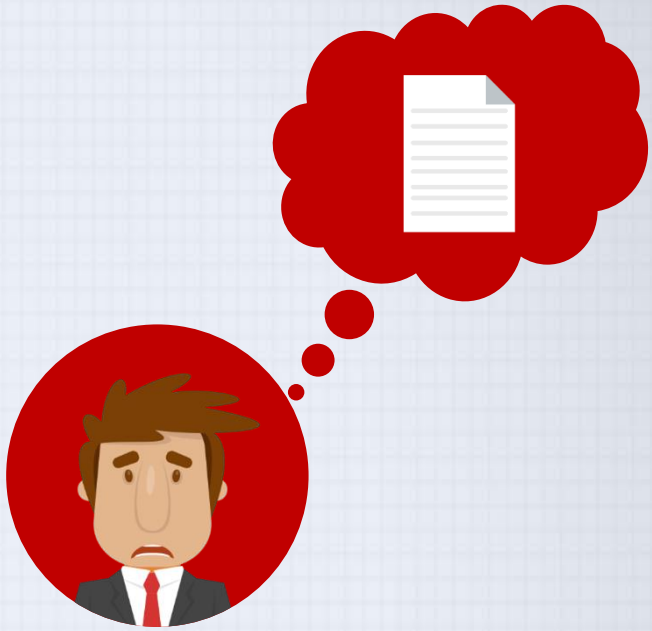
Medidas de Segurança: Correção e Recuperação

Após o tratamento do incidente, o trabalho da segurança da informação passa a abranger a correção, posterior recuperação do sistema, das falhas e danos que foram gerados pelo incidente ou ataque. A recuperação pode ocorrer em diversos níveis, mas os mais comuns seriam:

- Restauração de backups.
- Retorno para situações estáveis anteriores, via restauração de sistemas ou rotinas de roll back ou back out.
- Fallbacks, no caso de softwares ou sistemas, para versões estáveis anteriores.
- Situações mais graves exigem medidas customizadas, a serem aplicadas após avaliações mais detalhadas do incidente, seus danos e consequências, inclusive da própria restauração ou recuperação.

Planejamento e Implementação

Uma vez que é feito uma análise para definir os novos padrões, controles e medidas de segurança, é preciso planejar sua implementação, para que a situação desejável seja atingida.



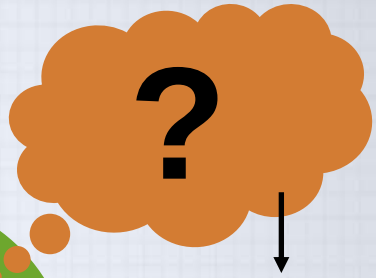
- Realizar reavaliações mensais, trimestrais ou simplesmente seguir com um regime de metas e cumprimento das mesmas... o **planejador** é quem decide.

- **E não se esqueça:** a implementação de uma política de segurança da informação precisa considerar despesas e receitas.

O objetivo?

Que a direção da empresa possa tomar decisões relacionadas à segurança da informação, mesmo sem conhecimento de detalhes técnicos.

Segurança das Suas Informações



Todas

Tenha em mente que além dos dados pessoais, as informações que precisam ser seguras também englobam outras mais específicas, como o IMEI do seu aparelho celular, ou os números de registros ou licenças dos softwares, etc.

Isto porque informação nada mais é do que uma série de dados, que se usados fora de contexto, podem acabar gerando de sérios problemas.

Segurança de Dados

A Segurança da informação trabalha para que todos os dados sejam sempre protegidos, e usa uma série de ferramentas para isto.

Tripé CIA:

Confidentiality **(Confidencialidade)**: ou seja, só teve acesso quem era autorizado.

Integrity **(Integridade)**: a informação está perfeita, do jeito que deveria estar.

Availability (**Disponibilidade)**: todos que devem ter acesso conseguem usar, não há bloqueios impedindo.

Para que os dados sejam preservados, precisamos evitar que pessoas não autorizadas tenham acesso para modificar, compartilhar, ou danificar as informações. Ou melhor, que possam causar danos, mas, não basta manter apenas **o tripé CIA** de **confidencialidade, integridade, disponibilidade**, e sim, outros conceitos da segurança da informação, como a autenticidade, privacidade, autenticação, autorização etc.

Confiabilidade, Integridade e Disponibilidade

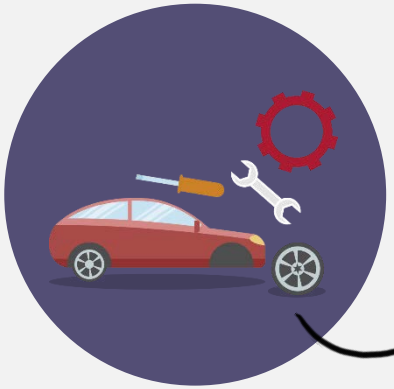
A informação pode ser controlada de diferentes formas, dependendo de cada empresa, vai mudar muito a maneira como ela coleta e organiza os seus dados.

- **Algumas usam softwares específicos;**
- **Outras apenas organizam os próprios arquivos.**
- **O que não muda são as premissas de como criar um ambiente seguro.**

Só são possíveis quando o acesso é realmente restrito às pessoas autorizadas.

- **Confiabilidade**
- **Integridade**
- **Disponibilidade**

Confiabilidade, Integridade e Disponibilidade



Loja de equipamentos automotivos

Onde cada vendedor possui uma senha particular para o sistema

E apenas o gerente possa liberar com a senha dele, um desconto para um cliente.

EX.: O mesmo ocorre em senhas de operadores de caixa, se uma empresa utiliza uma senha padrão, a segurança está comprometida, porque não há como saber qual operador efetuou uma movimentação especifica, já que todos usam a mesma senha.

Para que a informação esteja sempre íntegra – sem alterações, é preciso limitar e garantir que quem use saiba o que faz.

Dois Objetivos da Segurança da Informação

objetivo implícito

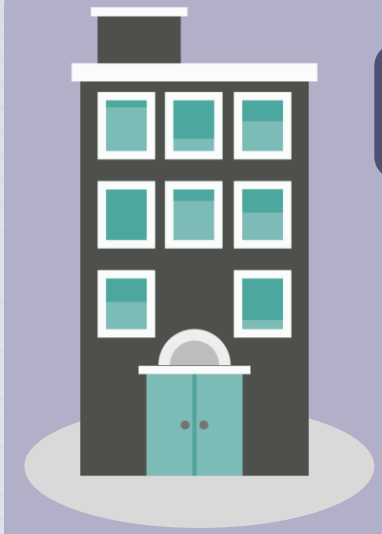
- **é aquele que está "embutido".**

objetivo explícito

- **é aquele que está claro, que foi formulado.**

A segurança é uma necessidade Implícita, porque é preciso que tudo esteja sempre seguro, esteja de acordo com as normas – que mesmo não sendo lei, devem ser seguidas para que tudo funcione bem.

Dois Objetivos da Segurança da Informação



Ela desenvolve hábitos, uma rotina, esta rotina é avaliada, para que cada ponto esteja cercado da segurança que precisa.

Implícita

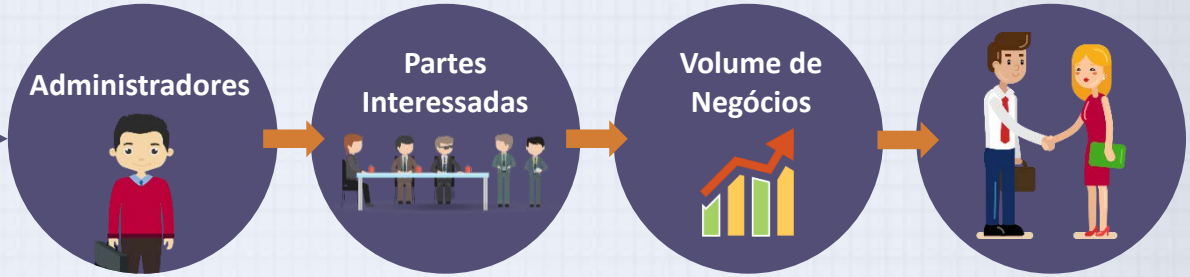
Explícita

É aquilo que é mencionado como uma necessidade, que pode não ser o óbvio para todo mundo, mas que é preciso, e por isto é solicitado.

A questão é que isto não é igual para todas as empresas, os requisitos de segurança podem ser parecidos, mas as respostas nem sempre serão as mesmas, porque cada empresa pode ter um negócio diferente, com abordagens diferenciadas.

Princípios Formadores da Segurança da Informação

Segurança da Informação



Três princípios que formam a segurança da informação:

1. *A avaliação de riscos para a empresa, com base nos objetivos e as estratégias de negócio.*

2. *As leis vigentes. Os contratos da empresa, as regras estabelecidas com os parceiros comerciais, com os provedores de serviço. Entre outros contratos.*

3. *Os princípios de cada empresa, os requisitos próprios de cada empresa quanto ao processamento, armazenamento, e a forma como ela faz a comunicação, até mesmo a forma como ela faz o arquivamento das informações que a empresa tem que criar para servir de apoio a sua própria produção e se manter em funcionamento.*

Princípios Formadores da Segurança da Informação

Na norma **ISO/IEC 27005,** sessão 11, é fornecida algumas informações que ajudaram a orientar a gestão de riscos de segurança, incluindo alguns conselhos sobre avaliação de risco, o tratamento de risco, aceitação de riscos, comunicação de risco, monitoramento de risco e avaliação de risco.

Conceitos – Chave I

Confidencialidade

- Confidencialidade da informação garante que apenas aqueles com privilégios suficientes podem acessar certas informações. Se as pessoas ou sistemas não autorizados acessarem a informação, então a confidencialidade é violada.

- **Classificação da informação;**
- **Armazenamento segura de documentos;**
- **Aplicação de políticas gerais de segurança;**
- **Educação dos responsáveis pela proteção de informação e dos usuários finais.**

Conceitos – Chave I

Integridade

- A integridade é a qualidade ou estado de estar completo, da totalidade e não corrompido. A integridade da informação é ameaçada quando ela é exposta a algum tipo de corrupção dos dados, danos, destruição, ou outras perturbações quanto ao seu estado autêntico. A corrupção pode ocorrer enquanto a informação está sendo compilada, armazenada ou transmitida.

Disponibilidade

- É a característica da informação que permite o acesso do usuário à informação sem interferência ou obstrução e em um formato desejado. Um usuário nesta definição pode ser uma pessoa ou outro sistema de computador.
- Não implica que a informação esteja acessível a qualquer usuário; pelo contrário, significa a disponibilidade somente aos usuários autorizados.

Conceitos – Chave II

Privacidade

- As informações que são coletadas, usadas e armazenadas por uma organização é para ser usada apenas para fins indicados pelo dono dos dados no momento em que foi coletada. A definição de privacidade significa que a informação será usada apenas com formas conhecidas pela pessoa que as forneceu.

Identificação

- Um sistema de informação possui a característica de identificação quando é capaz de reconhecer os usuários individuais. Identificação e autenticação são essenciais para estabelecer o nível de acesso ou autorização que é concebido a um indivíduo.

Autenticação

- A autenticação ocorre quando um controle fornece a prova de que um usuário possui a identidade que ele ou ela afirma.

Conceitos – Chave II

Autorização

- Após a identidade de um usuário for autenticada, um processo chamado de autorização fornece a garantia de que o usuário (seja uma pessoa ou um computador) é expressamente autorizado pela autoridade adequada para acessar, atualizar ou excluir o conteúdo de um ativo de informação.

Prestação de contas

- A característica da responsabilidade existe quando um controle fornece a garantia de que todas as atividades realizadas podem ser atribuídas a um nome de pessoa ou processo automatizado.

Autenticidade

- Autenticidade significa receber uma informação de uma fonte segura, e ter garantias que ninguém mudou nada durante o processo ou trajeto entre o emissor e o remetente.

Fundamentos do Gerenciamento da Segurança da Informação

Gerenciamento da Segurança da Informação

É um conjunto de atividades que administra determinado nível de segurança da informação em um sistema.

- Significa fazer tudo o que for necessário para manter o nível de segurança em determinado patamar para um conjunto de informações.

- Não importa o que possa mudar ou que ameaças venham a ser enfrentadas – o nível de segurança precisa permanecer sempre estável e com um grau de risco aceitável.

Fundamentos do Gerenciamento da Segurança da Informação

As bases para a realização do gerenciamento de segurança da informação seguem sempre em contrato – no qual constarão as especificações e segundo a ISO/IEC 27002, uma listagem de medidas e controles que inclua, pelo menos:

- Disponibilidade ou não de uma política interna de segurança da informação;
- Descrição dos controles usados para garantir a proteção dos ativos;
- Treinamento de pessoal e dos gestores;
- Provisões no caso de transferência de pessoal;
- Especificações para processos de sucessão ou mudanças no comando;
- Política de controle de acesso;
- Pontos de contato;
- Normas de conformidade (compliance);
- Detalhes sobre a auditoria de sistemas;
- Produção de relatórios.

Gerenciamento Contínuo da Segurança da Informação

Manter metas e objetivos futuros que possam ser atingidos, mesmo após um sistema ser declarado "seguro" e bem gerido.

Primeiro

Aquilo que tem de ser feito para que o nível de segurança atinja o patamar desejado, o que inclui a análise de riscos, avaliação dos riscos, definição de medidas e controles, criação de padrões para o uso e manutenção, e sistemas de monitoramento.

Segundo

Tudo o que deve ser feito para manter o nível de segurança no patamar atingido, incluindo tarefas como a produção de logs de incidentes e problemas, análises de tendências e relatórios, suporte, manutenção, gerenciamento de vulnerabilidades, comunicação, entre outros.

Gestor da Segurança da Informação

Como o Gerenciamento da Segurança da Informação é o processo que busca alcançar os objetivos usando um determinado conjunto de recursos...

...então, para tornar o processo de segurança da informação mais eficaz, é importante compreender alguns princípios fundamentais de gerenciamento, como por exemplo, o GERENTE.

É alguém que trabalha com e através das pessoas para coordenar suas atividades de trabalho, a fim de atingir as metas organizacionais.

- **Papel informativo**: Coleta, tratamento, e utilização de informação que pode afetar a realização do objetivo.
- **Papel interpessoal:** Interagindo com os superiores, subordinados, os agentes externos e outras partes que influenciam ou são influenciados pela conclusão da tarefa.
- **Papel de decisão**: Escolher entre abordagens alternativas, e resolução de conflitos, dilemas e desafios.

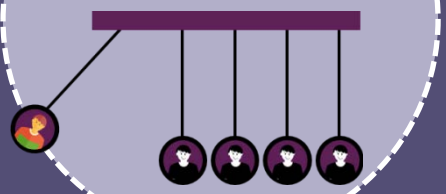
Gestor da Segurança da Informação

- **Aconselhamento**. Tomada de decisões em nível técnico, que exigem aconselhamento de profissionais especializados.
- **Compartilhamento**. Cooperação e comunicação entre o gestor e diversas áreas da organização, para troca de experiências e desenvolvimento de melhores práticas.
- **Independência**. A implementação da política de segurança é regularmente revisada por pessoas, em nível interno ou externo, independentes da gestão.

Gestor da Segurança da Informação

Por isso existem dois aspectos importantes para comprovar a eficiência financeira na segurança da informação:

O impacto dos riscos



E o custo necessário para evitá-los

Os Papéis de Gestão e Coordenação

O Gerenciamento, seja de segurança da informação ou de qualquer outro tipo, é ESSENCIAL. Sem ele, as projeções e previsões se tornam impossíveis, assim como as certificações e acreditações gerais.

- É o responsável por produzir relatórios e avaliar progressos e recuos dentro da aplicação da política de segurança.
- Ele definirá processos, funções e responsabilidades, além de lidar com outros departamentos e setores.
- Deve agir para criar uma espécie de "conselho" que possa ajudá-lo em sua tarefa.

***Não confundir esse "controle" com as medidas de contenção que levam mesmo nome.**

Os Papéis de Gestão e Coordenação

- Auxiliar na direção;
- Rever políticas e controles;
- Modificar medidas de contenção e a aplicação dos controles;
- Aprovar planos de segurança;
- Reiterar responsabilidades;
- Monitorar mudanças nas ameaças e incidentes.

Os Papéis de Gestão e Coordenação

A coordenação é outra função importante dentro do Gerenciamento da Segurança da Informação. Muitos confundem a figura do gestor com a do coordenador. Contudo, um coordenador possui uma ação mais operacional:

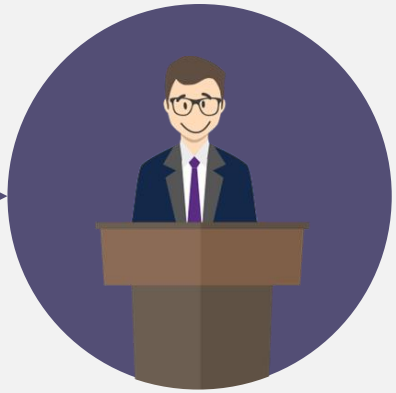
- **Implementando planos e medidas;**
- **Permitindo a cooperação entre diversas responsabilidades e tarefas relacionadas à segurança;**
- **Garantindo que as técnicas e métodos usados sejam harmoniosos;**
- **Ajudando a criar iniciativas que envolvam toda a organização.**

Ciclo de Vida da Informação

Ciclo de Vida da Informação

O ciclo de vida de uma informação não tem sempre o mesmo valor, ou seja, ela pode ficar mais valiosa, ou menos importante ao longo do processo. Isto depende do que acontecer com ela.

Se esta informação for divulgada, depois de roubada, tem um peso.



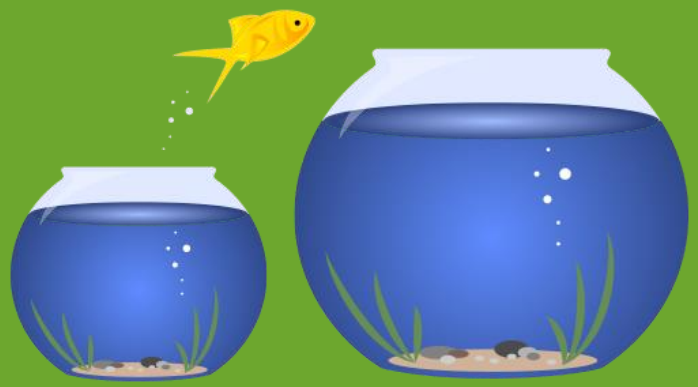
Se for divulgada publicamente pela empresa, antes de ser roubada, possivelmente já não valerá muita coisa.

Ciclo de Vida da Informação

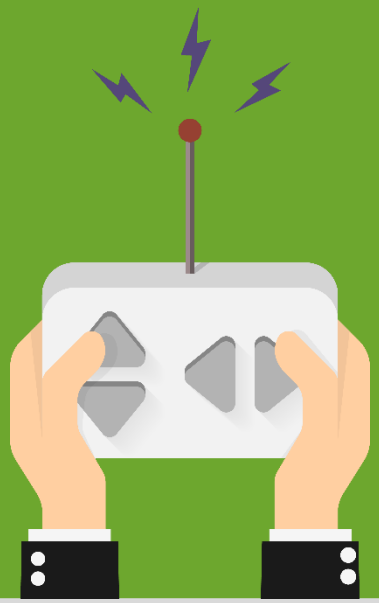
Os próprios sistemas de informação possuem um tipo de ciclo de vida, que começa quando os programas são projetados, depois especificados, saem do papel, são desenvolvidos e posteriormente são testados, entram em produção, quando são usados, e desde o momento em que foram implementados, começam a envelhecer, e mais tarde, são substituídos por outro ou são simplesmente descartados porque não atendem mais os objetivos de negócio da organização.

Ciclo de Vida da Informação

A cada mudança que a empresa passa, ela tem uma chance de se atualizar por isso é preciso que sejam revistos os controles também, ou seja, a medida que um ciclo de vida se conclui, os controles devem ser revistos.



Obviamente que os controles sempre devem ser reavaliados, mas essa reavaliação deve ocorrer, principalmente, quando uma mudança ocorrer.



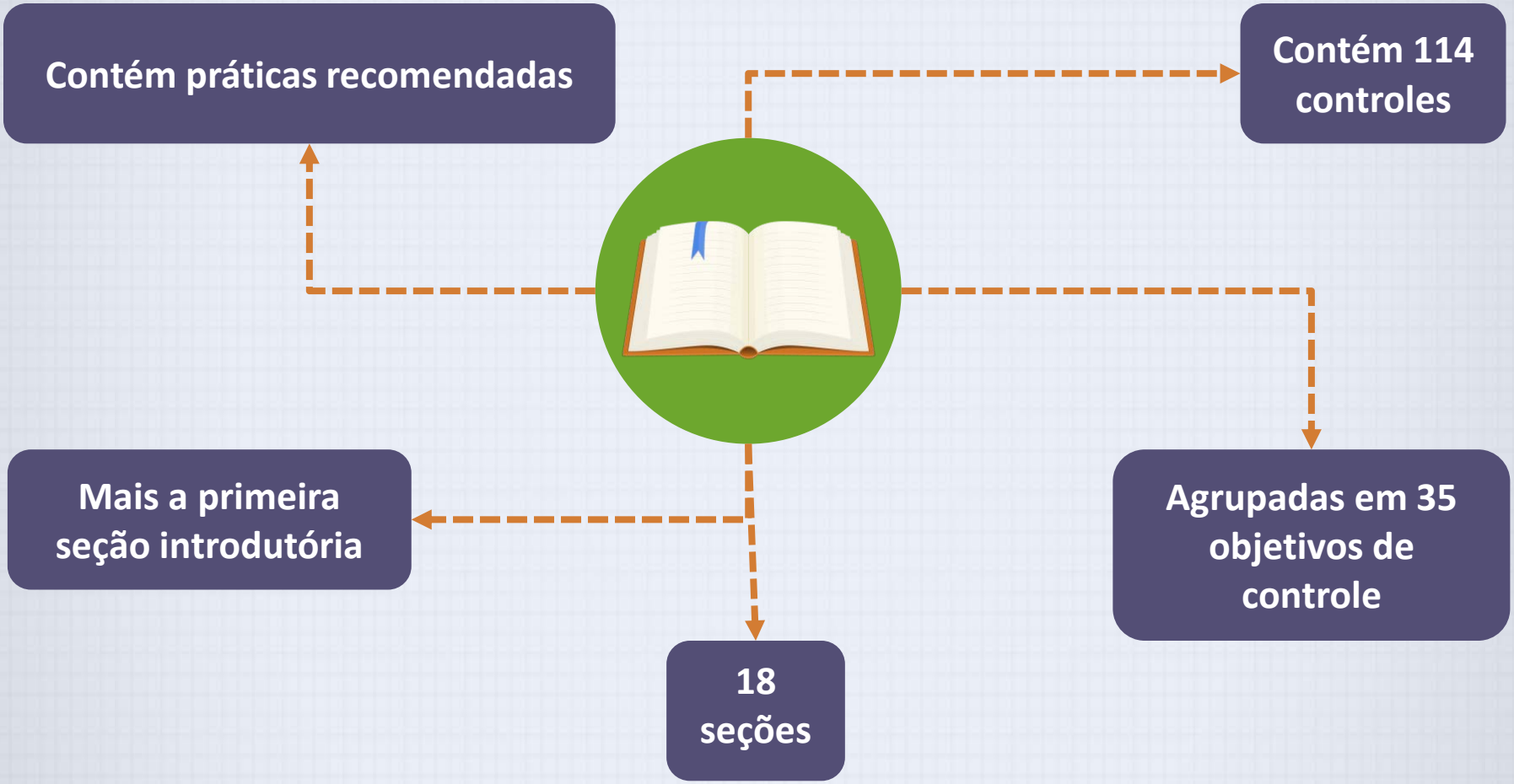
Estratégias da Segurança da Informação

A Segurança da Informação só pode ser melhorada através da execução de certos controles, independente se estratégicos, táticos ou operacionais, ou seja, de forma prática, basta seguir as atividades da fase de planejamento do ciclo, da quais são as mais importantes.

Estratégias - para melhoria da segurança da informação que o gestor pode decidir seguir, tais como:

- Concentrar-se no planejamento, conforme o PDCA e dependendo do caso, avaliar a terceirização da maior parte da execução das atividades:
- Ou a estratégia de concentrar-se exclusivamente na execução dos controles;
- E ainda, concentrar-se na verificação e ação, ou seja, o foco aqui é exclusivamente na melhoria contínua.

Estrutura da Norma ISO/IEC 27002:2013



Estrutura da Norma ISO/IEC 27002:2013

Cada controle tem aspectos processuais, técnicos, e às vezes, aspectos físicos.

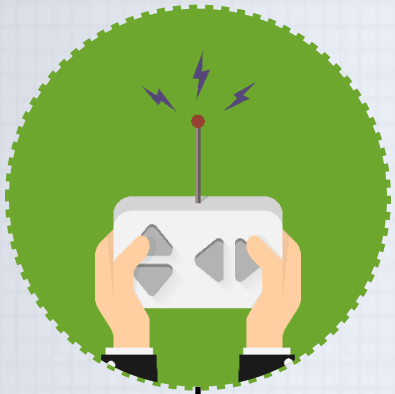
Apenas um conjunto limitado de controles trata de continuidade e aspectos humanos.

Estrutura da Norma ISO/IEC 27002:2013

A norma está dividida da seguinte forma:

0. Introdução 1. Escopo	7. Segurança dos Recursos Humanos	13. Gerenciamento da Comunicação
2. Referências Normativas	8. Gerenciamento de Ativos	14. Manutenção, Desenvolvimento e Aquisição de Sistemas Informação
3. Termos e Definições	9. Controle de Acesso	15. Relacionamento com Fornecedores
4. Estrutura da Norma	10. Criptografia	16. Gerenciamento de Incidentes de Segurança da Informação
5. Políticas de Segurança da Informação	11. Segurança Física e Ambiental	17. Aspectos do Gerenciamento de Segurança no Gerenciamento da Continuidade de Negócios
6. Organização da Segurança da Informação	12. Segurança da Operação	18. Conformidade

As Práticas da ISO/IEC 27002:2013



disponibilizam 114 controles

separados por 35 objetivos.

Não é necessário aplicar todos os controles em uma empresa, porque cada uma tem uma realidade diferente, mas é importante que se conheça a maioria destes controles, para distinguir quais serão os mais relevantes para a empresa.

A norma **ISO/IEC 27002:2013** está dividida em 18 seções, sendo que cada seção nos ajudará a tratar os aspectos de controle estratégico, tático e operacional.

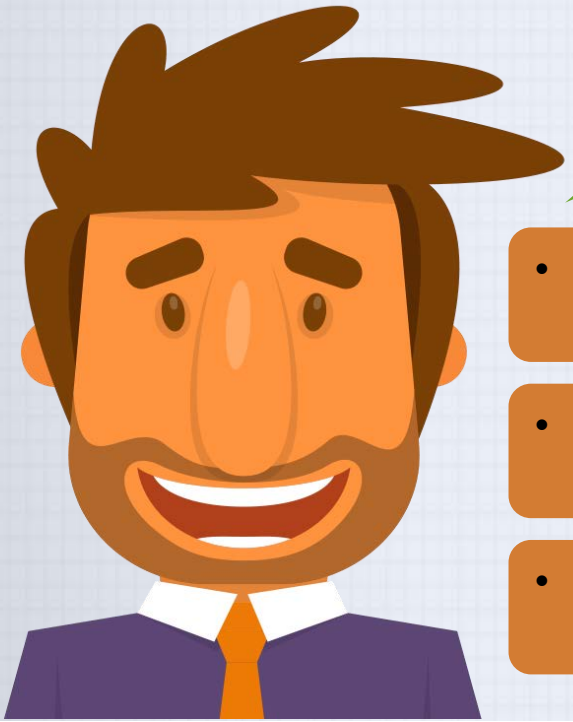
As Práticas da ISO/IEC 27002:2013

- Introdução 0
- Descrição do escopo da norma 1
- Referências normativas 2
- Termos e definições sobre Segurança da Informação 3
- Estrutura da norma em si 4
- Controles 5

Alguns dos controles abordam apenas da parte organizacional ou processual – dos processos, outros mais da parte técnica, como redes e softwares, e outros da parte física, entre outras coisas, como aspectos humanos, por exemplo.

Público-Alvo da ISO/IEC 27002:2013

A norma **ISO/IEC 27002** é indicada para as empresas que querem cuidar melhor da segurança de suas informações.



- **oferece diretrizes para o Sistema de Gerenciamento de Segurança da Informação (SGSI), e diretrizes diretas para as empresas.**
- **Ela auxilia desde a seleção de controles, até a implementação e manutenção, ou gerenciamento.**
- **E faz isto considerando as vulnerabilidades da empresa, considerando os riscos.**

Público-Alvo da ISO/IEC 27002:2013

Selecionar controles dentro do processo de implementação de um sistema de gestão da segurança da informação baseado na ISO/IEC 27001;

Implementar controles de segurança da informação comumente aceitos;

Desenvolver seus próprios princípios de gestão da segurança da informação.

Público-Alvo da ISO/IEC 27002:2013

- Estratégia do negócio;
- Das regulamentações, legislação e contratos;
- Do ambiente que sofre ameaças da segurança da informação, atual e futuro.

PDCA no Gerenciamento da Segurança da Informação

O PDCA é um ciclo que consiste em verbos em inglês, que indicam cada etapa dentro da gestão e são a base da ISO 27001:

PLAN – Planejar

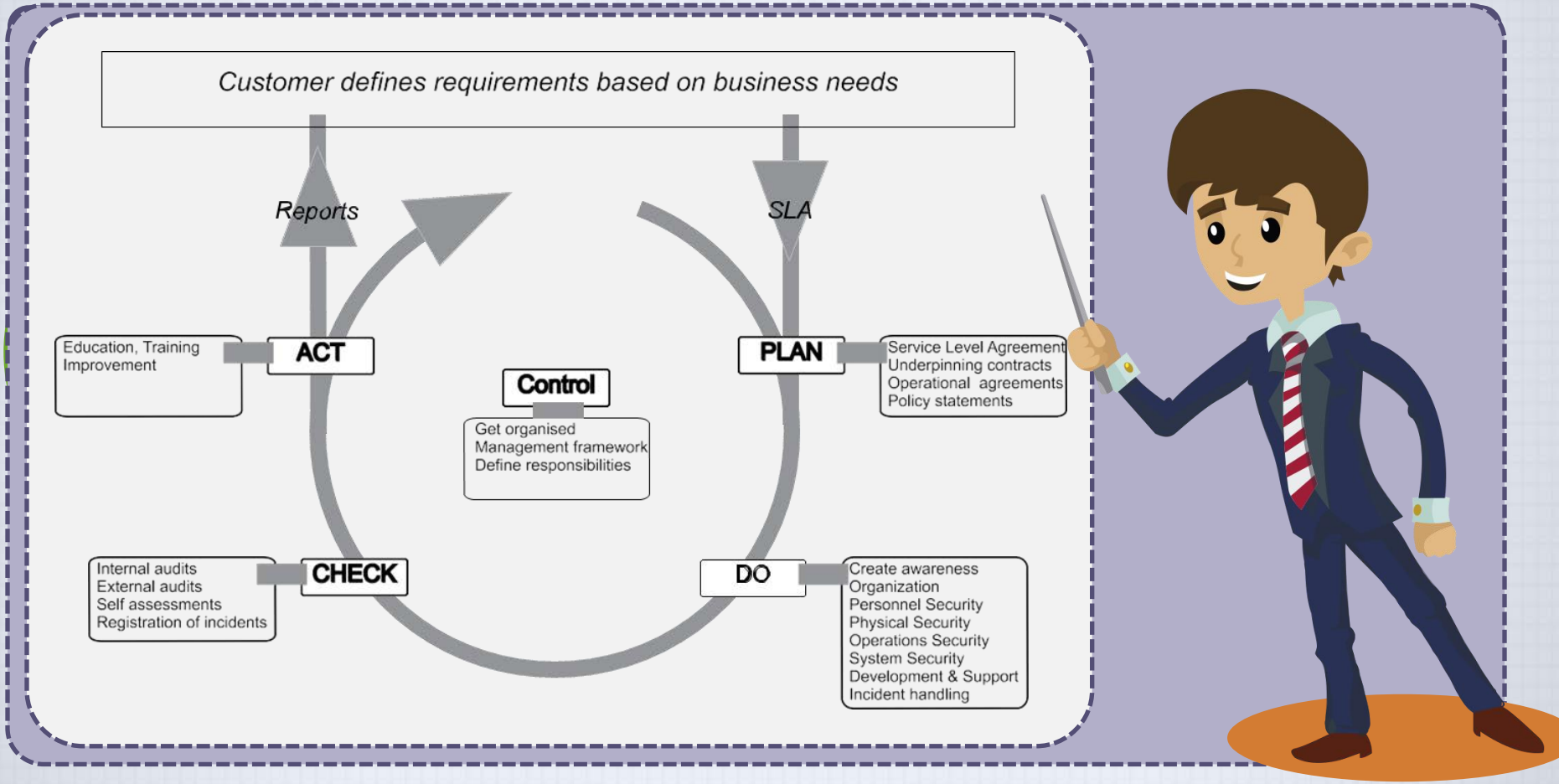
DO – Fazer ou realizar

CHECK – Checar ou verificar

ACT – Agir ou remediar

O ciclo PDCA fornece uma estrutura para a melhoria de um processo, embora careça de uma função de controle dos profissionais para manter o impulso deste ciclo.

PDCA no Gerenciamento da Segurança da Informação

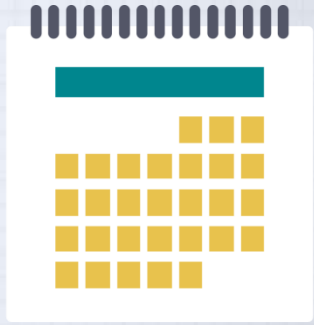


PLAN- Planejando a Segurança da Informação

O planejamento define controles que refletem diretamente os riscos apurados e que devem ser implementados no início de cada ciclo, gerando possibilidades de aprendizado e melhoria.

Exemplos desses planos:

- Modelos para relatórios;
- Descrições e processos para aplicação de medidas;
- Descrição de planos de melhoria para o tratamento de riscos;
- Revisões, avaliações e auditorias periódicas e planejadas;
- Coleta de dados sobre incidentes e ocorrências;
- Modelos de criptografia a serem utilizados;
- Descrições gerais de processos para incidentes, níveis de autorização e gestão.



Ciclo anual

DO – O Lado Operacional do Gerenciamento

O **ato** de "fazer" tem que ser encarado como as atividades que serão desempenhadas para manter os níveis ou qualidade na segurança da informação de uma organização.

Continuidade

Muitos dos processos operacionalizados são ações contínuas – elas são desenvolvidas várias vezes ao ano, ou novamente desempenhadas a cada ciclo.

Objetivo

Colocar em prática ações planejadas que possam refletir os requisitos dos clientes e os níveis de serviço.

DO – O Lado Operacional do Gerenciamento

Exemplos de processos contínuos:

- Lidar com incidentes, desde sua resolução até a produção de relatórios, ou ações conjuntas com outros âmbitos de suporte e resolução de problemas.
- Alinhar estratégias, sistemas e procedimentos a mudanças exigidas ou solicitadas.
- Gestão de identidades, usuários e autorizações.
- Atendimento a emergências, gerenciamento de vulnerabilidades e patches.
- Manter a organização sempre alerta e informada a respeito de riscos.
- Prestar suporte à avaliação de risco.
- Prestar suporte a revisões e auditorias.

CHECK – Revisando Tudo o Que Foi Feito

Uma gestão da segurança da informação simplesmente não funciona sem revisões constantes. É preciso avaliar e medir a eficiência, ou não, do que foi realizado pela parte operacional. Sempre haverá falhas humanas ou resistência ao aplicar certos procedimentos.

Objetivo

Verificar o cumprimento e alinhamento do que de fato ocorre com os padrões e políticas definidos em contrato ou no SLA (*Service Level Agreement* – Acordo de Nível de Serviços).

CHECK – Revisando Tudo o Que Foi Feito

Atividades

- Checagem a respeito do uso impróprio de informações e recursos, desde crimes relacionados a esse segmento até práticas fora do permitido pela empresa, como o acesso a conteúdo de risco ou uso de jogos eletrônicos.
- Cumprimento das medidas e padrões de segurança, checando regularmente se os padrões estão sendo seguidos.
- Conformidade com medidas legais, avaliando inclusive o uso de softwares ilegais.
- Revisão de segurança dos sistemas existentes.
- Auditorias, planejadas e executadas, com o mínimo grau possível de interferência no operacional.

ACT - Mantendo a Segurança em Dia

Atividades

- Análise de relatórios de desempenho;
- Fornecer dados para o processo de planejamento (PLAN), planos de curto prazo e melhorias anuais;
- Fornecer dados para as atividades de manutenção no SLA, bem como de atividades de manutenção em nível operacional.
- A revisão da gestão é parte do processo de gerenciamento da segurança. Essas revisões ocorrer para checar os níveis de eficácia da implementação e dos controles e medidas atuais. Essa revisão deve produzir dados e informações como:
- Análise dos incidentes e vulnerabilidades detectados;
- Feedback de partes interessadas;
- Resultados de auditorias e revisões;
- Status de ações corretivas e preventivas;

ACT - Mantendo a Segurança em Dia

- Níveis de segurança precisam ser mantidos e algumas razões ou argumentos para aplicação de melhorias apenas virão a partir de incidentes, vulnerabilidades detectadas e auditorias realizadas.
- Análises de risco precisam ser sempre atualizadas
- Guias e descrições precisam ser atualizados, para que novos ciclos possam ter início já com as melhorias realizadas.

Objetivos

- Melhoria do planejamento, inclusive de situações incluídas no SLA, na política de segurança da informação, em guias e manuais e em procedimentos operacionais;
- Melhorar a implementação de medidas de segurança específicas;
- Oferecer relatórios aos clientes sobre a performance dos fatores de segurança.

ACT - Mantendo a Segurança em Dia

Atividades

- Desempenho dos processos e conformidade com a política de segurança;
- Mudanças que possam afetar o ambiente de segurança da informação da organização, incluindo circunstâncias ambientais, de recursos, contratuais, regulatórias, técnicas e outras;
- Tendências relacionadas a ameaças e vulnerabilidades;
- Recomendações de autoridades relevantes;
- Laudos e conclusões de fornecedores e parceiros;
- Melhorias nos controles e metas;
- Melhoria na abordagem do tema dentro da organização;
- Melhoria na alocação de recursos e distribuição de responsabilidades.

Pronto para o próximo?

Curso Preparatório para Certificação
Em Gestão de Segurança da Informação Avançada – Baseada na ISO/IEC 27002:2013

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 2

Perspectivas de Segurança da Informação

Resumo

Neste módulo você precisa entender o interesse pela segurança da informação em algumas perspectivas, tais como:

- Distinguir os tipos de informação baseado nos seus valores de negócio e explicar as características de um sistema de gerenciamento para segurança de informação.
- Explicar a importância do controle da informação ao terceirizar e Recomendar um fornecedor com base na garantia dos controles de segurança.
- Distinguir aspectos da segurança em processos de gerenciamento de serviços e apoiar as atividades para conformidade.

Tipos de Informação

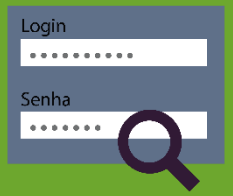
Nem tudo é livre, público, ou liberado para qualquer um ter acesso.

Tipos de Informação

públicas

Pode ser compartilhada com o público. São, em resumo, todas as informações que não representam riscos ao funcionamento da empresa.

confidenciais



Deve ser limitada a empresa, pois se saírem da empresa podem causar um desequilíbrio operacional, gerar vantagens aos concorrentes ou levar os clientes a perderem a confiança na empresa.

secretas

Toda informação crítica, cujo vazamento ou alteração pode ser muito prejudicial para as atividades da empresa, e cuja integridade deve ser mantida a qualquer custo.

internas

Não é uma informação que seja divulgada, é mais parecida com as normas e funcionamentos, dentro de uma empresa.

Valor da Informação

O valor da informação depende do uso que será feito dela. Para ficar mais claro, vamos estabelecer o seguinte:

- O valor da informação muda conforme o contexto e sua aplicação.
- É com base em informações adequadas que se pode tomar uma boa decisão.
- Informações precisas e atualizadas auxiliam na tomada de decisões.
- Informações ultrapassadas podem gerar perdas financeiras em um mercado competitivo.
- Excesso de informação pode causar confusão, desperdício de tempo.
- Dados sem importância são todos aqueles que não têm um impacto real.

Valor da Informação

Uma informação terá valor financeiro para uma empresa se ela ajudar a empresa a ter mais lucro ou se ajudar a obter uma vantagem competitiva.

- Conferência do processo;
- Identificação de custos;
- Acompanhamento de recursos;
- Entendimento da cadeia produtiva;
- Cálculo dos retornos de investimentos;
- Informações financeiras, despesas relativas à manutenção da empresa com funcionários e outras coisas.

Valor da Informação

É possível mensurar – medir – o quanto cada funcionário rende ou não, por exemplo.

Sistemas de Gerenciamento

ERP

Pode criar um relatório de vendas, com base nas vendas feitas em determinado período. Com base nisto, é possível saber se um produto foi mais vendido que outro, e assim, começar a delinear uma estratégia de venda para os menos vendidos, ou mesmo definir se ele ainda será ou não comercializado.

Aspectos da Informação

Privacidade – deriva da confidencialidade, e está relacionado aos direitos que um indivíduo possui sobre seus dados confidenciais.

Autenticidade – relacionado à confidencialidade e também à disponibilidade, a autenticidade garante a origem de uma informação e também a identidade das pessoas que a manipularam.

Anonimidade – confidencialidade relacionada à identidade das pessoas envolvidas. Por exemplo, em casos de denúncias online, por exemplo, nas quais o denunciador pode ser afetado pela divulgação de seus dados pessoais.

Auditabilidade – possibilidade de verificação da idoneidade e procedência das informações e se as mesmas estão em conformidade com as premissas básicas de segurança da informação.

Ciclo de Vida da Informação

Especificar quais os pontos do ciclo de vida da sua informação, para ajudar na criação de um sistema que seja adequado. A segurança desta informação deve estar bem alinhada, ponto a ponto, com cada parte deste ciclo.

Quando uma empresa resolve trocar computadores antigos. Aos olhos da empresa, é uma máquina que não serve mais, que já funcionou o que poderia e agora pode ser repassada em leilões ou doada à instituições. Neste caso, algumas empresas cuidam das máquinas fazendo uma formatação e apagando as informações existentes, mas outras, não se dão conta disto, encaram tanto as máquinas quanto a informação contida ali, como 'lixo' ou material que pode ser descartado.

Ciclo de Vida da Informação

- Se estas máquinas possuem ERPs que usavam banco de dados locais, é possível que haja relações inteiras de números de documentos associados aos nomes e endereços de clientes, por exemplo.

- A segurança acompanha desde o momento de desenhar a ideia do sistema, até o momento em que este sistema seja substituído por outro.

Importância da Informação

Interna

A organização precisa ter acesso a informações confidenciais, precisas e completas para que possa operar – é função da segurança da informação zelar por isso. Se nós descuidamos internamente, imagine só com aquilo que vem de fora...

Externamente

- Informações inadequadas e sem segurança podem levar a produtos e serviços imperfeitos ofertados ao público externo.
- Informações sem segurança podem gerar problemas que afetem a imagem e até a saúde financeira da empresa frente ao público externo.

Importância da Informação

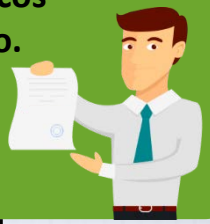
A gestão da segurança da informação deve ser uma parte integral dos critérios e procedimentos de qualidade dentro de qualquer empresa.

- O dono deste processo dirá o que é importante ou não.
- A gerencia da empresa que define quais informações podem ou não ser compartilhadas, são eles que definem o grau de controle.
- São eles que sabem o valor da informação e o quão critica pode ser para a empresa.
- O gerente de segurança trabalha para garantir que esta informação receba o cuidado adequado, mas quem define o grau de cuidado, é o proprietário da informação.

Interessados no SGSI

A informação é o bem mais valioso para muitas das empresas e organizações. Diante disso, a informação, devido sua importância, é chamada de ativo dentro do conceito de Segurança da informação.

Documentar um plano de ação, bem detalhado e objetivo para lidar com as ameaças e riscos da informação.



Funcionários

Diretoria

Gerência

Este plano vai viabilizar o controle dos riscos, pois não faria sentido identificar as ameaças e os riscos, se não forem controlados efetivamente.

Interessados no SGSI

- As normas ISO podem ser usadas para criar os parâmetros de segurança para vários setores, incluindo os diferentes interessados no SGSI (Sistema de Gerenciamento de Segurança da Informação).
- Deve haver uma perspectiva diferente para o cliente, para a empresa, para o gerente de segurança da informação, ou para o próprio negócio, porque a falta de segurança os atinge de modos diferentes.
- Os fornecedores não devem ficar de fora, não só por serem uma peça fundamental na cadeia de fornecimento de informação, mas porque eles também devem ser atestados quanto à qualidade dos serviços, pois eles também se beneficiam da confiabilidade e da segurança que a marca da empresa passa.
- Os próprios funcionários ou colaboradores devem aprender a política da empresa, por meio de treinamentos, para que possam melhor colaborar com ela.

Perspectivas da Segurança da Informação

A **Segurança da Informação** não é um objetivo em si, mas sim um meio para que todos os objetivos da empresa sejam alcançados.

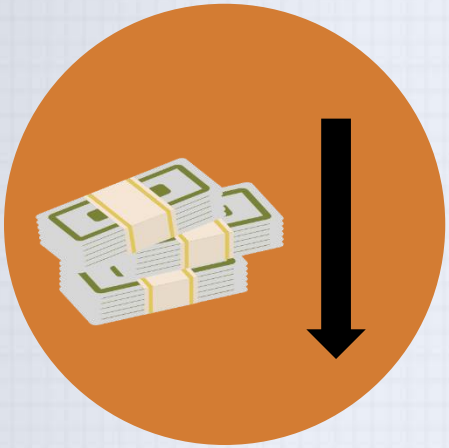
Uma empresa coleta e organiza dados. Esses dados são armazenados, processados e disponibilizados para consulta quando necessário.

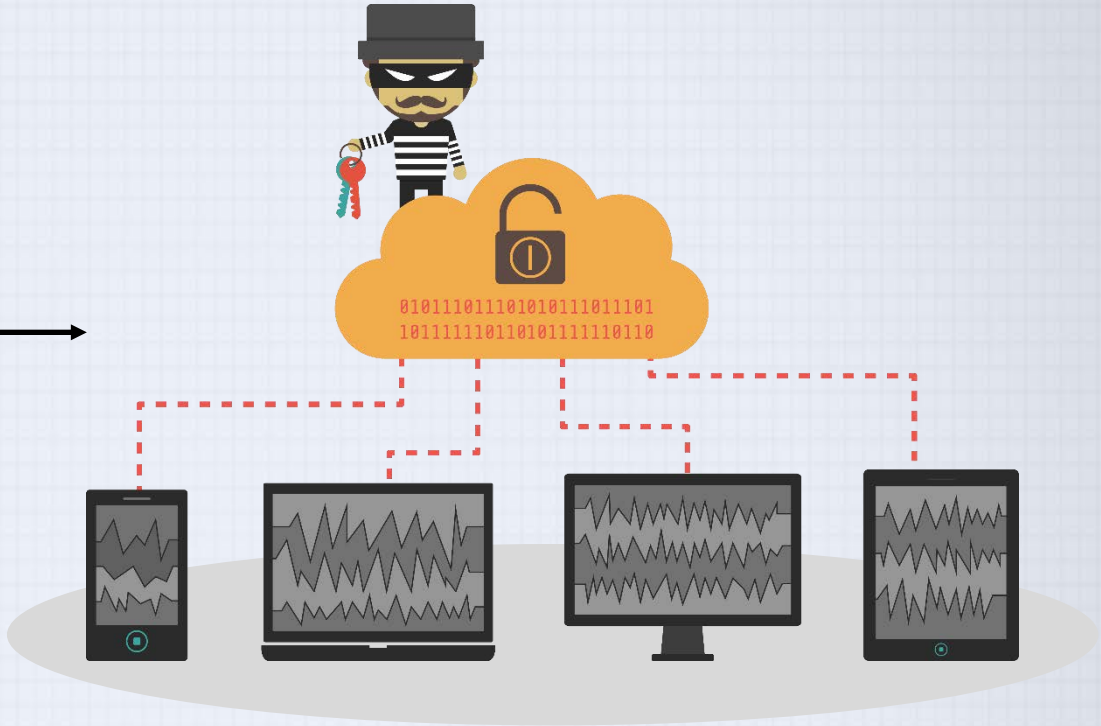
- As pessoas responsáveis pelo gerenciamento da informação precisam confiar na integridade desses dados.
- É preciso garantir que apenas as pessoas realmente autorizadas tenham acesso a esses dados.
- Confiabilidade, integridade e disponibilidade são características que têm de existir como padrão em todas as operações – isso não é discutível.
- Qualquer empresa, desse modo, precisa organizar a coleta, armazenamento, manuseio e processamento das informações, de modo a atender a essas premissas.

Perspectivas da Segurança da Informação

- **Para determinar o grau de segurança, é preciso então conhecer o valor da informação que será gerida e os riscos envolvidos em seu gerenciamento.**

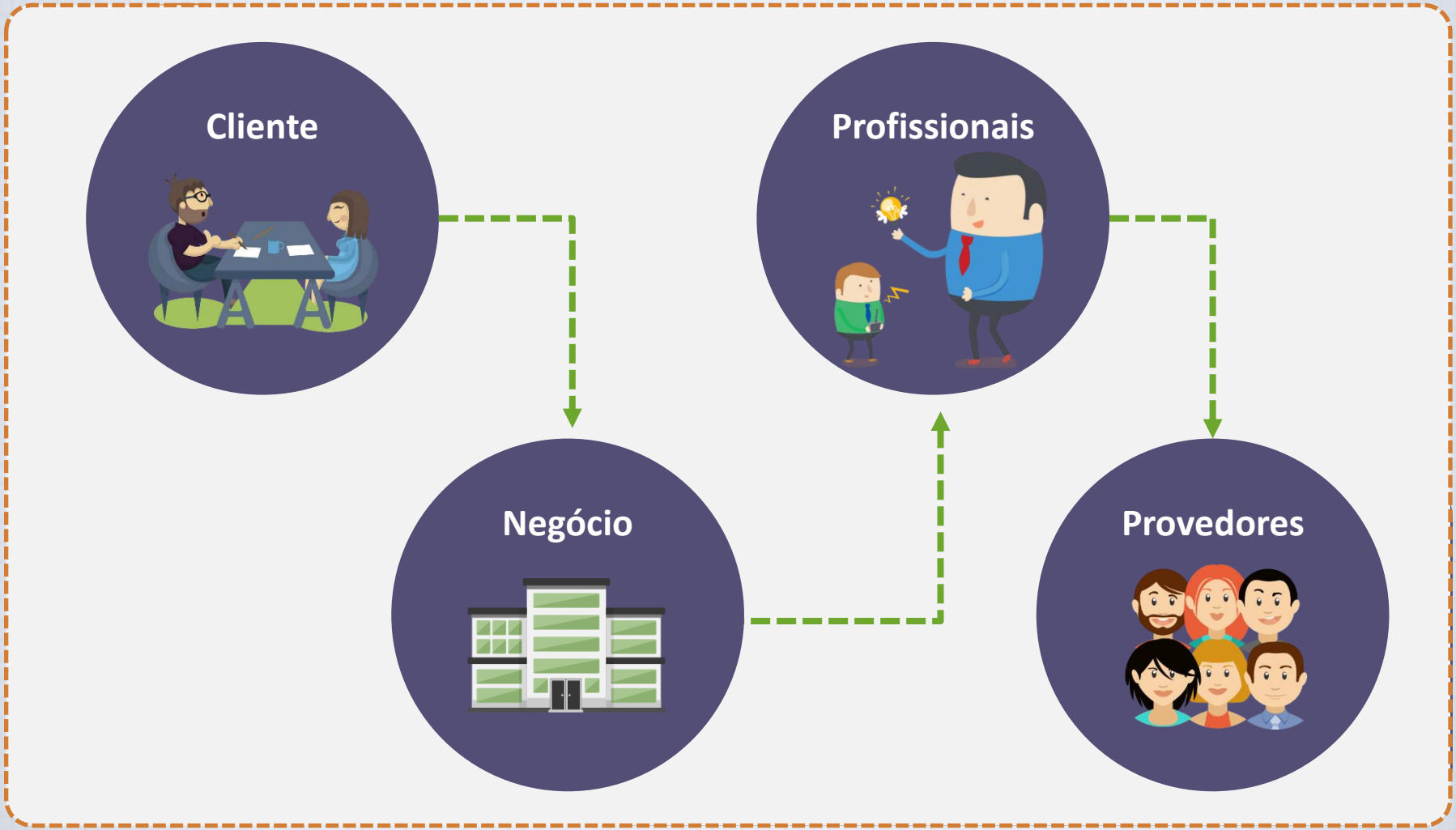
Partes Interessadas





Os riscos nem sempre estão muito longe da realidade diária, e não estão restritos às grandes corporações, porque mesmo se você for apenas um simples usuário de computador, pode ainda estar sujeito aos riscos mais comuns, ou seja, a necessidade de controles de segurança é perceptível até mesmo a quem não trabalha com a área, ou não entende muito a respeito.

Partes Interessadas



O Cliente

"trust me" → "prove to me"

Endosso da diretoria. Uma espécie de declaração, geralmente contratual, de que os níveis de segurança adotados são geridos e atendem a normas locais ou internacionais.

Certificações. Certificados externos que garantem que o provedor de serviços é capaz de atender determinados requisitos, seguindo normas como a ISO 27001 e possuindo as respectivas certificações.

Auditoria. Relatórios elaborados por outras empresas e terceiros que aprovem e endossem as políticas de segurança adotadas.

O Cliente

Processos comuns, como gestão de incidentes, gerenciamento de autorizações e planos de continuidade.

Responsabilidades e contatos para cada uma das situações.

Relatórios.

Mecanismos para o ganho de escala.

Perspectiva do Cliente

Você deve entender a perspectiva do cliente das informações dentro de um escopo de segurança da informação e de governança também, tais como:

O cliente hoje em dia tem muito mais poder de voz.

O cliente compartilha o que ama e o que odeia em cada empresa, e isto se espalha de modo viral.

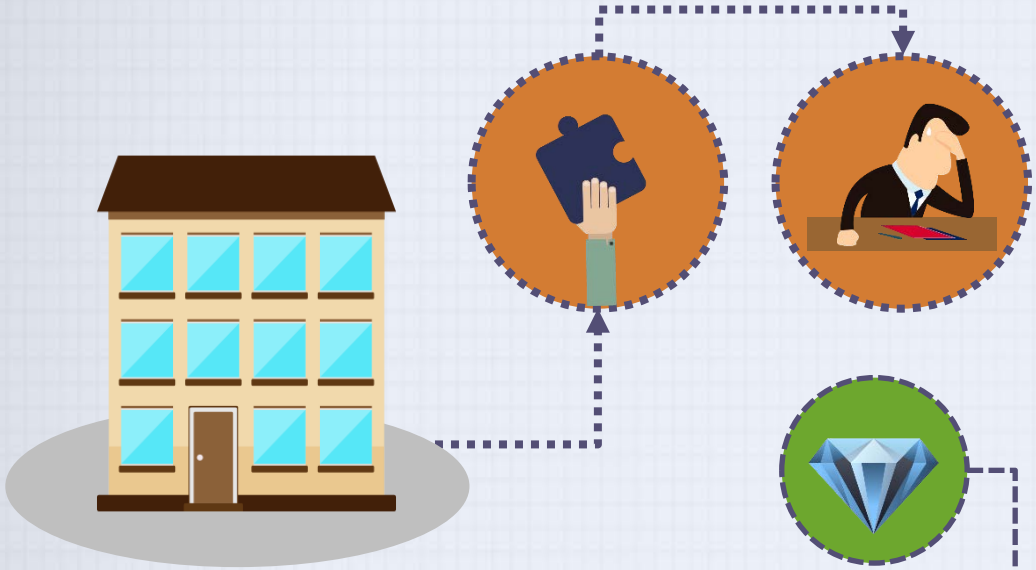
O cliente gosta de quem é transparente, de quem demonstra segurança.

Perspectiva do Cliente

Para os negócios em ambientes B2B ou e-commerce, a confiabilidade tanto da empresa quanto do próprio ambiente é fator indispensável.

- Clientes exigem uma continuidade integral das operações de TI;
- Devido um mercado mais aberto os clientes podem resolver seus negócios em outro lugar, em outra empresa;
- As preocupações com a privacidade ainda são muito fortes, embora o uso de mídia social mostre que essa é uma "faca de 2 gumes";
- Os clientes costumam expor na mídia sobre os incidentes de segurança;
- Clientes depositam confiança nas organizações que são transparentes na forma como lidam com os riscos;
- Infelizmente os usuários finais não recebem quase nada de treinamento, principalmente treinamento em segurança da tecnologia da informação que é praticamente ausente;
- Usuários finais não percebem os riscos de segurança da mesma forma que os profissionais de TI, de segurança, etc;
- Segurança é frequentemente considerada como algo opcional ao invés de um requisito integrado à tecnologia.

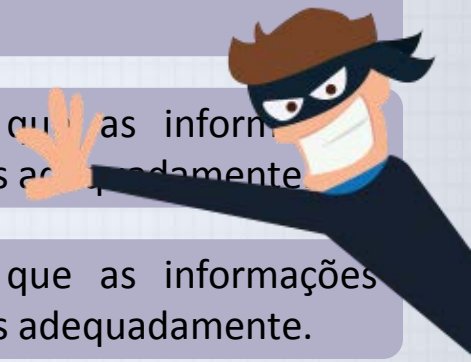
O Negócio



A **ISO/IEC 27002:2013** fala que o valor da informação não está apenas nas palavras escritas ou nos números e nas imagens. Está na informação como um todo. O modo operacional, o conhecimento, e isto inclui fórmulas de produtos, os conceitos adotados pela empresa, as estratégias financeiras e de marketing, as marcas e patentes, são intangíveis, mas que formam o valor da empresa como um todo, e este valor deve ser protegido.

SGSI

- Atua prevenindo e orientando as pessoas.
- Cuida para que as informações sejam usadas adequadamente.
- Cuida para que as informações sejam usadas adequadamente.
- Para que as pessoas que possuem acesso sejam autorizadas.
- Para que os equipamentos estejam protegidos.
- E para que nada das informações vazem ou sejam alteradas.



O Negócio

O mundo atual é totalmente interconectado, e por isto estas informações requerem proteção contra vários riscos. Na empresa, a segurança da informação é um ativo, é algo com o qual ela se preocupa, e onde ela investe, porque sabe o que pode acarretar com a falta de cuidado.

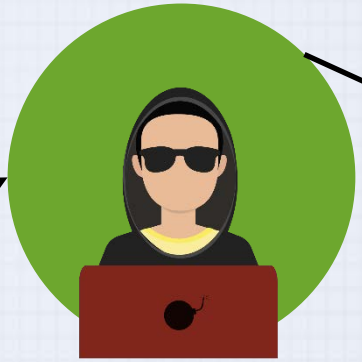
Perspectiva de Negócio

- A Informação se tornou o ativo mais importante para a maioria dos negócios;
- É fundamental e vital proteger esse valioso ativo contra perdas, adulterações e divulgações;
- As informações estão por toda a parte;
- Os responsáveis pela informação precisam demonstrar que eles são confiáveis e estão em conformidade, por isso a gestão das informações é a chave para o sucesso;
- Quando as normas internacionais são respeitadas, como a série da ISO 2700, acabam ajudando a entender como lidar com a conformidade;
- As leis e os regulamentos forçam as organizações a cumprirem com a privacidade dos dados e as melhores práticas de propriedade intelectual;
- Os clientes e até mesmo os fornecedores exigem transparência e conformidade;
- O conhecimento da ocorrência de um incidente se prolifera rapidamente, e isso causa danos à reputação da empresa, podendo estar fora de seu controle, por isso é necessário um enfoque na prevenção;
- O monitoramento, o registro e uma organização proativa são os elementos-chave, por isso que a detecção imediata de incidentes e o gerenciamento de incidentes são processos cruciais;
- Como a informação está por toda parte, a segurança da informação e a consciência dos riscos necessitam da atenção de todos, ou seja, precisa estar incorporada na organização.

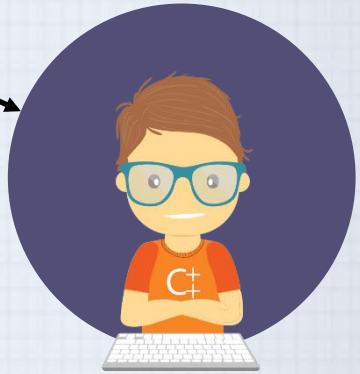
O Profissional de SGSI

Assim como em vários outros negócios, é preciso entender os interesses da empresa, por isso o profissional de SGSI precisa conhecer a empresa para poder ser capaz de definir - juntamente com os membros da própria empresa - uma estratégia de trabalho eficaz.

É impossível o profissional trabalhar sozinho



Hackers Maliciosos



Hackers Éticos

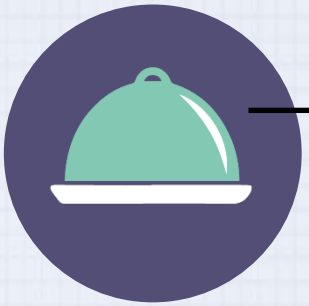
Ou seja, o profissional que não destrói, e sim, ajuda a proteger, uma vez que ele conhece bem o sistema por dentro.

Perspectiva do Profissional de SGSI

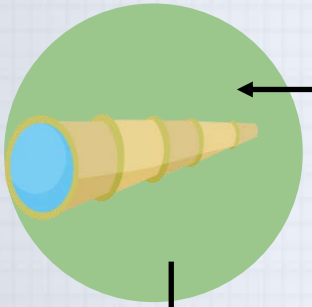
- Os profissionais de segurança precisam descer do “salto alto”;
- Capacitação é essencial;
- Precisam estar aptos para mostrar conformidade em relação à base de conhecimento;
- Não lida apenas com tecnologia da informação, mas é... uma profissão multidisciplinar;
- Precisa entender os princípios de negócio e como a segurança pode capacitar a organização;
- Nenhuma solução serve para tudo;
- Educação contínua faz parte do trabalho;
- Precisa entender a mentalidade dos seus adversários, conhecer seu inimigo e suas táticas;
- Precisam entender os riscos que sua organização enfrenta e os riscos internos e externos;
- Contratar outro profissional para realizar o trabalho, como por exemplo, um hacker ético.

Os Fornecedores

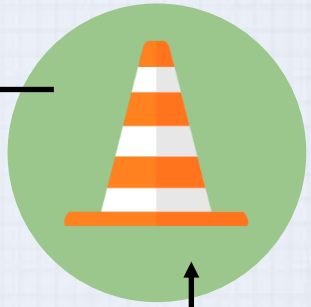
Precisa seguir os requisitos de segurança de seus clientes, mesmo possuindo suas próprias diretrizes e normas para segurança de sua equipe e dos recursos próprios.



Os **fornecedores de serviços** ou de produtos fazem parte da cadeia de interesse na segurança da informação, tanto como quem fornece como ou para quem está se relacionando no processo.



Mudar a forma de lidar com o fornecedor, ou até mudar o fornecedor.



- **SLA** (Service Level Agreement)
- **ANS** - Acordo de Nível de Serviço

Os fornecedores precisam mostrar muito cuidado com quem se relacionam, e é sempre ideal seguir os padrões de melhores práticas.

Os Fornecedores

Manter a **transparência** sempre.

É preciso também ter uma **segunda ou terceira opinião** quanto aos serviços oferecidos.

Os prestadores de serviços que atendem a empresa precisam entender as exigências dos seus clientes para conseguir atender corretamente, neste caso, um gerenciamento de segurança de que busca por vulnerabilidade precisa ser implementado usando padrões das melhores práticas como ITIL, CobIT e a própria ISO, por isso é preciso criar um manual pelo qual o fornecedor possa se guiar.

Perspectivas dos Fornecedores

- Provedores precisam demonstrar cuidado com a segurança da informação;
- O uso de padrões das melhores práticas prevalece;
- O gerenciamento contínuo de incidentes e das mudanças são processos-chave;
- Segurança da informação deve se tornar uma parte dos processos de gerenciamento do ANS;
- Monitoramento ativo e gerenciamento de vulnerabilidade precisam de mais atenção;
- Transparência é chave, mas difícil de manter em um ambiente de serviço compartilhado;
- Fornecedores do serviço precisam entender os requerimentos dos negócios de seus clientes;
- ... usando padrões de melhores práticas, como ITIL, CobiT e padrões ISO;
- É vital que terceiros avaliem esses riscos;
- Ter indicadores de desempenho é a chave para o sucesso no controle e monitoramento;
- ... mas a segurança de dados é ainda mais, já que isto requer uma nova mentalidade, bem como soluções e produtos diferenciados.

Relacionamento com os Fornecedores

Garantir a proteção dos ativos da organização que são acessíveis por eles, por isso deve ser garantido que os requisitos de segurança da informação, para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização, sejam acordados com o fornecedor e principalmente...

- **A organização deve identificar e documentar dos tipos de fornecedores.**
- **Os controles englobam os procedimentos e processos a serem implementados, tanto da empresa quanto do fornecedor para a sua implementação.**
- **Desenhar um processo padronizado e o ciclo de vida para gerenciar as relações com o fornecedor, juntamente com a definição dos tipos de acesso à informação que diferentes tipos de fornecedores terão permissão.**

Documentados e assinados por ambas as partes;

Relacionamento com os Fornecedores

Os requisitos mínimos de segurança da informação para cada tipo de acesso e tipo de informação devem ser levantando, assim como aquelas informações que são transferidas entre as partes.

Garantir também treinamento de conscientização para o pessoal da organização envolvido com a aquisição, relativo aos procedimentos, processos e políticas aplicáveis, para o pessoal da organização que interage com o pessoal do fornecedor.

Requisitos de Segurança com os Fornecedores

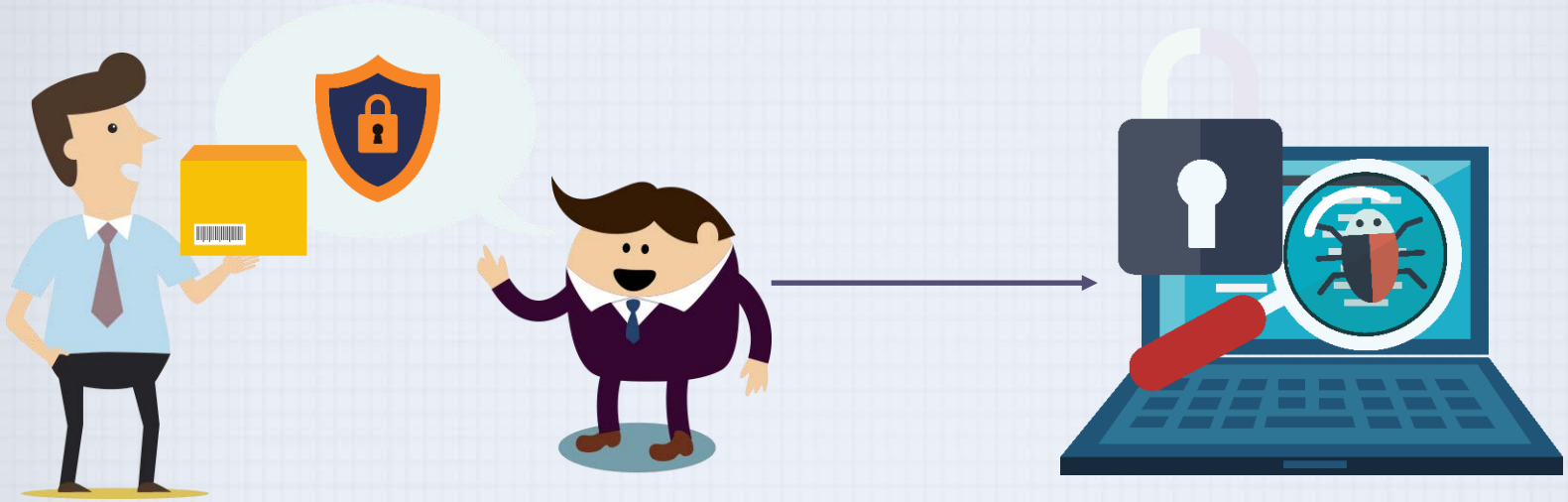
- Descrição da informação a ser acessada/fornecida e os métodos de acesso a informação;
- Classificação da informação de acordo com o esquema de classificação da organização, ou ainda, mapeamento do esquema de classificação da organização com o do fornecedor;
- Requisitos regulamentares e legais, incluindo a proteção de dados, os direitos de propriedade intelectual e direitos autorais, e uma descrição sobre como isto será assegurado que os fornecedores cumprirão.
- Obrigação de cada parte contratual para implementar o conjunto de controles acordados, incluindo o controle de acesso, a análise crítica do desempenho, o monitoramento, o reporte e a auditoria;
- Regras de uso aceitável da informação, incluindo o uso inaceitável, se necessário;
- Uma lista explícita do pessoal do fornecedor autorizado a acessar ou receber as informações da organização ou as condições e procedimentos para autorização e remoção do pessoal do fornecedor para acessar ou receber as informações da organização;
- Políticas de segurança da informação relevantes para o contrato específico;
- Procedimentos e requisitos de gestão de incidentes (especialmente para notificação e colaboração durante a correção de um incidente);

Requisitos de Segurança com os Fornecedores

- Requisitos de treinamento e conscientização para procedimentos específicos e requisitos de segurança da informação, por exemplo, resposta à incidentes, procedimentos de autorização;
- Regulamentações relevantes para subcontratação, incluindo os controles que precisam ser implementados;
- Acordos relevantes com parceiros, incluindo um contato pessoal para as questões de segurança da informação;
- Requisitos de seleção, se necessário para o pessoal do fornecedor...;
- Direito de auditar os processos do fornecedor e os controles relacionados ao acordo;
- Processos para resolução de defeitos e de conflitos;

- Obrigações do fornecedor para, periodicamente, apresentar um relatório independente da eficácia dos controles e um acordo das correções em tempo hábil, das questões relevantes apresentadas no relatório;
- Obrigações do fornecedor de cumprir com os requisitos de segurança da informação da organização.

Acordos com Fornecedores



Os acordos com fornecedores devem incluir os diversos requisitos vistos anteriormente.

Assim, será possível contemplar os riscos de segurança da informação associados com a cadeia de suprimento de produtos e serviços de tecnologia das comunicações e informação.

Nestes acordos devem incluir a definição dos requisitos de segurança da informação na aquisição de serviços ou produtos.

Acordos com Fornecedores

Exija que os fornecedores divulguem os requisitos de segurança da informação da organização em toda a cadeia de suprimento, caso os subfornecedores sejam parte do serviço de tecnologia da comunicação e informação a ser fornecido para a organização.

Exija que os fornecedores divulguem as práticas de segurança da informação apropriadas ao longo de toda a cadeia de suprimento, caso esses produtos incluam componentes comprados de outros fornecedores.

Um processo de monitoramento e métodos para validação destes serviços e produtos deve estar aderente aos requisitos de segurança da informação.

Deve ser considerado também um processo para identificação dos componentes do serviço ou produto que são críticos para manter a funcionalidade.

Garanta que sejam inclusas definições de regras para compartilhamento da informação com relação a cadeia de suprimento e quaisquer questões potenciais e compromissos assumidos entre a organização e os fornecedores.

Monitoramento dos Fornecedores

fazer uma analise crítica

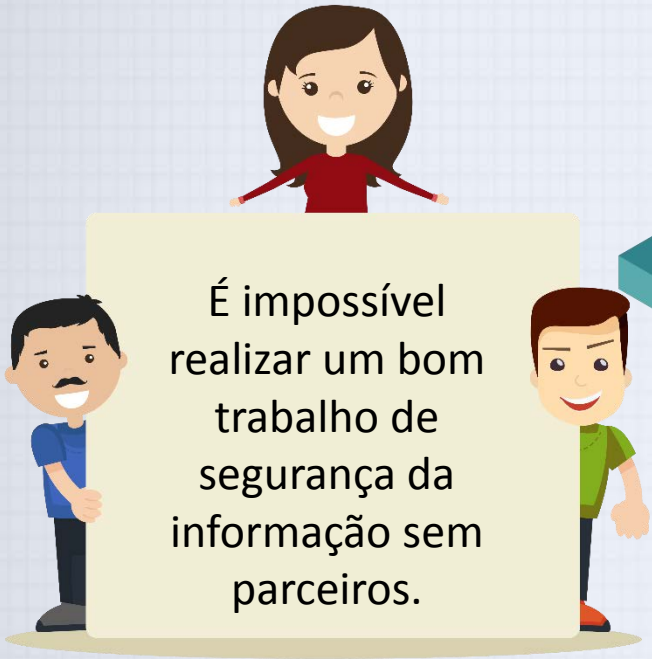
Isso garante que os termos e condições dos acordos de segurança de informação sejam cumpridos e que os incidentes e problemas de segurança da informação sejam gerenciados de forma apropriada.

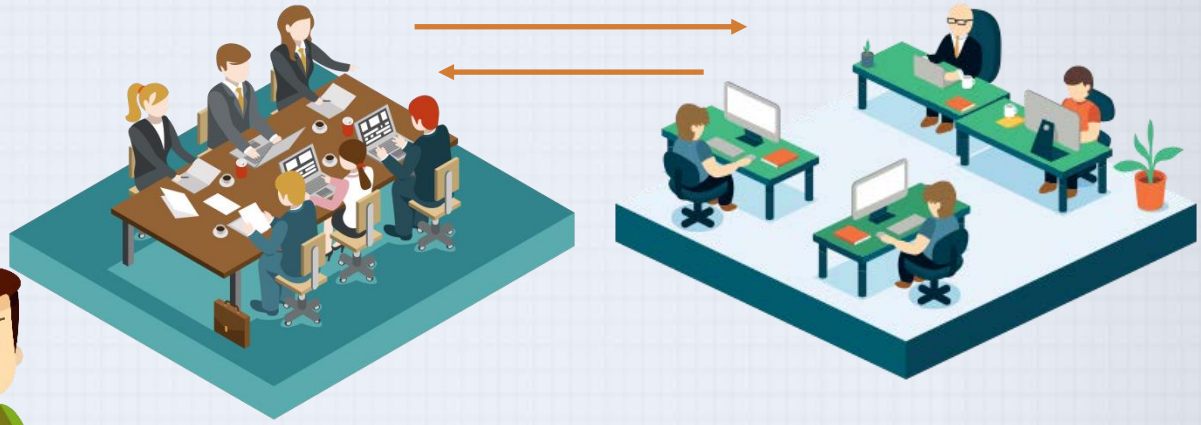
- **O monitoramento, análise e a auditoria englobam os relatórios de serviços produzidos pelos fornecedores.**
- **Mas também informações sobre incidentes de segurança de informação, problemas operacionais, falhas, investigação de falhas e interrupções relativas ao serviço entregue, assim como a sua capacidade de serviço.**
- **Tais mudanças que devem ser gerenciadas pela organização incluindo mudanças nos acordos com o fornecedor, mudanças feitas pela organização para implementar melhorias dos serviços atualmente oferecidos, desenvolvimento de quaisquer novas aplicações e sistemas, modificações ou atualizações das políticas e procedimentos da organização...**

A Quem Mais Interessa?

- Cliente que se sente seguro com a aquisição de um bem ou serviço de uma empresa;
- O vendedor também sente segurança na oferta dos seus produtos e serviços;
- E o dono da empresa que confia nas informações que recebe.

Perspectiva do Parceiro





As informações precisam trafegar entre essas empresas e organizações de duas formas distintas:

- **Gestão centralizada**. Os parceiros fornecem e recebem informação de um único ponto, ou um dos parceiros que gerencia tanto a apuração quanto o compartilhamento de informações.
- **Gestão descentralizada**. Parceiros que fornecem e recebem informações estabelecendo rotas de acordo com o necessário – em termos de arquitetura, funciona quase como uma rede social.

Perspectiva da Supervisão e Auditoria

- Objetivos e controles que estejam realmente implementados;
- Supervisão e coordenação interna, usando relatórios para apontar exceções que exijam uma análise mais minuciosa;
- Mecanismos e processos sempre revisados;
- Treinamento, conscientização e educação de todos nas atividades necessárias para garantir a segurança, com bom nível de instrução e motivação;
- Penalidades ou advertências no caso de irregularidades;
- Alinhamento e padrões de qualidade em linha com os requisitos necessários para atender ao compliance em cada sistema;

Perspectiva da Supervisão e Auditoria

- As empresas precisam de um ambiente dinâmico, liberdade de inovação, competitividade e também aceitar alguns riscos.
- Mas precisam agir com responsabilidade, consciente dos riscos e minimizando seus impactos, de modo a não afetar parceiros envolvidos.

- Inadequações na política de segurança da informação;
- Controles ineficientes e ineficazes, uso pobre de recursos ou baixa governança;
- Estratégias, políticas, controle e práticas ineficazes em TI;
- Checam o 'compliance' para verificar a adequação dos sistemas a todas as normas internas e externas.

O que auditores de TI reveem?

Desafios e Fatores de Sucesso

Principais Desafios:

- Fraco envolvimento da gerência e lideranças de outros setores no processo de segurança da informação;
- As metas e objetivos do programa de segurança da informação são ambiciosos demais em relação aos recursos e disponibilidades;
- Desenvolvimento de soluções “perfeitas” no papel, mas que não se adequam ao perfil da organização;
- Falta de comprometimento do pessoal;
- Não há como relatar os incidentes “invisíveis”;
- Inconsistências entre departamentos, processos e sistemas ao lidar com a segurança;
- Exceções que são transformadas em rotina;
- Sistemas e mecanismos de segurança que “aparecem” só depois do projeto estar desenhado e concluído;
- Falta de avaliações e de feedback.

Desafios e Fatores de Sucesso

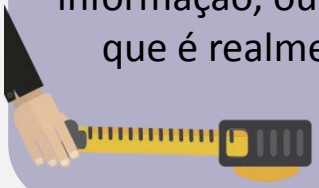
Fatores críticos para o sucesso:

Envolvimento amplo das pessoas no processo de gestão e manutenção das normas e diretrizes de segurança.

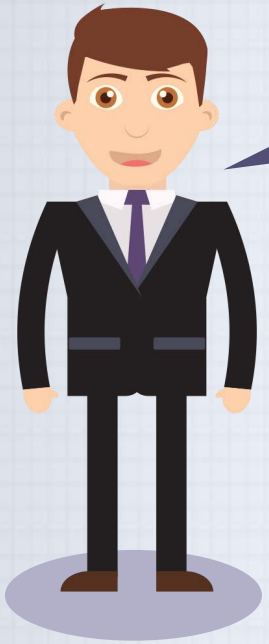
Comunicação e alerta a todos os usuários e profissionais envolvidos.

Delegação clara das responsabilidades e das tarefas nos processo de segurança da informação.

Realizar a medição e as tarefas do processo condizentes com o valor da informação, ou seja, medir e gerenciar o que é realmente importante para o negócio.



Desafios na Governança e na Empresa



Episódios relacionados à segurança da informação com grandes organizações tornaram a necessidade de governança indiscutível. A segurança da informação é parte desse foco em governança e gestão de riscos.

As normas da ISO 27001

É preciso garantir que todas as responsabilidades e papeis a serem desempenhados estejam descritos a fundo:

- Em manuais de RH;
- Em contratos de trabalho;
- Em descrições das funções;
- Em medidas disciplinares.

O profissional de TI geralmente ignora questões de governança. Elas são essenciais para a segurança da informação.

Os líderes precisam de visão estratégica e comunicação com lideranças de outros setores.

Estratégica, tática ou operacional.

Desafios com a Documentação

Dica: cuidado, no entanto, com regras e normas excessivas ou redundantes – elas podem tornar o exercício da gestão algo impossível.

- Processos de autorização e aprovação
- Verificação de normas de compliance

- Treinamentos e campanhas com usuários
- Inspeções, auditorias e revisões de terceiros

Estratégica

Tática

Operacional

- O nível estratégico, por exemplo, contará com a política de segurança, que considera a organização como um todo.
- O nível tático detalha de certo modo os métodos e ferramentas a serem utilizados.
- O operacional pode incluir os planos e guias para o usuário final.

Documentação

O Gerenciamento da Segurança da Informação requer uma estrutura de documentação que auxilie na padronização para se evitar inconsistências e para documentar o que foi feito, e para fins específicos, incluindo:

- Evidenciar um processo, políticas, etc.
- Formação e sensibilização dos usuários
- Avaliação da conformidade
- Revisões por terceiros

Estrutura de documentos:

- A política documentada;
- Documentação que descreva a situação atual, derivada de uma autoavaliação, auditorias internas e externas. A situação atual é descrita:

Para a organização como um todo

Por unidade de negócio dentro da organização ou do sistema

Documento Operacional

Para garantir uma operação segura e correta dos ativos, é necessária a documentação dos procedimentos de operação, mas não só documentados, mas também disponibilizados a todos os usuários que necessitem deles.

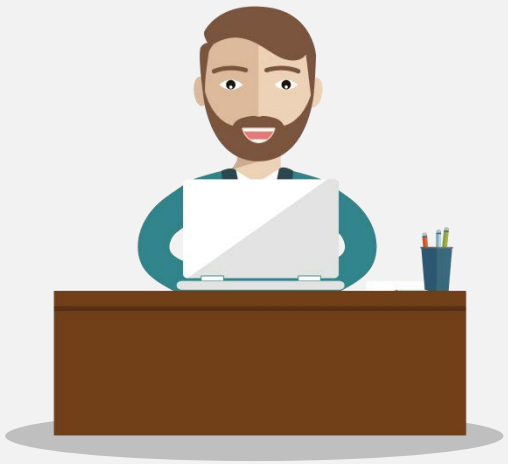
Uma documentação operacional contém procedimentos e atividades operacionais associadas a recursos de comunicação e informações, tais como:

- Procedimentos de inicialização;
- Desligamento de computadores;
- Geração de cópias de segurança (backup);
- Manutenção de equipamentos;
- Tratamento de mídias;
- Segurança e gestão do tratamento das correspondências e das salas de computadores.

Documento Operacional

A documentação operacional pode incluir:

- Procedimentos de instalação e configuração de sistemas;
- Tratamento da informação tanto automática como manual;
- Backup;
- Agendamento de tarefas;
- Instruções para tratamento de erros;

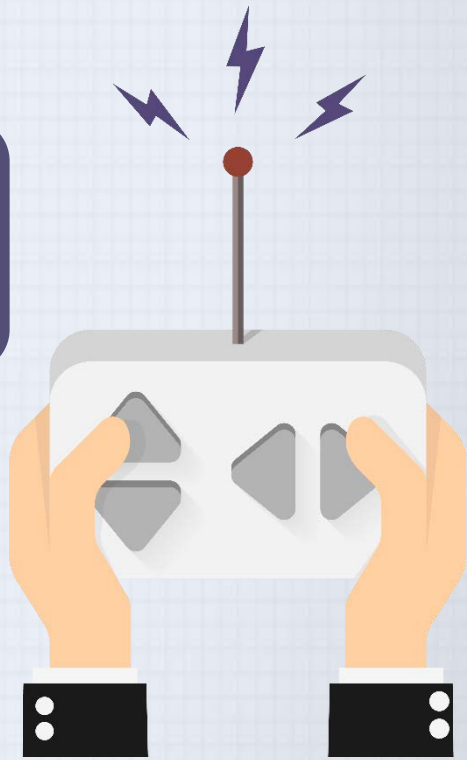


- Contatos para suporte e escalação, incluindo contatos de suporte externos, para o caso de eventos operacionais inesperados ou dificuldades técnicas;
- Instruções no manuseio de mídias, incluindo procedimentos para o descarte seguro;
- Procedimento para o reinício e recuperação em caso de falha do sistema;
- Trilhas de auditoria e informações de registros (logs) de sistemas e procedimentos de monitoramento.

Controles dos Fornecedores

1

- Referente aos requisitos de segurança que servem para mitigar todos aqueles riscos que estão associados ao acesso de fornecedores aos próprios ativos da organização.



2

- Estes devem ser estabelecidos e acordados com cada fornecedor, para que os mesmos tenham acesso, possam processar, armazenar e prover as informações dentro do sistema da organização.

Controles dos Fornecedores

3

Acordos com fornecedores e que devem incluir todos os requisitos para lidar com riscos associados à segurança da informação e serviços de comunicação, além é claro, dos riscos relativos ao setor ou da cadeia produtiva da empresa – sempre dentro do escopo de comunicação.

Implemente controles para que seja possível a organização monitorar regularmente, revisar e auditar as entregas dos fornecedores.

4

Controlar as mudanças nos serviços entregues por fornecedores.

Direitos de Propriedades Intelectuais

- Garantir a segurança da informação da organização.
- Para evitar violação de quaisquer obrigações legais, regulamentares ou contratuais relacionadas à segurança da informação, é necessário que todos os requisitos sejam explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização.

Direitos de Propriedades Intelectuais

- Manter conscientização das políticas para proteger os direitos de propriedade intelectual e notificar caso existe alguma intenção de tomar ações disciplinares contra pessoas que violarem tais políticas, por isso da importância em se manter provas e evidências da propriedade de licenças, discos-mestres, manuais etc.

- Conscientizar que não seja duplicado, convertidos para outro formato ou que sejam extraídos os registros comerciais de filme, áudio, imagens ou outros que não os permitidos pela lei de direito autoral. Devem-se conduzir verificações para que somente produtos de software autorizados e licenciados sejam instalados.

Proteção de Registros

Contábeis

De base de dados

De transações

De auditoria e procedimentos operacionais

- contra perda
- destruição
- falsificação
- acesso não autorizado
- e liberação não autorizada

- papel
- microficha
- meio magnético
- ótico

Proteção de Registros

Deve ser dada uma atenção especial em relação a **deterioração das mídias** usadas no armazenamento destes registros, por isso os procedimentos de armazenamento e manuseio devem ser implementados de acordo com as recomendações dos fabricantes. 987061042

Convém que sejam incluídos procedimentos para assegurar a capacidade de acesso aos dados durante o período de retenção, para proteger contra perdas ocasionadas pelas futuras mudanças na tecnologia.

Proteção de Registros

1. Emitir diretrizes gerais para retenção, armazenamento, tratamento e disposição de registros e informações

2. Elaborar uma programação para retenção, identificando os registros essenciais e o período recomendado para que cada um seja mantido

3. Manter um inventário das fontes de informações-chave.

Privacidade de Informações de Identificação Pessoal

É essencial a **criação** de uma política que deve ser comunicada a todas as pessoas envolvidas no processamento de informação de identificação pessoal.

ISO/IEC 29100

A conformidade com esta política e todas as regulamentações e legislação relevantes, relativas à proteção da privacidade das pessoas e da proteção da informação de identificação pessoal requer um controle e uma estrutura de gerenciamento apropriada.

Fornecer orientações aos gestores, usuários e provedores de serviços sobre as suas responsabilidades.

Conformidade com Análises

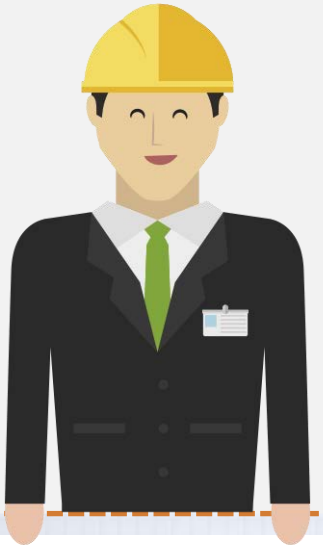
É papel dos gestores analisem criticamente, em intervalos regulares, a conformidade dos procedimentos e do processamento da informação.

- Convém que os gestores identifiquem as causas da não conformidade;
- Avaliem a necessidade de ações para atender à conformidade;
- Implementem ação corretiva apropriada e por fim;
- Analisem criticamente ação corretiva tomada, para verificar a sua eficácia e identificar quaisquer deficiências ou fragilidades.

Se for encontrada NÃO CONFORMIDADE:

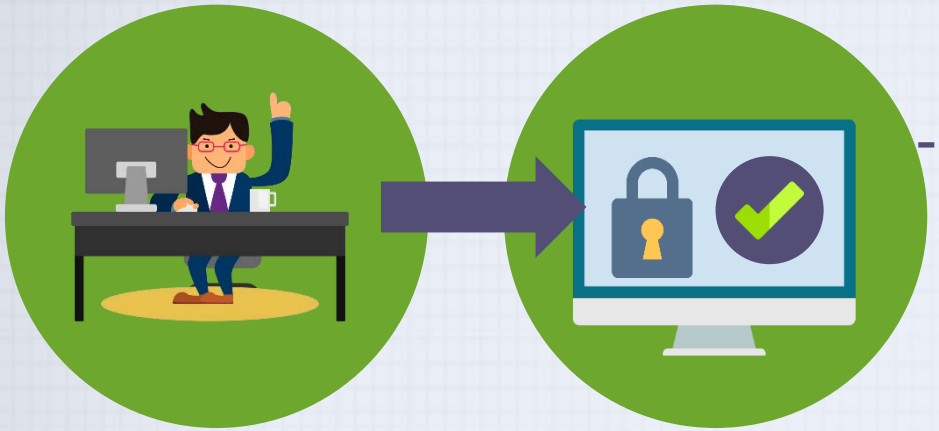
Conformidade com Análises

- Os sistemas de informação devem também ser analisados criticamente, a intervalos regulares.
- Contar com o apoio de uma ferramenta automática, que gera relatórios técnicos para a interpretação dos especialistas técnicos.
- Ocorrer também análises criticas de forma manual através de um engenheiro de sistemas experiente, por exemplo.



Análise crítica da CONFORMIDADE TÉCNICA

Parcerias e Terceirização



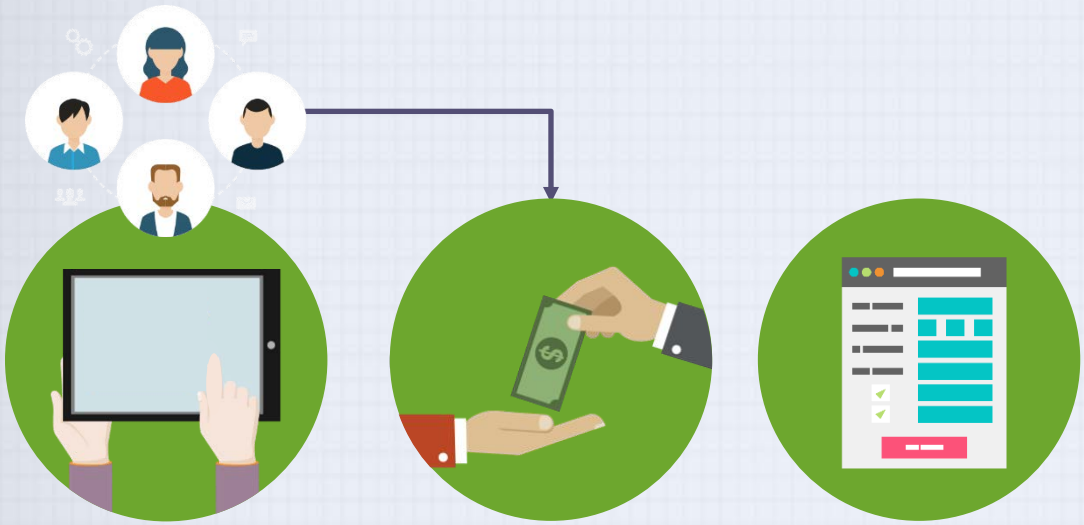
E como proceder com estas relações?

Uso de serviços de parceiros e de empresas terceirizadas.

Parcerias e Terceirização

- Proteção dos ativos do cliente, incluindo informações, software e hardware;
- Procedimentos para determinar modificações ou corrupção de ativo;
- Estrutura clara de comunicação;
- Controles para garantir dados e destruição de ativos ao final do contrato;
- Processos de autorização e de concessão de privilégios bem desenhados;
- Processo claro e bem detalhado;
- Garantias de continuidade, disponibilidade e acesso bem alinhados às prioridades dos clientes;
- Sistema de notificação e tratamento de incidentes e vulnerabilidades;
- Condições contratuais em relação à quebra de cláusulas ou até a suspensão do serviço;
- Conhecimento das medidas de controle de cada parceiro;
- Planos de contingência definidos em contrato;
- Possibilidades de renegociação em caso de não cumprimento de cláusulas.

Lidando com a Terceirização



Terceirização ou "outsourcing" | **Preços** | **Funcionalidades**

Lembre-se: uma organização que terceiriza suas informações sem medidas de controle ou precauções está colocando em xeque seus próprios níveis de segurança da informação.

Lidando com a Terceirização

Há três tipos de padrões que são utilizados em conjunto:

Normas técnicas e formais, como as emitidas pela ISO e ABNT.

Melhores práticas criadas por profissionais e empresas de TI, sem valor de certificação, porém úteis para criar padrões de excelência de serviço.

Normas técnicas ou instruções, geralmente emitidas por fabricantes e desenvolvedores.

Auditoria de Sistemas

Minimizar o impacto das atividades de auditoria nos sistemas operacionais.

Devem ser cuidadosamente planejados e acordados para minimizar interrupção dos processos do negócio.

- **O escopo dos testes técnicos da auditoria seja acordado e controlado, e que os testes de auditoria sejam limitados ao acesso somente para leitura de software e dado;**
- **Os outros acessos diferentes de apenas leitura sejam permitidos somente através de cópias isoladas dos arquivos do sistema;**
- **Os testes de auditoria não podem afetar a disponibilidade do sistema.**

Padronização e Normas ISO

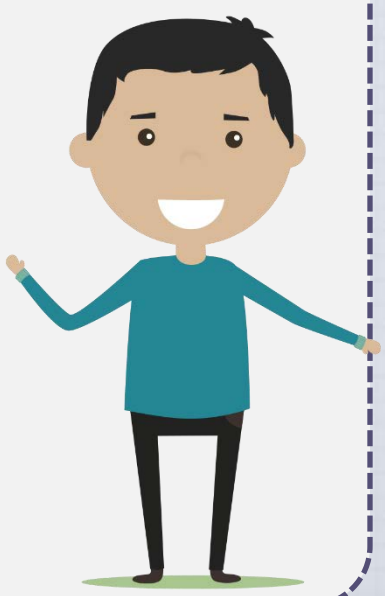
- **ISO 27001** – cria as bases para a gestão da segurança da informação sob o ponto de vista da melhoria contínua, como ocorre com a ISO 9001;
- **ISO 27002** – instruções e melhores práticas para implementação da segurança da informação e de controles diversos, criando padrões de compliance (conformidade);
- **ISO 27003** – foco total no uso do ciclo PDCA nos processos;
- **ISO 27004** – padrões de métricas e índices para auferir a eficiência de um sistema de segurança da informação;
- **ISO 27005** – foco no gerenciamento de riscos, dando detalhadamente os passos que devem ser tomados ao gerir os riscos;
- **ISO 27006** – guidelines para organizações e instituições que oferecem certificações e registro na área de segurança da informação.

Padronização e Normas ISO

- **ISO**/IEC 13335:2004 – modelos e técnicas para gestão da segurança em sistemas baseados na tecnologia da informação e comunicação;

- **ISO** 7498-2 – estabelece controles para a segurança em sistemas interconectados e sua troca de informações. Contudo, como a norma não é atualizada desde 1989, vários dos controles e mecanismos que foram sugeridos estão de certo modo defasados;

- **ISO**/IEC 20000:2005 – não necessariamente focado na TI, mas essencial para lidar com clientes, com os serviços que são entregues aos clientes. Essa norma estipula padrões para a gestão de serviços de TI com base na ITIL®.



Pronto para o próximo?

Curso Preparatório para Certificação
Em Gestão de Segurança da Informação Avançada – Baseada na ISO/IEC 27002:2013

Área de Aprendizagem

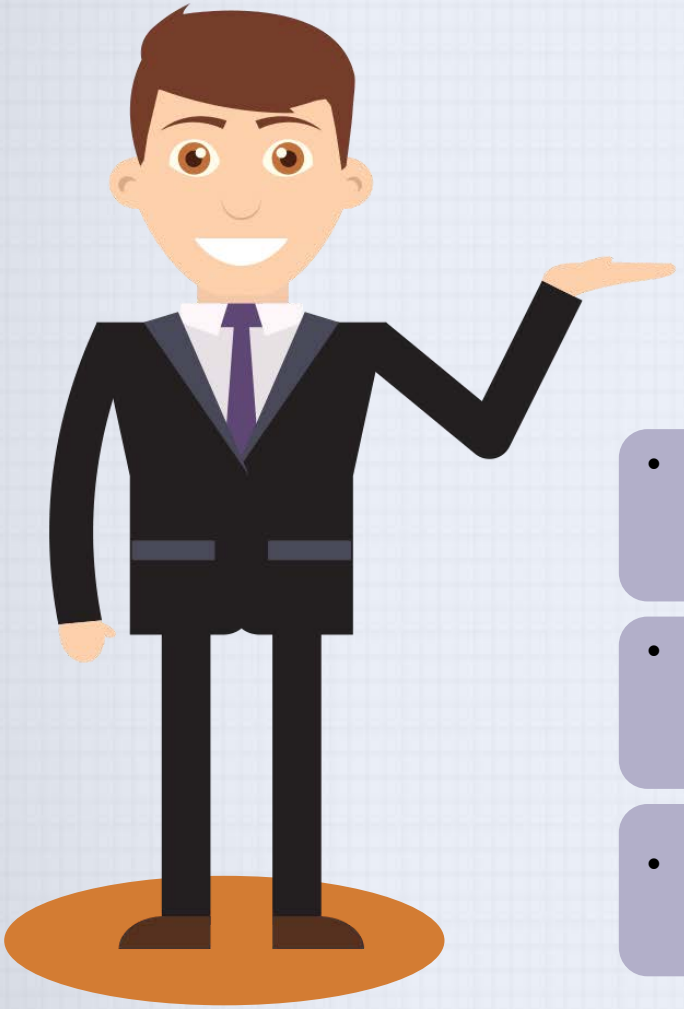
www.pmgacademy.com

Official Course

Módulo 3

Perspectivas de Segurança da Informação

Resumo



- Avaliação de risco;
- Seleção de controles e estratégias;
- Risco residual.

- Controlar os riscos, classificando os controles com base na Confidencialidade, Integridade e *Disponibilidade (CIA, Confidentiality, Integrity and Availability).*
- Escolher controles baseados nos estágios de ciclos de incidentes e escolher guias relevantes para aplicação de controles.
- Distinguir as estratégias de risco, produzir estudos de caso para controles e produzir relatórios de análises de risco.

Como Gerenciar a Segurança da Informação

A política ou normas de conduta.

Os processos ou tudo o que precisa ocorrer para atender aos objetivos de segurança.

Os procedimentos, com detalhes de quem deve fazer o que e quando.

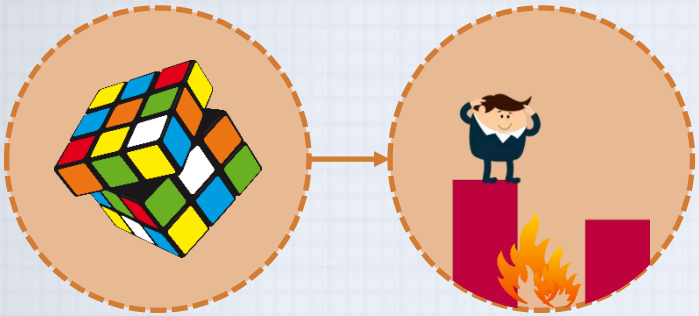
Instruções claras de trabalho, se possível descritas em passos.

Como Gerenciar a Segurança da Informação

Entre os fatores que exigem adaptações, podemos destacar:

- Mudanças nas demandas de negócios;
- Fusões e aquisições;
- Mudanças nas funções e nas principais tarefas;
- Realocação, mudanças de sede e expansões físicas;
- Mudanças no hardware e software utilizados;
- Mudanças ambientais;
- Mudanças legais;
- Novas ameaças;
- Equipamentos obsoletos e antigos;
- Introdução de novas tecnologias.

Gerenciamento de Riscos



O gerenciamento de risco assume exatamente esta tarefa, e este processo ajudará a buscar e tratar da melhor maneiras os riscos.

Ao invés de ficarmos na tentativa e erro

Quais são os riscos – se falhar em proteger estas informações?

Quais são as informações – ou ativos – que precisam ser protegidos?

Quais são as opções para lidar com esses riscos?

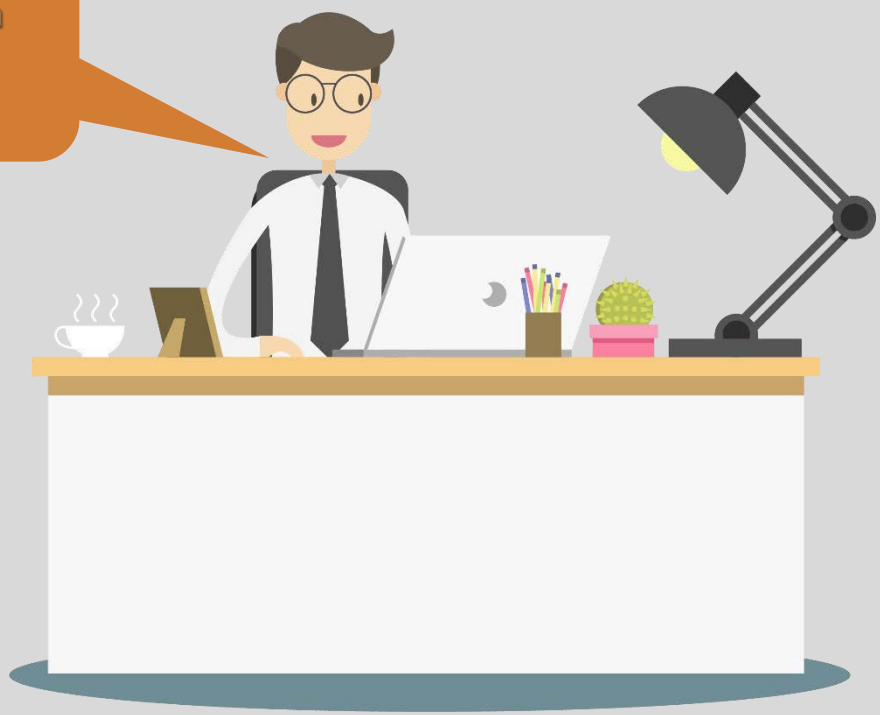
Quais são as prioridades para lidar com esses riscos?

Por que é preciso proteger estas informações?

Gerenciamento de Riscos

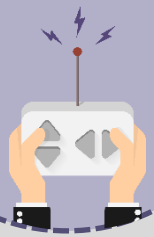
Gerenciamento riscos é uma das principais responsabilidades dos gerentes dentro da organização.

Dois processos formais devem sempre ser considerados:



Identificação e Avaliação de Riscos

Controle de Risco



Sun Tzu, a Arte da Guerra

Sun Tzu - A Arte da Guerra

"Se você conhece o inimigo e se conhece, não precisa temer o resultado de cem batalhas."

"Se você se conhece, mas não o inimigo, para cada vitória que você ganha, também sofrerá uma derrota."

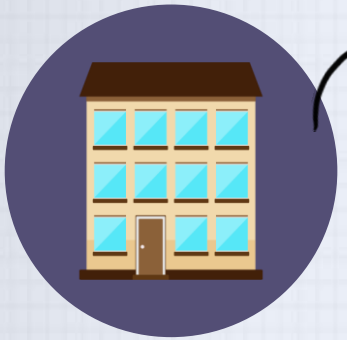
"Se você não conhece nem o inimigo nem você mesmo, você sucumbirá em cada batalha."

- Identificar, examinar e compreender como as informações são processadas, armazenadas e transmitidas.
- Conhecer o inimigo significa identificar, examinar e compreender as ameaças que enfrentam os ativos de informação da organização.
- Com esse conhecimento, podemos iniciar um programa de gerenciamento de risco em profundidade.
- Os gerentes devem estar preparados para identificar plenamente as ameaças que representam riscos para a organização.
- As salvaguardas e os controles que são planejados e implementados não devem ser considerados como dispositivos que são instalados e depois esquecidos.
- O gerenciamento de riscos é o processo que avalia os riscos para as informações de uma organização e determina como esses riscos podem ser controlados ou mitigados.

Responsabilidade no Gerenciamento de Riscos

- Identificar ameaças aos ativos catalogados;
- Identificar ativos vulneráveis, vinculando as ameaças específicas aos ativos específicos;
- Avaliar riscos, incluindo:
- Determinação da probabilidade de ataques aos sistemas vulneráveis por ameaças específicas;
- Avaliação do risco relativo dos ativos de informação, de modo que as atividades de gerenciamento e controle de riscos sejam priorizadas;
- Calcular os riscos pelos quais os ativos estão expostos na sua situação atual;
- Revisar controles de vulnerabilidades identificadas e informar que se deve controlar os riscos enfrentados pelos ativos;
- Documentar os resultados da identificação e avaliação dos riscos.

Tratando de Situações que Ainda não Ocorreram



A maioria das pequenas empresas não possui sequer um backup do sistema

Porque muitas vezes não entende os riscos de perder os seus dados.

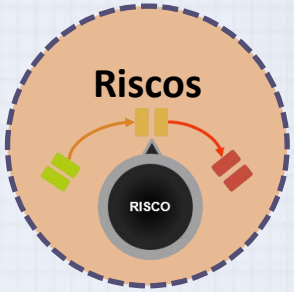
É preciso o auxílio de algumas ferramentas que ajudem a medir possíveis danos.

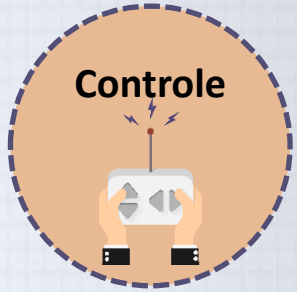
Conte com a ajuda de profissionais com perfil de especialista ou um analista em Segurança da Informação.

- Ajudar as pessoas a verem o problema.
- Ajudar a mensurar – a medir- o valor do bem, e o tamanho da perda.

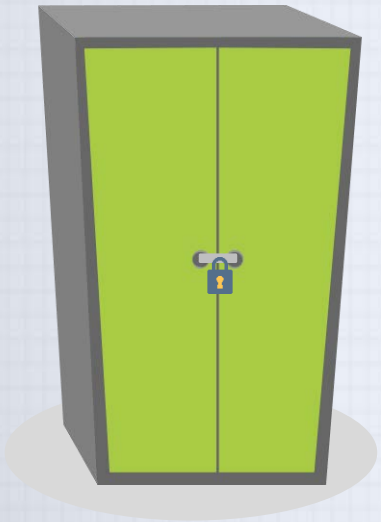
Quanto mais envolvidos estiverem os departamentos da empresa, mais fácil vai ser conseguir implementar os controles, análise e avaliação de riscos.

Base para a Segurança da Informação



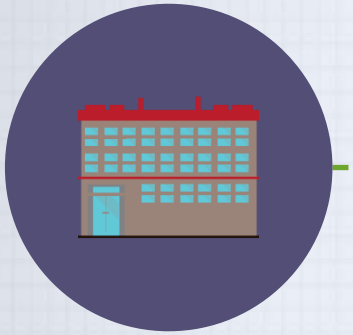


Base da segurança da informação:



- Definir **QUEM** são os proprietários dos ativos;
- Definir também **QUAIS** são estes ativos de informações.
- Discutir com os donos das informações quais as possíveis ameaças;
- É fundamental que seja determinado quais as possíveis fontes de ameaça, os agentes de ameaça e quais são as vulnerabilidades.
- Veja com o dono da empresa quais os riscos aceitáveis ou o quanto ele quer realmente ficar seguro, e encontre um meio de lidar com os riscos que foram considerados inaceitáveis.

Requisitos de Segurança da Informação

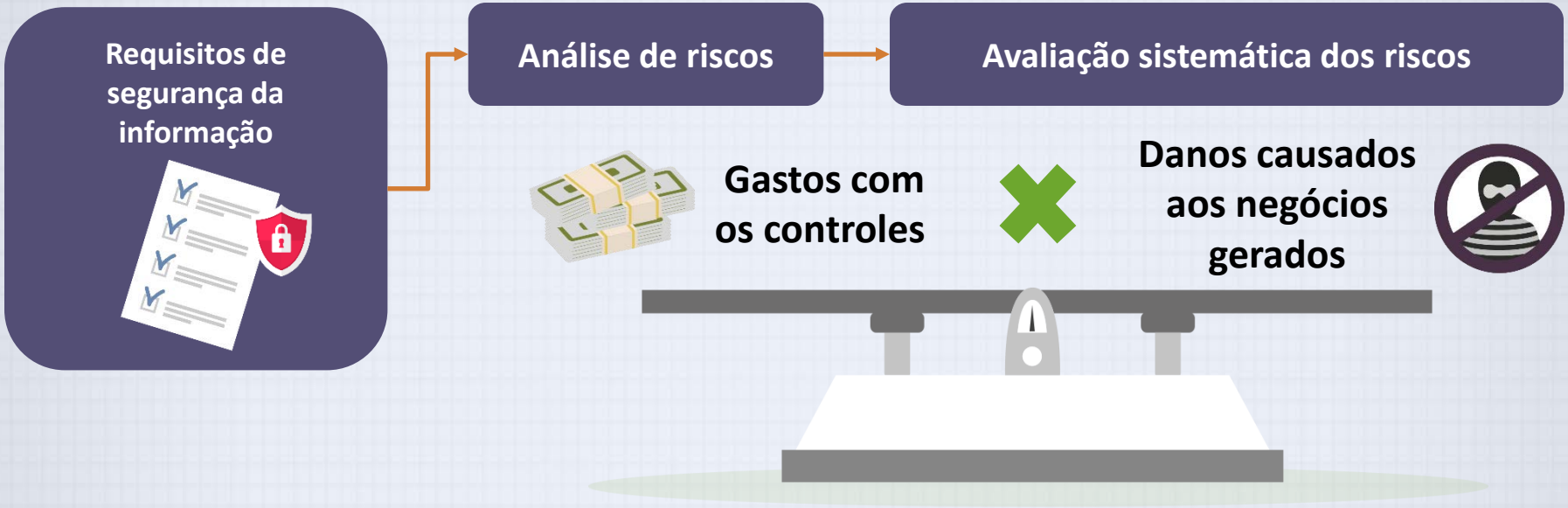


A partir da análise de risco ou da avaliação de riscos para a organização, levando-se em consideração os objetivos e as estratégias globais dos negócios da empresa.

A legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço têm que atender, além do seu ambiente sociocultural.

Um conjunto particular de princípios, objetivos e os requisitos do negócio para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

Analisando e Avaliando os Riscos de Segurança da Informação



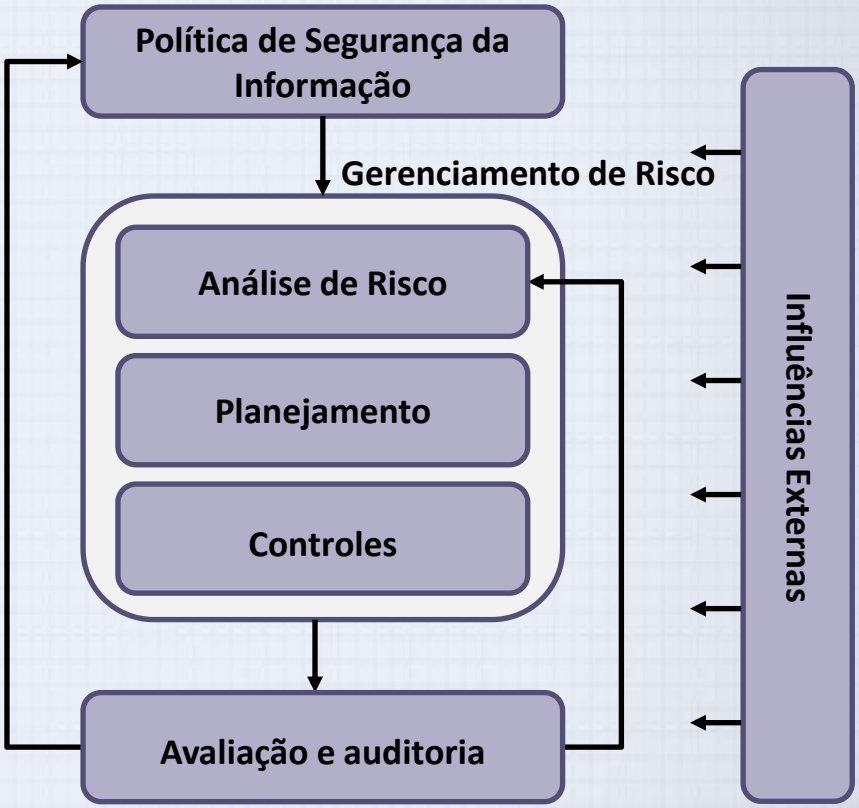
- Os resultados das avaliações de riscos ajudarão a direcionar, determinar as ações gerenciais apropriadas, as prioridades para o gerenciamento dos riscos da segurança da informação, e a implementação dos controles selecionados para a proteção contra eles.

- Convém que a análise e avaliação de riscos sejam repetidas periodicamente para contemplar quaisquer mudanças que possam influenciar os resultados.

Ciclo do Gerenciamento da Segurança da Informação

ISO 9000

ISO/IEC 27001



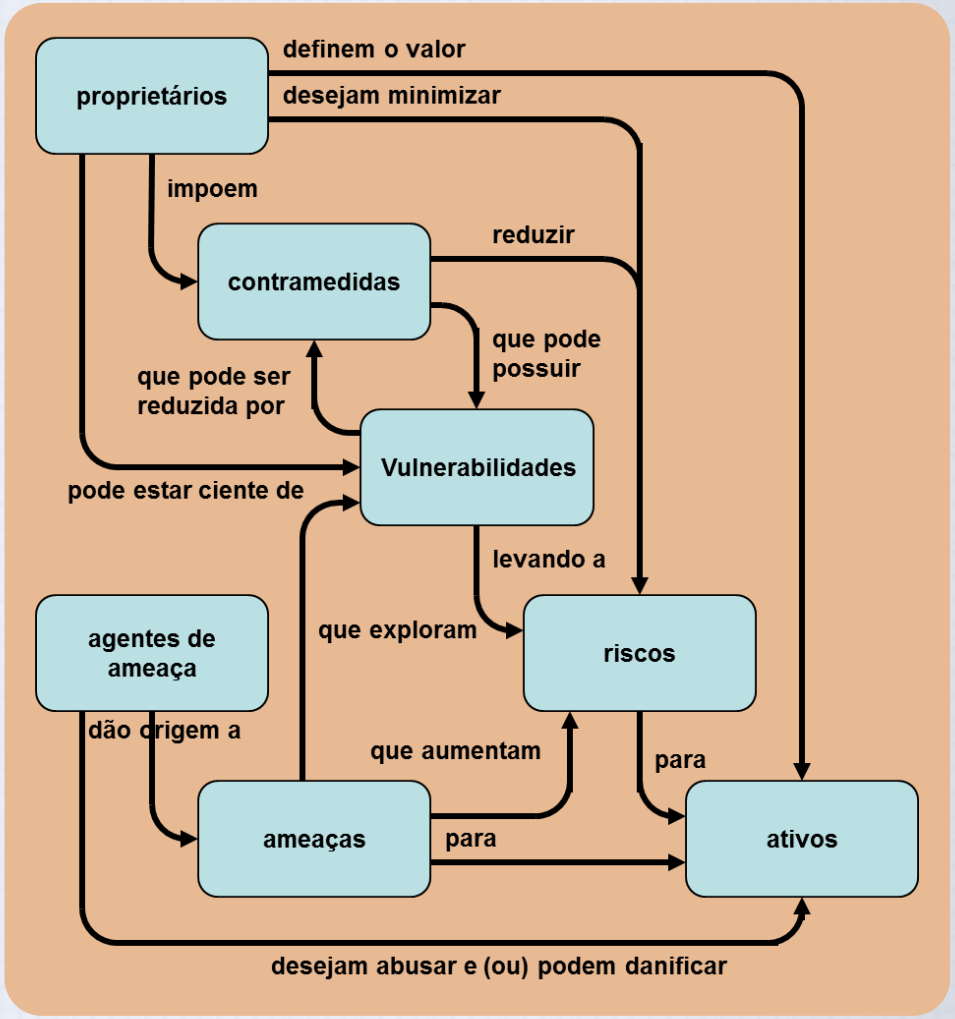
Esse ciclo não se aplica apenas a empresas maduras e grandes conglomerados. Pequenas empresas, devem considerar os riscos dessa área em seus planos de negócios – para posteriormente implementar suas políticas com sucesso.

Fluxo do Tratamento dos Riscos

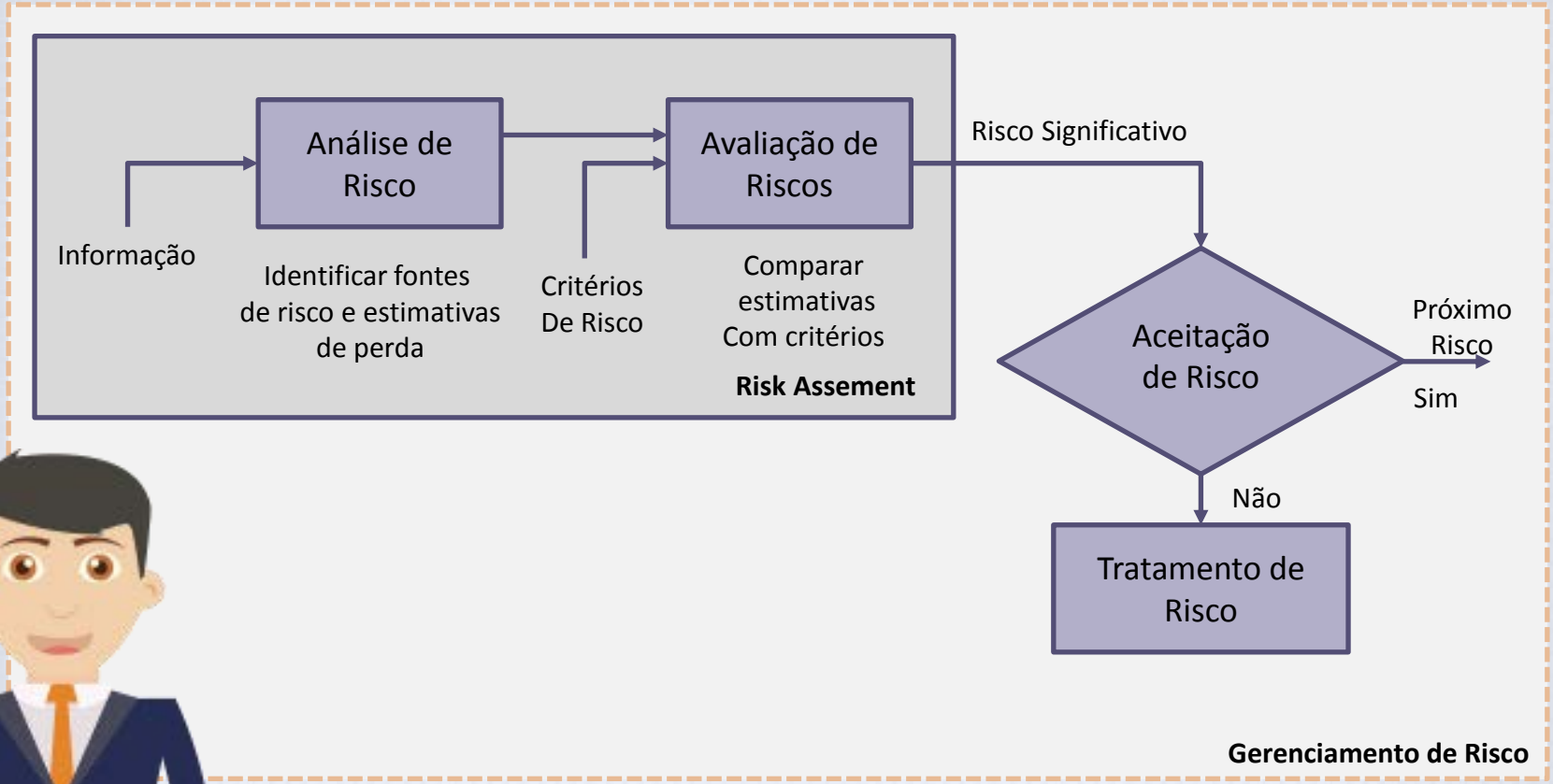
Estes proprietários reconhecem e estão cientes que os seus ativos têm vulnerabilidades, por isso, para reduzi-las, é necessário impor contramedidas.

Essas contramedidas podem gerar novas vulnerabilidades, levando então, a novos riscos para os ativos.

O objetivo principal é reduzir os riscos.



Gerenciamento de Risco de Acordo com ISO / IEC 27001/2



A ISO/IEC 27001 refere-se explicitamente e alinha-se com a norma ISO/IEC 31000 – Gerenciamento de riscos – Princípios e orientações.

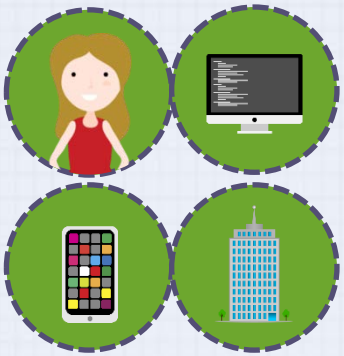
Passo 1: Determinar o Que Deve Ser Protegido

- Passo 1: Determinar o que deve ser protegido;
- Passo 2: Determinar quem são os proprietários desses ativos;
- Passo 3: Conversar com estes proprietários sobre as ameaças aos ativos;
- Passo 4: Conhecendo o inimigo;
- Passo 5: Obter opiniões de especialistas;
- Passo 6: Definir o impacto;
- Passo 7: Realizar uma avaliação;
- Passo 8: Criar uma fórmula para calcular o risco;
- Passo 9: Definir o apetite ao risco;
- Passo 10: Mitigar o risco inaceitável;
- Passo 11: Implementar controles;
- Passo 12: Reavaliação;
- Passo 13: Entender e mitigar os novos riscos vindos dos próprios controles;
- Passo 14: Aceitar os riscos residuais e refazer o processo.

Passo 1: Determinar o Que Deve Ser Protegido

De que modo?

Análise de impacto nos negócios, para observar quais os processos podem causar maiores problemas em caso de perda, dano ou divulgação da informação sem autorização.



Como proceder?

Ter um inventário do que deve ser protegido; e criar uma lista de possibilidades – de informações que podem ser protegidas eventualmente, uma espécie de margem de segurança.

Determinar o que Deve Ser Protegido.

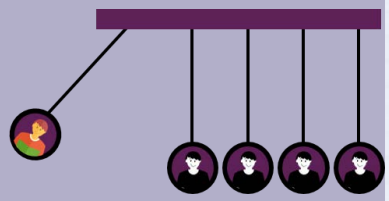
1

- Saber o que deve ser protegido, entender qual o ativo da empresa.
- Determinar quais ativos serão avaliados durante os próximos passos.

Passo 2: Determinar Quem São os Proprietários Desses Ativos

De que modo?

Durante a análise de impacto, porque é quando se descobre os processos e os pontos de risco.



Como proceder?

- Informar ao responsável, o proprietário ou aos gerentes de áreas, as medidas necessárias.
- Determinar os proprietários de ativos compartilhados.
- Informar que o proprietário será o gerente responsável – delegado - pela manutenção desses ativos.

2

Determinar Quem São os Proprietários Desses Ativos.

- Eles podem dizer e entender o real valor da informação referente ao ativo em questão.
- Somente os proprietários podem discutir claramente o valor dos ativos.

Passo 3: Discuta com os Proprietários as Ameaças aos Ativos

De que modo?

- Criando uma lista das ameaças mais importantes.

Como proceder?

- A lista deve ser tão completa quanto possível. Não filtre ameaças neste momento.
- Busque compilar uma lista de ameaças inerentes, não as ameaças para as quais existem riscos residuais neste momento.

3

Discuta com os Proprietários as Ameaças aos Ativos.

- Determinar quais ameaças são aplicáveis aos ativos dentro do escopo.
- Verificar quais ameaças serão tratadas agora e quais serão vistas depois.

Passo 4: Decidir Quais São os Agentes de Ameaça

De que modo?

- Descobrir quem pode atacar a empresa ou quais são os pontos internos com fraquezas – inclusive, de pessoal.
- Discutir quem possa estar interessado em atacar a sua organização e os meios que esses adversários têm à sua disposição.

Como proceder?

- Identificar um leque maior de inimigos "tradicionais".

funcionários	criminosos	hackers
fornecedores	clientes	concorrentes

4

Decidir Quais São os Agentes de Ameaça.

- O que pode ocasionar falhas, gerar danos.
- Melhores probabilidades de determinar vulnerabilidades.

Passo 5: Obter Opiniões de Especialistas

De que modo?

- O especialista pode ser convidado para um *Workshop* ou realizar entrevistas sobre os aspectos de segurança da informação relevantes aos ativos em questão.

Como proceder?

- Os dados obtidos precisam ser qualificados em termos de **alta, média e baixa vulnerabilidade**. Tente ser exaustivo.

5

Obter Opiniões de Especialistas.

- Obter opiniões de especialistas durante *Workshops* de avaliação de risco, a fim de coletar informações detalhadas para tomada de decisão.

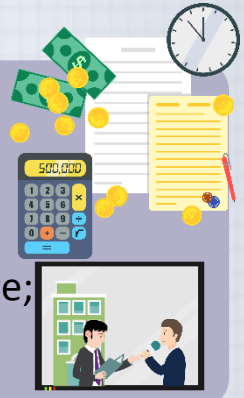
Passo 6: Definir o Impacto

De que modo?

- Discutir com especialistas qual será o impacto máximo quando ocorrer uma ameaça.

Como proceder?

- Perdas monetárias;
- Problemas legais;
- Perda de negócios;
- Vantagens para um concorrente;
- Perda de imagem, etc.



Definir o Impacto.

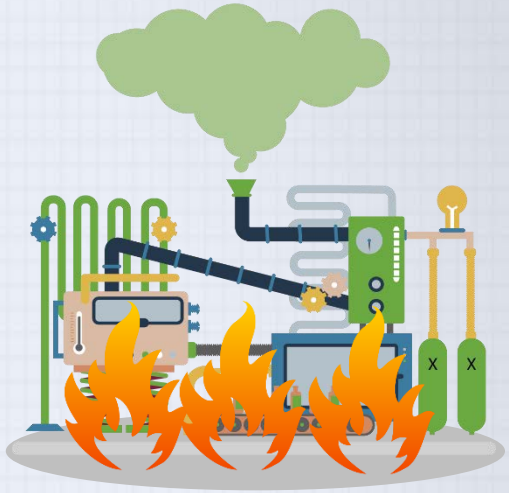
6

- Saber qual o impacto para todas as ameaças, o que pode dar errado e o impacto para a empresa.

Passo 7: Realizar uma Avaliação

Vulnerabilidade é o quanto alguma coisa é frágil ou passível de ataque.

Probabilidade é o quanto alguma coisa pode ser atacada.



Realizar uma Avaliação.

7

Realizar a comparação dos riscos, conforme o resultado da análise de riscos. É o momento de aceitar o não a dimensão ou magnitude de um determinado risco.

Passo 7: Realizar uma Avaliação

De que modo?

- Determinando a probabilidade, a vulnerabilidade e os impactos.

Como proceder?

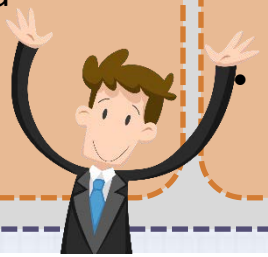
- Antes de se fazer uma avaliação de risco, tente obter o consenso em classes de probabilidade, vulnerabilidade e impactos de todos os envolvidos.

Probabilidade:

- **Alta:** isso pode acontecer qualquer dia;
- **Média:** poderia acontecer anualmente;
- **Baixa:** nunca vai acontecer.

Vulnerabilidade:

- **Alta:** quando acontece há um impacto total;
- **Baixa:** quando isso acontecer, haverá impacto menor.



Impacto:

- **Alto:** poderia levar à falência;
- Médio: impactos no lucro;
- **Baixo:** nenhum impacto.

Passo 8: Criar uma Fórmula para Calcular o Risco

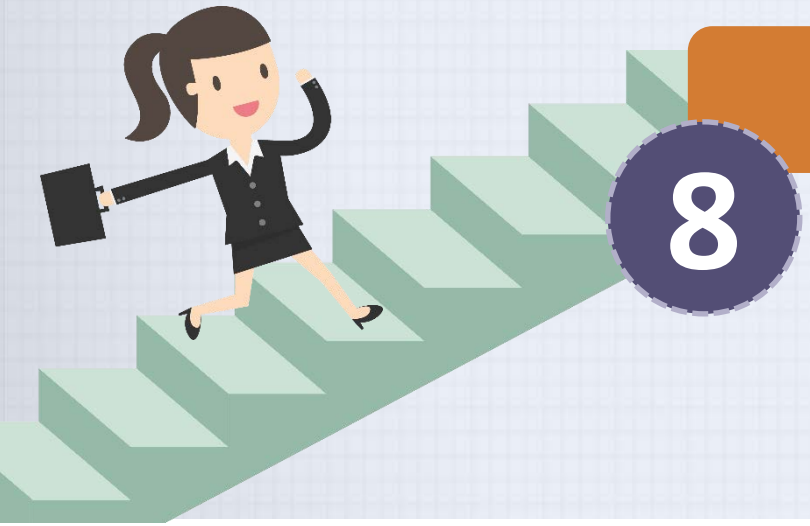
De que modo?

Usando classes de risco, associadas a valores para alta, média e baixa:

1 para Baixa	BBM de Baixa Probabilidade, Baixa Vulnerabilidade, Médio Impacto, ou multiplique o BBM = 1 * 1 * 3 = 3, ou ainda, use alguma outra fórmula.
2 para Média	
3 para Alta	

Como proceder?

- Criar alguma medida que avalie probabilidade, vulnerabilidade e impacto;
- Haver uma distinção clara entre as opções de Baixa, Média e Alta, já que um AMB e MBA de probabilidade...



8

Criar uma Fórmula para Calcular o Risco
Opiniões de Especialistas.

- Criar uma fórmula para calcular o risco, com base em todas as informações, usando um meio para quantificar.

Passo 9: Definir o Apetite ao Risco

De que modo?

- Pode ser em uma escala geral ou por riscos separados.

Como proceder?

- Buscar outras visões além dos limites da empresa; conhecer o que clientes, fornecedores e parceiros da empresa acreditam como sendo limite, ou consideram como aceitável.
- Buscar também o que as leis e regulamentos vigentes acham ser o limite aceitável.

Definir o Apetite ao Risco.

Aceita assumir um risco, pensando em seu beneficio.

9

- Definir o limite, o nível do risco. Determinar acima de qual nível o risco é inaceitável.

Passo 10: Mitigar o Risco Inaceitável

De que modo?

Definir se um risco pode ser aceito, se deve ser evitado, ou se deve ser mitigado – ou transferido.

Como proceder?

Transferência de risco - é o uso de um seguro; você perde, mas não tudo.

10

Mitigar o Risco Inaceitável.

Abrandar um risco inaceitável ou ainda, buscar solucionar o problema.

- Selecionar quais os riscos que devem ser atenuados, receber um controle que suavize o risco geral.

Passo 11: Implementar Controles

De que modo?

Usando um conjunto de medidas de boas práticas, neste caso, a **Norma ISO/IEC 27002:2013.**

Como proceder?

- Usando o conhecimento adquirido.
- **Boas referências:** as publicações PD3005 do Instituto British Standards; publicações da ISACA; a metodologia de avaliação de risco Octave da Universidade Carnegie Mellon; e do Manual de Linha de Base de Proteção da alemã BSI.

- Prevenir os riscos acordados anteriormente, através dos controles.

Passo 12: Reavaliação

De que modo?

Usar um conjunto de linha de base (*baseline*) para as melhores práticas, como da ISO/IEC 27002; e selecionar os controles a partir dele a fim de atenuar um determinado risco.

Diretrizes:

É necessário ter conhecimentos legais, processuais, dos aspectos técnicos e físicos. Certifique-se que o ponto de vista dos especialistas sobre todos estes aspectos está disponível.

Reavaliação. → **É importante manter-se atualizado.**

12

- Para aqueles riscos que não podem ser aceitos, os controles precisam ser selecionados e implementados para diminuir a probabilidade, vulnerabilidade e (ou) impacto.

Passo 13: Entender e Minimizar os Novos Riscos dos Próprios Controles

De que modo?

- Análise da situação atual e conversa com especialistas para verificação se as medidas tomadas valem a pena.
- Discussão com os especialistas sobre as implicações dos controles selecionados.
- Encontre estratégias de mitigação quando novos riscos são encontrados.

Como proceder?

Ponto com leitura biométrica.

chaves em todos os armários

Catraca com acesso via cartão.

Chaves criptográficas ou chaves eletrônicas com senhas e certificados.

Entender e Minimizar os Novos Riscos dos Próprios Controles.

13

- Determinar se os controles que são selecionados para atenuar os riscos inaceitáveis introduzem novos riscos.

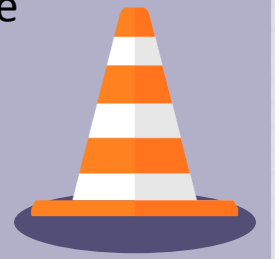
Passo 14: Aceitar os Riscos Residuais e Refazer o Processo

De que modo?

- Criar um documento que mostre quais os riscos tratados e, se possível, criar outro que demonstre quais os riscos que ainda serão cuidados.
- ISO/IEC 27001, ISO 9001 (qualidade) ou ISO/IEC 20000 (gerenciamento de serviços de TI).

Como proceder?

- Criar um processo de gerenciamento de incidentes e gerenciamento de mudanças.



14

Aceitar os Riscos Residuais e Refazer o Processo

- Aceitar os riscos residuais e refazer o processo. Além de aceitar formalmente os riscos residuais, deve-se incorporar esse processo.

Outras Normas

- **ISF** - International Security Forum;
- **SABSA** – o Sherwood Applied Business Security Architecture;
- **COBIT** – Conjunto de melhores práticas em tecnologia da informação compiladas pelo Instituto de Governança em TI e pela ISACA.

Outras normas de padronização e segurança da informação:

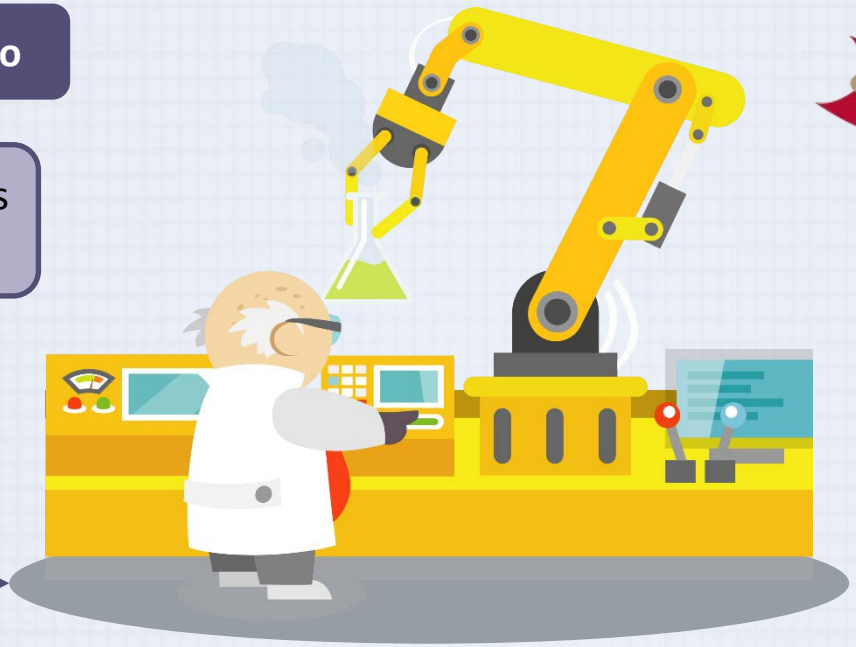
- PCI/DSS – os padrões de segurança da indústria de pagamentos em cartões. O DSS – Data Security Standard;
- Certificação em Gestão da Segurança da Informação – a certificação na área é baseada na ISO/IEC 27001.

Operações de Serviços

Operação de Serviço

É responsável pelas atividades diárias.

“Fábrica" da TI

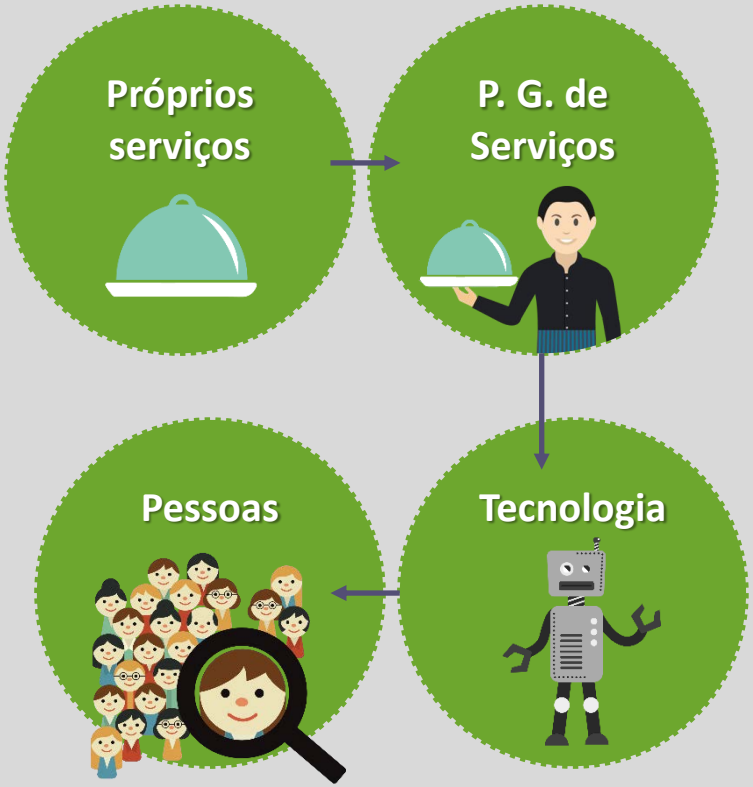


Responsável pelo gerenciamento contínuo da tecnologia utilizada para fornecer e prestar serviços de suporte.

Coordenar e realizar as atividades e processos necessários, para entregar e gerenciar serviços, em níveis acordados para usuários e clientes corporativos.

Operações de Serviços

Escopo da Operação de Serviço



- Gerenciamento de Eventos;
- Cumprimento de Requisição de Serviços;
- Gerenciamento de Incidentes;
- Gerenciamento de Problemas;
- Gerenciamento de Acesso.

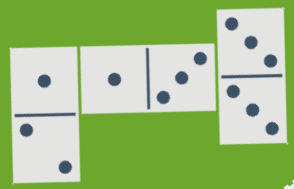
- Central de Serviços;
- Gerenciamento de aplicativos;
- Gerenciamento Técnico;
- Operações de TI.

Processos Importantes

Gerenciamento de Incidentes

Lida com os incidentes e conduz, através de tarefas, responsáveis, escalonamento e procedimentos, a sua resolução. Trata do arquivamento das informações e cria um histórico dos “erros” ou incidentes, que serve como apoio à futuras ações.

Gerenciamento de Continuidade



Busca garantir que toda a empresa tenha noção de suas responsabilidades em momentos de crise, diante de um incidente grave, desastres, catástrofes etc. Visa proteger a empresa para que não perca seus negócios e ajuda a tomar decisões nestes momentos difíceis.

Gerenciamento de Mudanças

Mantém os procedimentos de mudanças, decisões, como os riscos podem ser minimizados e como controlar os efeitos de algumas mudanças.

Gerenciamento de Mudanças

- Identifique e registre as mudanças significativas;
- Planeje e teste as mudanças;
- Avalie os impactos potenciais, incluindo impactos de segurança da informação;
- Execute o procedimento formal de aprovação das mudanças propostas;
- Verifique se os requisitos de segurança da informação foram atendidos;
- Comunique os detalhes das mudanças para todas as pessoas relevantes;
- Execute os procedimentos de recuperação;
- Provisione um processo emergencial de mudança para permitir uma implementação rápida e controlada de mudanças, necessárias para resolver um incidente.

Gerenciamento de Mudanças

Para garantir que haja um controle satisfatório de todas as mudanças é necessário que seja estabelecido procedimentos e responsabilidades.

Quando as mudanças forem realizadas, é conveniente manter um registro de auditoria contendo todas as informações relevantes.

Gerenciamento de Capacidade

Os requisitos de capacidade devem ser identificados levando-se em conta a criticidade do negócio.

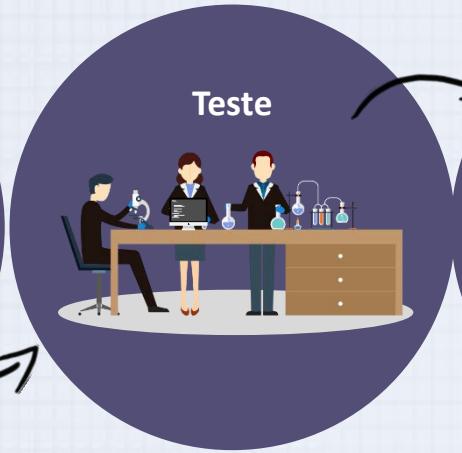
É recomendável que os controles de detecção sejam implantados para identificar problemas em tempo hábil.

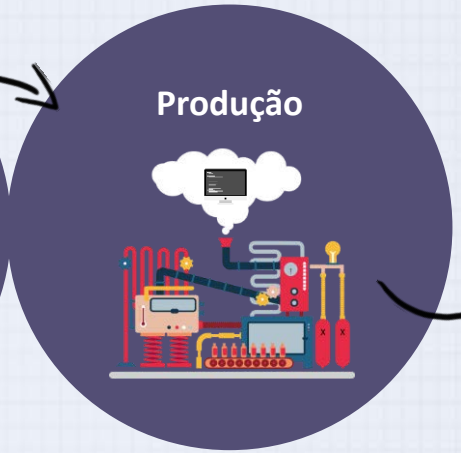
É conveniente que projeções de capacidade sejam levadas em consideração, principalmente para aqueles recursos que possuem um ciclo de renovação longo ou com custo alto. Além disso, é de responsabilidade dos gestores fazer o monitoramento da utilização dos recursos-chave dos sistemas.

Gerenciamento de Capacidade

- **Exclusão de dados obsoletos (espaço em disco);**
- **Desativação de aplicações, sistemas, bases de dados ou ambientes;**
- **Otimização da programação e dos processos em lote;**
- **Otimização da lógica de aplicação ou das consultas à base de dados;**
- **Negação ou restrição da largura da banda para serviços que demandam muitos recursos, se estes não são críticos ao negócio (por exemplo *streaming* de vídeo).**

Separação do Ambiente





Deve ser identificado um **NÍVEL** de separação dos ambientes de produção, testes e desenvolvimento necessário para prevenir problemas operacionais.

Software em desenvolvimento → **Software em produção**

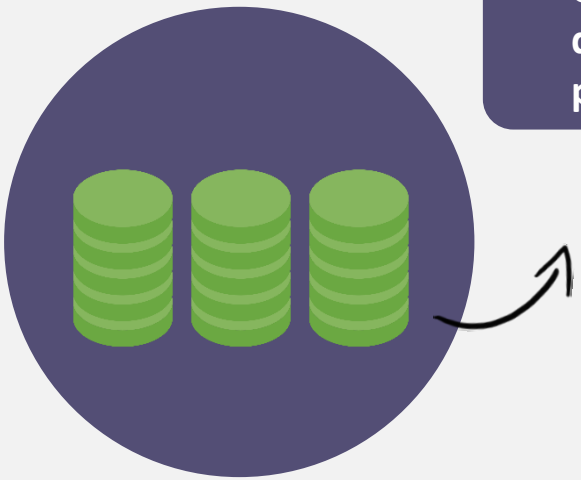
- Executados em diferentes sistemas ou processadores e em diferentes domínios ou diretórios;
- Que as mudanças nas aplicações e nos sistemas operacionais sejam testadas em um ambiente de teste ou projeto piloto, antes de serem aplicadas aos sistemas operacionais;
- Que estes testes não sejam realizados nos sistemas operacionais, exceto em circunstâncias excepcionais.

Ajudará a definir e documentar as regras para a transferência de software do ambiente de desenvolvimento para o de produção.

Separação do Ambiente

É importante deixar inacessível:

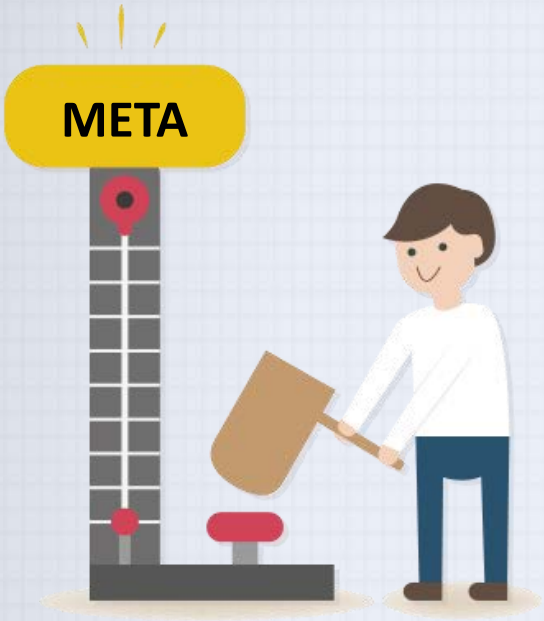
Compiladores.	Ferramentas de desenvolvimento.	Usuários tenham diferentes perfis para sistemas em testes e em produção.
Editores.	Utilitários de sistemas nos sistemas operacionais.	Menus com mensagens apropriadas de identificação para reduzir o risco de erro.



- **Os dados sensíveis não devem ser copiados para os ambientes de testes, a menos que controles equivalentes sejam fornecidos para o sistema de teste.**

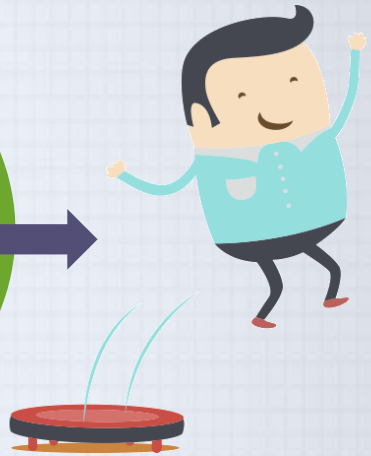
A separação dos ambientes de desenvolvimento, teste e produção é, portanto, desejável para reduzir o risco de modificações acidentais ou acessos não autorizados aos sistemas operacionais e aos dados do negócio.

Gerenciamento de Incidentes



Gerenciamento de Segurança da Informação

Gerenciamento de Incidentes

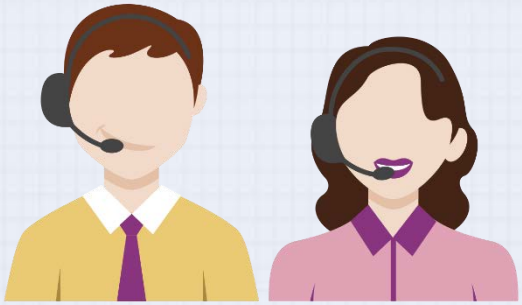


Central de Serviços (Help Desk ou atualmente Service Desk).

Visa minimizar as interrupções para o cliente e não necessariamente a resolução de problemas, pois estas atividades fazem parte de outro processo, o de gerenciamento de problemas.

Categorização de incidentes:

Administra, monitora e gerencia os incidentes e as ocorrências. Todos os incidentes são registrados, monitorados e atendidos imediatamente.



Categoria de Incidentes de Segurança

Quebra de confidencialidade:

- Acesso não autorizado a informações;
- Perda de dados;
- Perda ou roubo de laptop ou mídias;
- Tentativas de acesso em perfis mais altos de autorização;
- Tentativas internas ou externas de hacking.

Quebra de integridade:

- Perdas de dados, parcial ou total, em transações;
- Vírus e cavalos-de-troia;
- Falhas em trilhas de discos, HD e erros de memória;
- Registros faltantes ou corrompidos.

Quebra de disponibilidade:

- Interrupção do serviço por tempo inaceitável;
- Vírus e cavalos-de-troia;
- Roubo de laptops, componentes e dispositivos de armazenamento.

Relatórios

Os relatórios são gerados com a finalidade de apresentar certas conclusões e as provas do seu desempenho para os clientes.

- Relatórios sobre planos e estratégias;
- Relatórios de conformidade com o SLA, incluindo (KPIs);
- Relatórios sobre o funcionamento dos controles;
- Relatórios operacionais;
- Status do planejamento, com medidas até então implementadas, treinamentos e revisões realizadas, riscos analisados;
- *Overview* de incidentes registrados e reação aos mesmos;
- Resultados de auditorias e revisões;
- Perigos, vulnerabilidades, ameaças e tendências;

Registro de Eventos

Todos os registros de eventos - log – que forem produzidos devem ser mantidos e analisados criticamente, em intervalos regulares, incluindo as exceções, falhas e eventos de segurança da informação.

- **Identificação dos usuários;**
- **As atividades do sistema;**
- **Datas;**
- **Horários;**
- **Detalhes de eventos-chave.**

- Hora de (login) e (logoff);
- Identificação do dispositivo ou sua localização;
- Tentativas de acesso ao sistema;
- Tentativas de acesso a outros recursos e dados;
- Alterações na configuração do sistema;
- Uso de privilégios;
- Uso de aplicações e utilitários do sistema;
- Arquivos acessados e o tipo de acesso;
- Endereços e protocolos de rede;
- Alarmes provocados pelo sistema de controle de acesso; Alarmes dos sistemas de antivírus e ...

Registro de Eventos

- **Essas pessoas, que não necessariamente são administradores, mas que possuem uma conta de usuário com muitos privilégios, podem ser capazes de manipular os logs.**

- **Um sistema de detecção de intrusos (IDS), gerenciado fora do controle dos administradores de rede e de sistemas, pode ser utilizado para monitorar a conformidade das atividades dos administradores dos sistemas e de rede.**

É importante ajustar todos os relógios dos servidores, para garantir que não haja discrepância nos horários de um registro no log.

Impactos de Único Incidente

Note que a emissão de relatório dos incidentes de segurança nem sempre é fornecida pelos usuários ou colaboradores da TI, mas também através do gerenciamento, com base nos alarmes ou relatórios de dados de auditoria dos sistemas.

- **Lidando com incidentes**
- **Implicações legais**
- **Estimativa de danos**
- **Antecipação de danos**
- **Sigilo**

É **inicialmente** uma violação de **disponibilidade.**

Existem potenciais quebras de **confidencialidade** e **integridade.**

Controles nos Estágios do Ciclo de Vida do Incidente

Controles nos Estágios do Ciclo de Vida do Incidente

- **Categorização** – a classificação dos incidentes não pode apenas descrever a natureza do incidente em si, mas deve possuir valor de comunicação, ou seja, advertir usuários a respeito da possibilidade e de como agir.
- **Controle** – os incidentes ocorrerão, a despeito de qualquer preparação. Às vezes, no entanto, um incidente pode não ser tão visível, por isso eles precisam ser processados de maneira ordenada.
- **Registro** – todo incidente precisa ser registrado e catalogado devidamente. Entre os dados que devem acompanhar seu relato, podemos citar:

- Data e horário da ocorrência
- Números de série
- Título descritivo
- Estimativas de dano
- Descrições detalhadas
- Nível de urgência
- Risco de proliferação
- Estruturas afetadas
- Pessoa ou área de comunicação
- Unidades e departamentos
- Relatório de procedimentos
- Solução adotada

Segurança da Informação no Gerenciamento de Projetos

O processo de Gerenciamento de Incidentes faz parte da fase de Operação no ciclo de vida do gerenciamento de serviços de TI, ou seja, do cotidiano do departamento. Porém, a segurança da informação deve ser considerada nas fases iniciais, tal como no planejamento, no processo de Gerenciamento de Projetos.

Gerenciamento de Projetos

É responsável por definir os objetivos a serem atingidos, de forma a otimizar os recursos.

ISO/IEC 27002:2013

Segurança da Informação no Gerenciamento de Projetos

- O gerenciamento de projetos avalia todos os pontos da mudança e as planeja;
- E a gestão da Segurança da Informação vai observa o passo a passo e verifica se tudo está de acordo, se a instalação deste novo sistema oferece algum risco, se abre alguma brecha ou cria uma nova vulnerabilidade.

O ideal é que o projeto seja criado respeitando os objetivos gerais da segurança da informação.

Que seja feita uma prévia avaliação dos riscos quanto à segurança da informação, para que se possa ter uma ideia do que é preciso controlar e que todas as fases do projeto estejam cobertas por medidas de segurança.

Gerenciamento de Ativos

Os ativos associados à informação e seu processamento devem ser identificados e inventariados neste processo, caso contrário seria praticamente impossível realizar o processos de Gerenciamento de Mudanças, Incidentes e Continuidade.

Critérios relevantes para inventário dos ativos no ciclo de vida da informação:

criação	processamento	armazenamento	transmissão	destruição

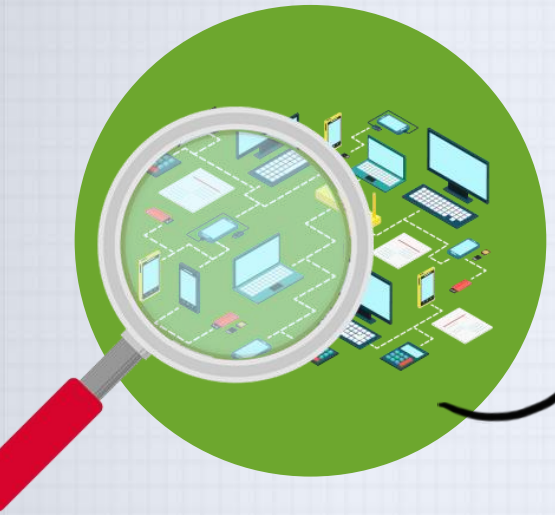
- Os ativos sejam inventariados;
- Sejam classificados e protegidos;
- Sejam definidas e revisadas periodicamente as restrições de acesso para ativos importantes.

Deve haver regras para o uso aceitável de ativos associados à informações.

Funcionários locais e externos precisam ser alertados a respeito das exigências da organização.

Todos os colaboradores locais e externos devem retornar todos os ativos em sua posse ao final do contrato.

Responsabilidades Pelos Ativos



Devem ser identificados os ativos da organização

Definidas as responsabilidades

- Um inventário destes ativos deve ser estruturado e mantido.
- Lembrando que o ciclo de vida da informação contempla a criação, o processamento, o armazenamento, a transmissão, a exclusão e a sua destruição.

Responsabilidades Pelos Ativos

O proprietário do ativo será o responsável pelo próprio gerenciamento deste ativo ao longo do seu ciclo de vida.

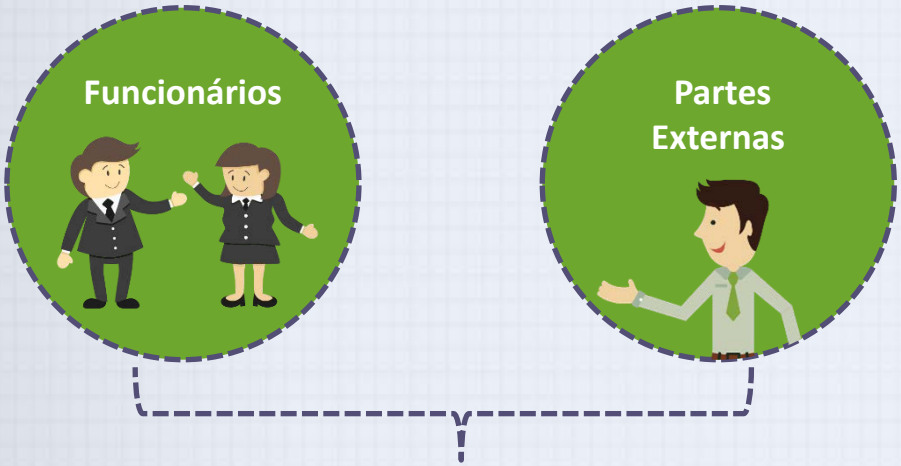
Assegurar que os ativos serão inventariados e adequadamente classificados e protegidos.

Definir e periodicamente analisar criticamente as classificações e restrições de acesso aos ativos importantes, levando em conta as políticas de controle de acesso.

Assegurar um adequado tratamento quando o ativo for excluído ou destruído.

Devolução dos Ativos

As regras para o uso aceitável das informações, dos ativos associados com a informação e dos recursos de processamento da informação devem ser identificadas, documentadas e implementadas.



Devem estar conscientes dos requisitos de segurança da informação, já que são responsáveis pelo seu uso.

- Devem devolver todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo.
- Pode comprar o equipamento da organização, por isso deve haver um procedimento para assegurar que toda a informação relevante seja transferida para a organização e apagada de forma segura do equipamento.
- É essencial que a organização monitore possíveis cópias de informações relevantes.

Teste

Pronto para o próximo?

Curso Preparatório para Certificação
Em Gestão de Segurança da Informação Avançada – Baseada na ISO/IEC 27002:2013

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 4

Identificação e Avaliação de Riscos

Identificar os Riscos

Identificação de Riscos

Começa com um processo de autoexame.

Os gestores identificam os recursos de informação da organização.

Os classificam em grupos úteis.

Os priorizam pela sua importância global.

Inventário de ativos de informações

- **Pessoas**
- **Procedimentos**
- **Dados**
- **Informações**
- **Software**
- **Hardware**
- **Elementos de rede**

Identificar os Riscos

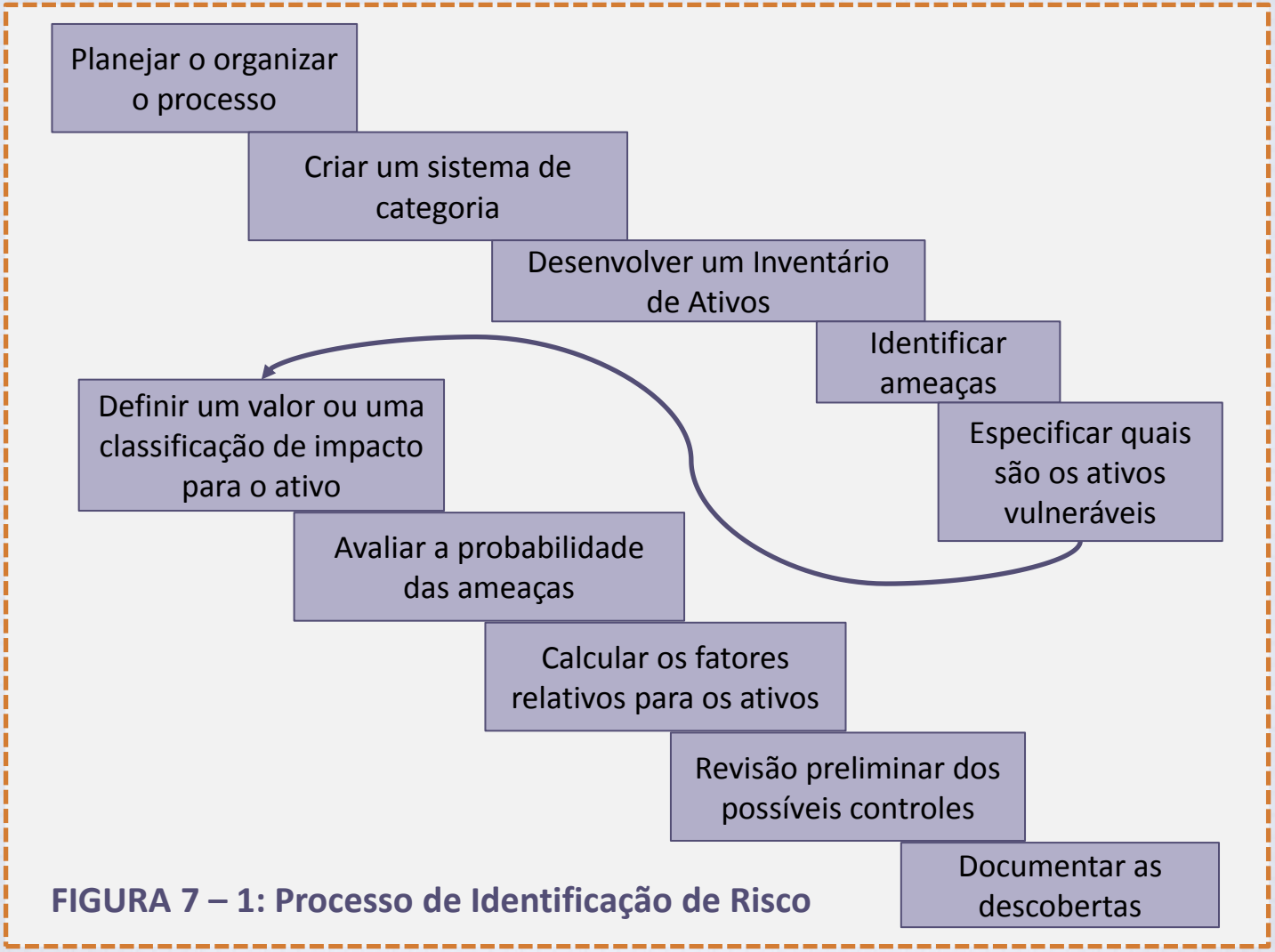


FIGURA 7 – 1: Processo de Identificação de Risco

Conhecendo as Fraquezas

- Criar um inventário com os programas instalados nos computadores, conhecer bem o conteúdo destes computadores, e saber as versões de cada equipamento.
- Definir quem vai ficar responsável por esta tarefa.
- Esta pessoa vai cuidar da gestão das vulnerabilidades e o monitoramento, além de uma eventual avaliação dos riscos, além de acompanhar as correções, quando necessário.

Administrador de Redes

Para acabar ou minimizar com as fraquezas, é possível ainda:

- Desativar os serviços nestes computadores, se possível.
- Colocar mais controles de acesso, como firewalls e outras barreiras.
- Aumentar a forma como tudo é monitorado, para prevenir os possíveis ataques.
- Melhorar a conscientização dos usuários quanto às fraquezas e às vulnerabilidades.

Identificando Hardware, Software e Recursos de Rede

Deve se determinar quais atributos de cada um desses ativos de informações devem ser rastreados.

Dependerá das necessidades da organização e de seus esforços de gerenciamento de riscos, bem como das preferências e necessidades das comunidades de segurança da informação e tecnologia da informação.

- **Nome**
- **Endereço de IP**
- **Endereço MAC**
- **Tipo de imobilizado**
- **Número de série**
- **Nome do fabricante**
- **Modelo do fabricante ou número da peça**
- **Versão do software, número da atualização etc.**
- **Localização física**
- **Local lógico**
- **Entidade controladora**

Identificando Pessoas, Procedimentos e Ativos de Dados

A responsabilidade pela identificação, descrição e avaliação desses ativos de informação deve ser atribuída aos gerentes que possuam o conhecimento, experiência e julgamento necessários.

Eles devem ser registrados por meio de um processo confiável de processamento de dados, como o usado para hardware e software.

- Pessoas;
- Posição / número / ID;
- Nome / número / ID do supervisor;
- Nível de segurança;
- Habilidades especiais;
- Procedimentos;
- Descrição;
- Finalidade;
- Dados;
- Classificação;
- Proprietário / criador / gerente;
- Tamanho da estrutura de dados;
- Estrutura de dados utilizada;
- Online ou offline;
- Localização;
- Procedimentos de backup.
- Elementos de software / hardware / rede aos quais está vinculado;
- Local onde está armazenado para referência; fins de atualização;

Classificando e Categorizando Ativos

- Determinar se as suas categorias de ativos são significativas, conforme o programa de gerenciamento de risco da organização.
- Refletir a sensibilidade e a prioridade de segurança atribuída a cada ativo de informação..
- Deve ser desenvolvido um esquema de classificação, que categorize esses ativos de informação, com base em suas necessidades de sensibilidade e segurança (confidenciais, internas e públicas etc.).

Categorias de classificação designam o nível de proteção necessário para um determinado ativo de informação.

Alguns tipos de ativos podem exigir um esquema de classificação alternativo.

As categorias de classificação devem ser abrangentes e mutuamente exclusivas.

Princípio da Classificação

O princípio por trás da classificação do ativo é permitir que apenas aquilo que é exigido seja protegido.

Serão os responsáveis por classificar a informação, baseando-se no impacto de sua perda, dano ou divulgação.

Secreta

Confidencial

Pública

Deve haver técnicas de advertência na manipulação das informações.

Aplicada em documento que será compartilhado com terceiros ou de uso restritos para um grupo, etc.

Classificação da Informação

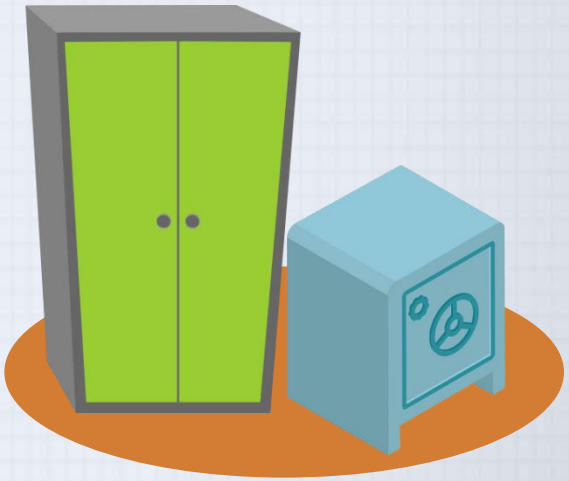
É assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.

Outros ativos, além dos de informação, também devem ser classificados de acordo com a classificação da informação armazenada, processada, manuseada ou protegida pelo ativo.

Deve haver certas convenções e critérios para classificação e para análise crítica da classificação ao longo do tempo.

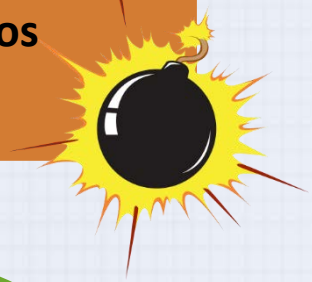
Deve-se pensar no armazenamento, distribuição, portabilidade e destruição desses ativos de informações.

Considere a informação como um valioso bem da organização



Processo de Classificação da Informação

Gerenciamento de Riscos



Identifica e avalia os níveis de risco enfrentados por uma empresa, especificamente as ameaças à segurança da organização e as informações armazenadas e processadas pela organização.

- **É essencial que a classificação seja incluída nos processos da organização,e seja consistente e coerente em todos os colaboradores e envolvidos na empresa. Que fique claro que a classificação indica o valor dos ativos em função da sua sensibilidade e criticidade para a organização, em termos da confidencialidade, integridade e disponibilidade.**

Considere o dono deste processo de Gerenciamento de Risco - ou de outro processo - como o dono do ativo que deve ser classificado.

- **Existe um ciclo de vida que deve se considerado, pois uma informação pode deixar de ser sensível ou crítica após certo período de tempo. Exemplo: Quando a informação se torna pública.**

Processo de Classificação da Informação

O esquema de classificação de confidencialidade da informação poderia ser baseado em quatro níveis:

- Quando sua divulgação não causa nenhum dano;
- Quando causa constrangimento menor ou inconveniência operacional menor;
- Quando tem um pequeno impacto significativo nas operações ou objetivos táticos;
- Quando tem um sério impacto sobre os objetivos estratégicos de longo prazo, ou coloca a sobrevivência da organização em risco.

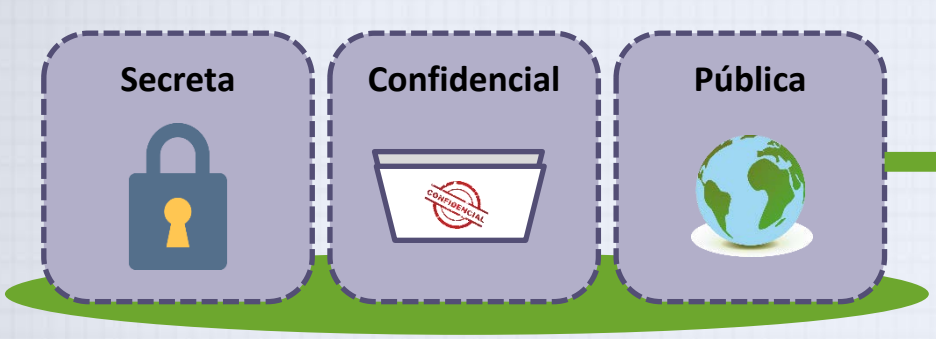
Rotulagem

A informação classificada serve de base para criar os rótulos.

Rotular é escrever em alguma parte bem visível o que há para saber sobre o documento.

- Desenvolver uma forma de rotular a informação, baseado nos níveis de classificação.
- As informações eletrônicas também devem ser rotuladas, como por exemplo, os e-mails.
- Os rótulos devem fazer sentido, criar um modo de que qualquer pessoa que ler, saiba do que se trata.
- Nem tudo precisa ser rotulado, informações que são públicas, por exemplo, não precisam passar por este processo.

Rotulando a Informação

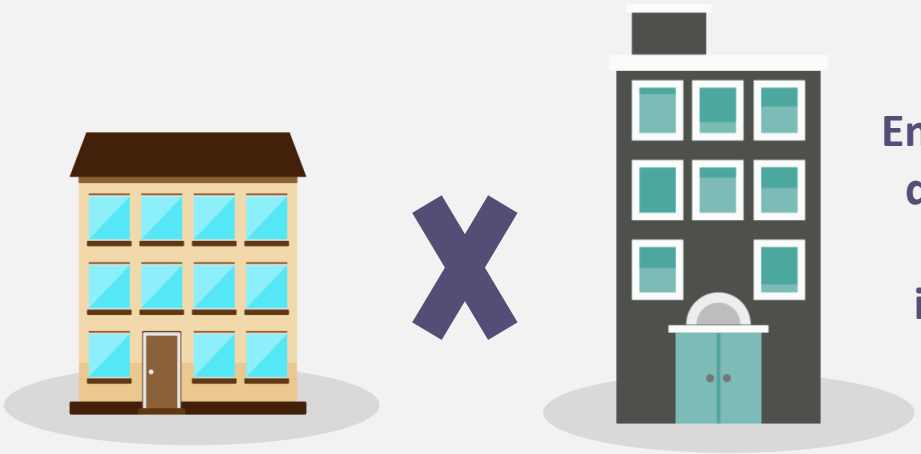


Averiguar quais controles cada informação requer.

Definir como a informação será tratada, processada, transmitida e armazenada.

- O acesso à informação classificada e rotulada deve ser restrito de acordo com o nível classificado.
- Deve haver um registro com o nome dos destinatários das informações.
- O armazenamento deve ser feito de acordo com a classificação e as recomendações dos fabricantes, dos proprietários ou outros.

Rotulando a Informação

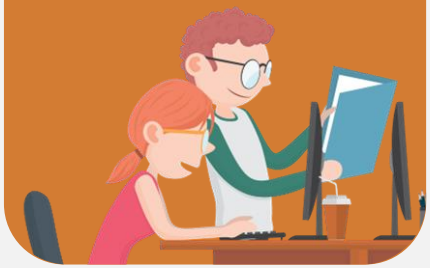


Empresas possuem políticas próprias, o que faz com que uma empresa possa considerar de uso Restrito uma informação que para outra empresa possa ser de Uso Interno.

A classificação costuma ser baseada nestes níveis:

Pública

Uso Interno



Restrita

Confidencial

Análise de Riscos

"Um Acordo de Nível de Serviço (ANS ou SLA, do inglês Service Level Agreement) é um acordo firmado geralmente, haja vista que outras áreas da empresa também podem se beneficiar desse recurso, entre a área de TI e seu cliente interno, que descreve o serviço de TI, suas metas de nível de serviço, além dos papéis e responsabilidades das partes envolvidas no acordo."

ISO/IEC 27005:	As ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27003:
Análise de riscos.	Planejamento, implementação e operação de controles.

O fato é que todas elas levam a uma Política de Segurança da Informação completa e contendo:

- Instruções obrigatórias;
- Framework de gestão dos controles;
- Responsabilidades e delegações;
- Escopo e aplicação de medidas e controles;
- Organização da segurança;
- Análise de riscos.

Avaliando os Riscos

- Identificados
- Quantificados
- Priorizados

Critérios de aceitação dos riscos

Objetivos da organização

- **Os resultados devem:**
  - ✓ Determinar as ações da empresa e as prioridades para o gerenciamento dos riscos de segurança da informação, com objetivo de implementar os controles apropriados.

- Devem ser realizadas periodicamente, para contemplar as mudanças nos requisitos de segurança da informação e na situação de risco;
- Devem ser realizadas de forma metódica, capaz de gerar resultados comparáveis e reproduzíveis.

Frentes na Avaliação de Riscos

3

Analisa-se a situação atual.

Medidas de segurança e controles são criados com base na análise.

Todas as medidas e controles, criados e aprovados, são incluídos no manual ou guia de instruções.

- **Quais ativos de informação nós precisamos proteger?**
- **Por que nós precisamos proteger esses ativos?**
- **Quais são os riscos?**
- **Quais são as prioridades na negociação desses riscos?**
- **Quais são as opções para lidar com esses riscos?**

Identificação de Ameaças

Bom senso

Senso crítico

Cada passo no processo da identificação de ameaças e da identificação de vulnerabilidades deve ser gerenciado separadamente e, ao final, ser coordenado em conjunto.

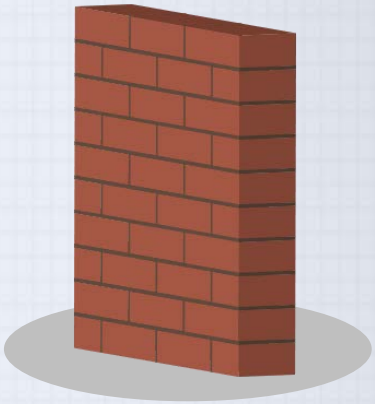
Cada uma deve ser examinada mais a fundo para determinar seu potencial real em afetar o ativo de informação almejado.

AVA

Avaliação da ameaça

Avaliação de Vulnerabilidade

Se uma ameaça significa que há probabilidade de um agente, acidentalmente ou propositalmente, gerar um dano. Então, concluímos que uma vulnerabilidade é uma fraqueza.



Depois de identificar os ativos de informações da organização.

→ **Documentar alguns critérios de avaliação de ameaças.**

↓

Começar a analisar cada recurso de informações para cada ameaça.

←

Criação de uma lista de vulnerabilidades

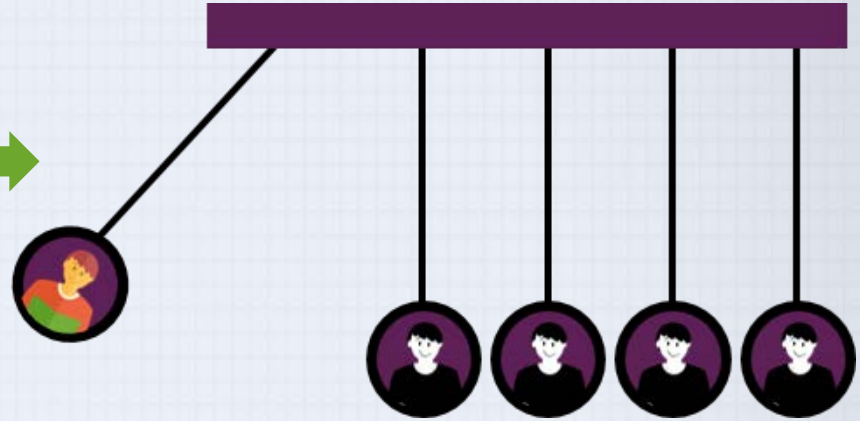
↓

AO FINAL: criação de lista de ATIVOS e suas vulnerabilidade

Criar um método para avaliar o risco relativo de cada vulnerabilidade listada.

Business Impact Analysis

Análise de impacto do negócio ou Business Impact Analysis (BIA).



- É feita para ajudar a empresa a identificar os processos onde uma melhora na segurança seria mais importante. Não deve ser feita sem a presença ou acompanhamento do dono da empresa.
- **NÃO** cuida da análise das informações ou das probabilidades, ela se concentra no foco no impacto dos eventos.

Consequências de desastres	Falhas de segurança
Perda de serviços	Disponibilidade de serviços

- Possibilita uma organização apontar os processos onde segurança é importante, deve ser realizado junto com o proprietário do negócio.

Cuida APENAS do impacto de um evento, como: a perda, o estrago, alteração ou divulgação de informações.

Risco e Probabilidade

O risco é a probabilidade da ocorrência de uma vulnerabilidade.

X

O valor do ativo de informação.

A probabilidade é uma classificação geral, ou seja, um valor numérico em uma escala definida. Por exemplo, de 0,1 a 1,0, algo que classifique a probabilidade de que uma vulnerabilidade específica seja explorada.

-

A porcentagem de risco mitigado ou atenuado pelos atuais controles.

+

A incerteza quanto ao conhecimento atual da vulnerabilidade.

Avaliar Perdas Potenciais

Quais ameaças representam um perigo para os ativos da organização em um determinado ambiente?

Que ameaças representam o maior perigo para as informações da organização?

Quanto custaria se recuperar de um ataque bem sucedido?

Que ameaças exigiriam maiores gastos para se prevenir?

Qual das perguntas acima é a mais importante para a proteção de informações contra ameaças dentro da sua organização?

Determinando os Riscos

Para efeitos de avaliação de risco relativo, como mencionado a pouco: o risco = a probabilidade da vulnerabilidade ocorrer; (X) o valor da ocorrência (ou do impacto), (-) o percentual de risco já controlado, (+) um elemento de incerteza.

A

- Valor de 50.
- 1 de vulnerabilidade.
- Probabilidade de 1,0 sem controles atuais.
- Essas suposições e dados estão 90% precisos.

B

- Valor de 100.
- 2 de vulnerabilidades:
- Probabilidade de:
  - **Situação 1:** 0,5 com um controle atual que já atende a 50% de seu risco;
  - **Situação 2:** 0,1 sem controles atuais.
- Essas suposições e dados estão 80% precisos.

Determinando os Riscos

Para efeitos de avaliação de risco relativo, como mencionado a pouco: o risco = a probabilidade da vulnerabilidade ocorrer; (X) o valor da ocorrência (ou do impacto), (-) o percentual de risco já controlado, (+) um elemento de incerteza.

Ativo A: Classificada como 55 = (50 × 1,0) - 0% + 10%.

Ativo B: Com a Probabilidade na Situação 1 classificada como 35 = (100 × 0,5) - 50% + 20%.

Ativo C: Com a Probabilidade na Situação 2: classificada como 12 = (100 × 0,1) - 0% + 20%.

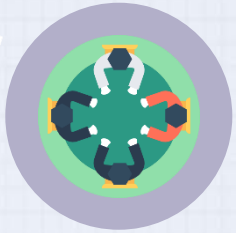
Considerações na Avaliação de Riscos

- Avalição de risco não é algo simples e muito menos uma tarefa fácil;
- Realize uma análise de impacto nos negócios para determinar onde a avaliação de risco é mais necessária;
- Implemente um patamar, um limite para tudo, exceto para aqueles controles extras de redução do risco, que devem ser implementados apenas quando necessário;
- Discuta os riscos que ainda não ocorreram, e para isso, é de extrema importância ter uma mente aberta;
- A análise de riscos pode ser facilitada por um especialista, mas requer também uma abordagem multidisciplinar com outros membros de todas as funções do negócio e da TI;
- Há muitas ferramentas disponíveis, mas elas podem ajudar apenas no processo, elas não farão o seu trabalho!

Identificando do Possíveis Controles

Deve ser criada então uma lista preliminar de ideias de controle.

Existem três categorias gerais de controles:



Organizacionais

Físicos

Controles técnicos

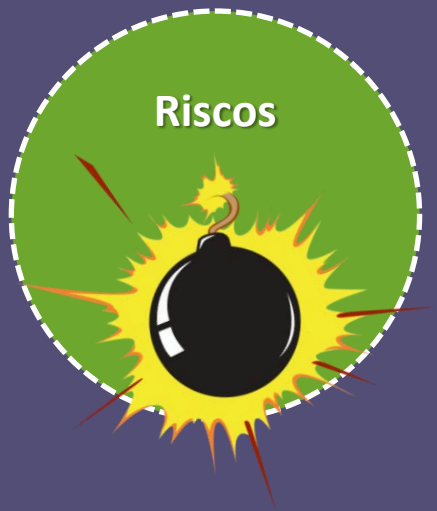
- **Risco residual - é o risco que permanece mesmo após o controle existente ter sido aplicado.**
- **Controles, salvaguardas e contramedidas - são todos os termos usados para descrever os mecanismos, políticas e procedimentos de segurança.**
- **Controles técnicos - também conhecidos como tecnologias de segurança - são as implementações técnicas das políticas (controles organizacionais) definidas pela organização.**

Processos de Avaliação de Risco

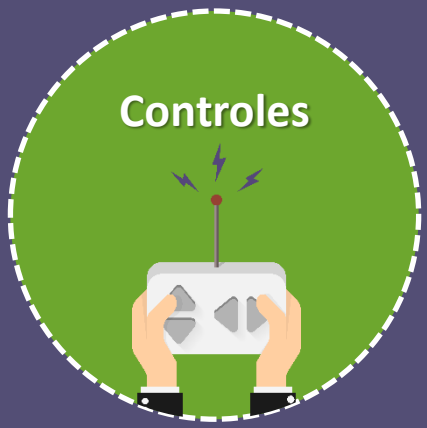
- Determinar os ativos no escopo da avaliação;
- Determinar os proprietários desses ativos;
- Discutir com os proprietários as ameaças para esses.

- Decidir quais são os agentes de ameaça;
- Obter opiniões de especialistas sobre as vulnerabilidades desses ativos;
- Obter opiniões de especialistas das probabilidades de que as ameaças ocorrem;
- Obter opiniões de especialistas sobre os impactos quando ocorrem as ameaças.

Processos de Avaliação de Risco



- Definir algum tipo de fórmula para calcular o risco
- Definir a inclinação de risco do proprietário
- Encontre opções para atenuar riscos inaceitáveis



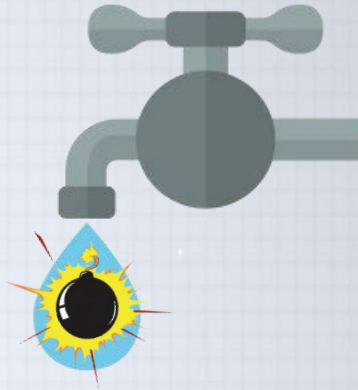
- Implementar controles
- Entender e mitigar os novos riscos dos próprios controles
- Aceitar quaisquer riscos residuais e repetir todos os itens acima

Processos de Avaliação de Risco

É o processo que visa compreender a magnitude, a estimativa e a natureza do risco, servindo inclusive como base para uma avaliação de riscos.

É feita a comparação dos riscos, conforme resultado da análise de riscos. Neste momento é determinado se a magnitude do risco é aceitável ou não.

Riscos Residuais



- **Quando as vulnerabilidades são controladas, podem permanecer riscos que não foram completamente removidos ou tratados. Este restante é chamado de RISCO RESIDUAL.**

Combina

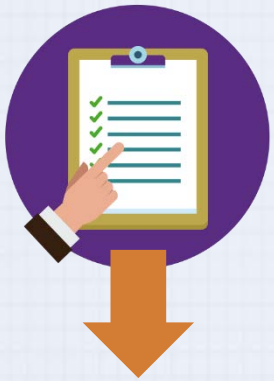
- Uma ameaça menos o efeito de salvaguarda na redução da ameaça;
- Uma vulnerabilidade menos o efeito de salvaguardas de redução de vulnerabilidade;
- Um ativo menos o efeito de salvaguarda de redução de valor do ativo.

Alinhar a estratégia de tratamento de risco conforme o apetite ao risco da organização.

Gerenciamento de risco concluído = Uma série de controles propostos, cada um dos quais é justificado por uma ou mais abordagens de viabilidade.

Documentando os Resultados da Avaliação de Riscos

O objetivo do processo de gerenciamento de riscos até agora foi identificar os ativos de informação e suas vulnerabilidades, classificando-os de acordo com a necessidade de proteção.



Além da documentação em si, é importante que nesse processo de identificação de risco seja designada qual função os relatórios terão, quem será o responsável pela sua preparação e quem os revisará.

DOCUMENTO FINAL

- Simples;
- Com grande valor;
- **AVA:** de Ameaça, Vulnerabilidade e Ativo.

Pronto para o próximo?

Curso Preparatório para Certificação
Em Gestão de Segurança da Informação Avançada – Baseada na ISO/IEC 27002:2013

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 5

Controlando o Risco

Resumo

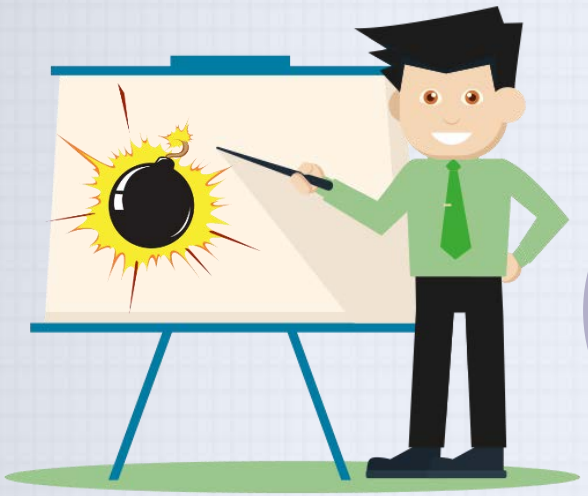
A identificação de categorias de classificação de controle de risco.

Aprenderá como manter e perpetuar estes controles de risco através da abordagem ACB, *Benchmark*, *Baseline* entre outros, para um estudo de viabilidade na seleção do melhor controle de risco e o OCTAVE e FAIR como método de Gerenciamento de Risco.

Compreender e selecionar as opções da estratégia de mitigação de risco para controlar o risco e identificar as categorias de classificação de controle de risco.

Apresentaremos as opções essenciais da estratégia de mitigação de riscos. Assim, teremos uma visão de como controlá-los.

Lidando com os Riscos



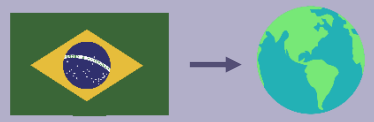
A organização deve definir os critérios para determinar se os riscos podem ser ou não aceitos.

- For avaliado que o risco é baixo.
- Custo do tratamento não é economicamente viável para a organização.

- Aplicar controles apropriados para reduzir os riscos;
- Conhecer e objetivamente aceitar os riscos, sabendo que eles atendem claramente à política da organização e aos critérios para a aceitação de risco;
- Evitar riscos, não permitindo ações que poderiam causar a ocorrência de riscos;
- Transferir os riscos associados para outras partes, por exemplo, seguradoras ou fornecedores.

Tratando os Riscos

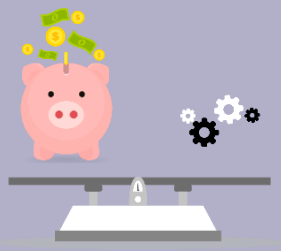
Requisitos e restrições da legislação e regulamentação nacionais e internacionais;



Objetivos organizacionais;

Requisitos e restrições operacionais;

A necessidade de equilibrar o investimento na implementação e operação de controles em relação aos danos suscetíveis de falhas de segurança.



Custo de implementação e operação em relação aos riscos que estão sendo reduzidos e que permanecem proporcionais às restrições e requisitos da organização;

- Podem ser selecionados a partir deste padrão ou de outros conjuntos de controle ou novos controles podem ser desenhados para atender às necessidades específicas.
- Devem ser considerados na especificação de requisitos de projetos e sistemas, e na fase de desenho.
- Nenhum conjunto de controles pode alcançar uma segurança completa, ações de gerenciamento adicionais devem ser implementadas...

Ciclo de Deming nos Controles de Segurança

Política

Avaliação

Gerenciamento de risco

Ciclo de Deming - PDCA

- Como os procedimentos, controles, etc.
- Mensure o desempenho e periodicamente revise tudo.

Planejar | **Executar** | **Verificar** | **Ajustar**

Ciclo de Deming nos Controles de Segurança

Act - Agir - Executar as ações corretivas e preventivas, com base nas verificações, além de comunicar os resultados.

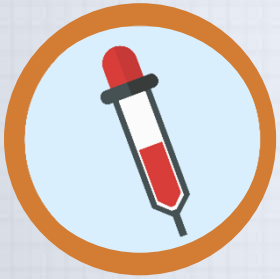
Plan – Planejar - estabelecer a política, os objetivos, processos e qualquer outro procedimento de SGSI, que possa ser útil no gerenciamento destes riscos. ***Statement of applicability– SoA*** (Declaração de Aplicabilidade).

Check - Avaliar – ou seja, conferir se está mesmo funcionando, e se precisar, ajustar os pontos. Nesta etapa faz-se o monitoramento e revisão.

Do - Executar – é colocar os controles em ação.

Estratégia de Controle dos Riscos I

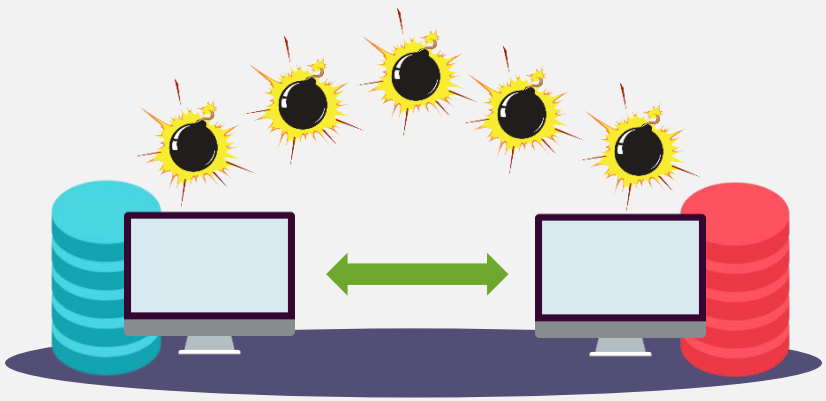
- **PREVENIR (Evitar):** Aplicar o esquema de salvaguardas para eliminar ou reduzir os riscos sem controles.
- **TRANSFERÊNCIA:** Transferir o risco para outras áreas ou para entidades externas.
- **MITIGAÇÃO:** Reduzir o impacto explorando a vulnerabilidade.
- **ACEITAÇÃO:** Compreender as consequências e aceitar o risco sem controle ou anular a mitigação.



Prevenção

Aplicação da política	**Combate as ameaças**
Formação e educação	**Implantação de controles de segurança técnica e salvaguardas**

Estratégia de Controle dos Riscos I



Transferência

A transferência é a abordagem de controle que tenta transferir o risco para outros ativos, outros processos, ou outras organizações.

É a abordagem de controle que tenta reduzir, por meio de planejamento e preparação, os danos causados pela exploração de vulnerabilidade. Esta abordagem inclui três tipos de planos:

- **O plano de recuperação de desastres (DRP);**
- **Plano de resposta a incidentes (IRP) e;**
- **Plano de continuidade de negócios (BCP).**

Estratégia de Controle dos Riscos II

A aceitação do risco é a escolha por não fazer nada para proteger um ativo de informação e a aceitar o resultado de qualquer exploração resultante.

O único uso válido da estratégia de aceitação ocorrerá quando a organização tiver:

- Determinado o nível de risco para o ativo de informação;
- Avaliada a probabilidade de ataque e a probabilidade de uma exploração bem sucedida ...;
- Taxa anual aproximada de ocorrência de falhas de exploit;
- Estimativa de perda potencial através dos ataques;
- Realizada uma aprofundada análise do custo-benefício;
- Controles de avaliação para cada tipo apropriado de viabilidade;
- Decisão se um recurso em particular não justifica o custo de proteção.

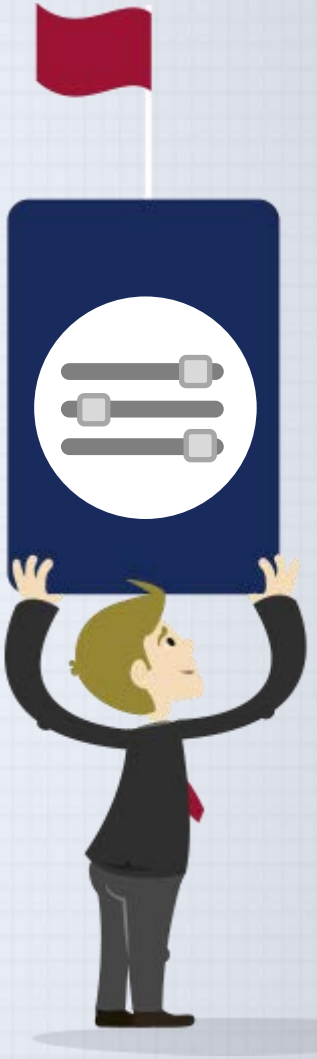
Seleção dos Controles

Dessa forma é possível assegurar que esses riscos sejam reduzidos a um nível aceitável.

Controle

Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

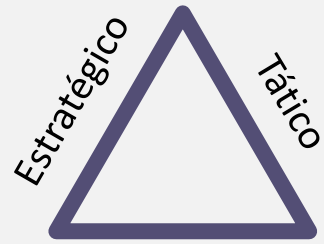
Proteção → **Contramedida**



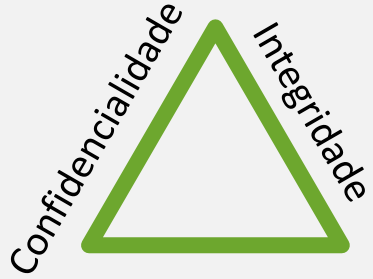
Controles podem ser selecionados a partir da Norma ISO/IEC 27002, de outro conjunto de controles ou novos controles podem ser desenvolvidos.

A seleção destes controles de segurança da informação vai depender muito das decisões da empresa.

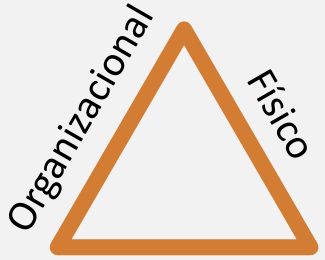
Tríade do Controle



Operacional

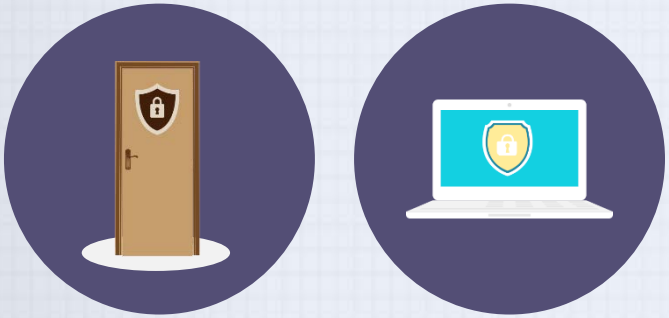


Disponibilidade



Lógico

Exemplo



Não há como controlar todos os acessos físicos e deixar as questões lógicas, como os programas, sem controles de disponibilidade.

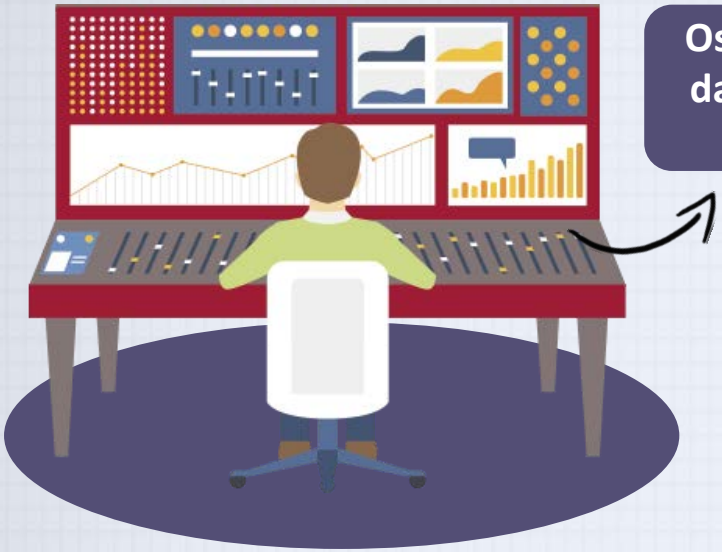
- Dever ser um controle equilibrado, para manter a confidencialidade, integridade e disponibilidade.
- Os controles devem sempre ser documentados e incorporados na organização.
- **Controle físico -** é preferível usá-lo ao invés do controle lógico, já que os controles físicos podem ser auditados muito mais facilmente.
- **Controle lógico -** é preferível usá-lo ao invés do controle organizacional/ controle processual, pois as pessoas cometem erros ao executarem os processos, e, por isso, um controle lógico funciona melhor neste caso.

Qual Controle Usar

- Observar os controles que ela apresenta;
- Consultar as três fontes dos requisitos de segurança;
- A legislação vigente;
- A avaliação de riscos para a empresa;
- E os objetivos e requisitos da própria empresa.

Norma ISO/IEC 27002:2013 + **Outros controles sugeridos em outras fontes** = Conjunto próprio de regras e controles.

Controles Estratégicos



Os controles estratégicos tratam especificamente da criação da política de segurança, motivo pela qual deva se começar antes mesmo de ter uma ideia mais clara dos riscos.

- Delegação e definição dos responsáveis da área de Gerenciamento ou da Governança.
- Responsável por fazer a gestão da segurança da informação, alocar recursos, contratar e capacitar o pessoal, além de definir valores para os ativos.
- Os controles estratégicos também devem lidar com a delegação das responsabilidades. É preciso ler os resultados dos relatórios constantemente para avaliar a situação atual.
- Criação de uma política de segurança; criação de um processo de avaliação.

Controles Táticos

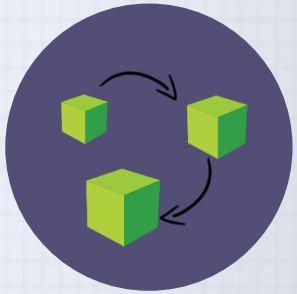
- **São controles específicos que iniciam as atividades práticas dentro da Segurança da Informação. Lidam especificamente com:**

- Atribuição de responsabilidades aos envolvidos na Segurança da Informação, tanto direta quanto indiretamente.

Formação do pessoal | **Treinamentos** | **Capacitação em SI**

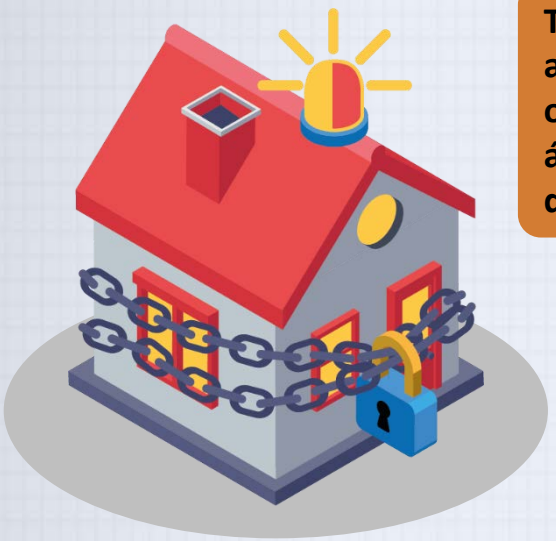
- Classificação e o gerenciamento dos ativos e das informações. Da melhoria do processo de gerenciamento de incidentes.

- Estes controles tratam também do cuidado dos aspectos de segurança quanto à continuidade de negócios.



- 6. A Organização da Segurança da Informação, 7. Gerenciamento de Ativos, 8. Segurança dos Recursos Humanos, 10. Criptografia, 13. Gerenciamento de Incidentes de Segurança da Informação, 15. Relacionamento com Fornecedores, 16. Gerenciamento de Incidentes de Segurança da Informação e 17. Aspectos do Gerenciamento de Segurança no Gerenciamento da Continuidade de Negócios.

Controles Operacionais



Tratam especificamente da proteção física para prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização, para que as instalações críticas ou sensíveis sejam mantidas em áreas seguras, protegidas por perímetros de segurança definidos, com barreiras de segurança e controles de acesso apropriados.

9. Controle de Acesso, 11. Segurança Física e Ambiental, 12. Segurança da Operação, 13. Gerenciamento da Comunicação e 14. Manutenção, Desenvolvimento e Aquisição de Sistemas de Informações.

Gerenciamento da Capacidade

Gerenciamento de Incidentes

- Solucionar problemas de segurança da informação.
- Criar formas de melhorar o ambiente, deixando-o mais seguro.

Gerenciamento de Problemas

Gerenciamento de Mudanças e Gerenciamento de Segurança

- Controle de acesso.
- Uso de um firewall.

Desenvolvimento de Software

Teste de Sistema

Soluções

Controles Organizacionais/ Controles Processuais *(Procedural Controls)*

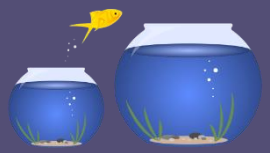
Política de Segurança

Organização Interna

Partes externas

Responsabilidade pelos ativos:

Gerenciamento de Mudanças



Relação com os Fornecedores

Responsabilidade pelos procedimentos operacionais

Lidar com a classificação das informações e com o seu correto manuseio.

Controle de Acesso

pass : *****

Gerenciamento de Incidentes

Uma coerente Identificação da legislação aplicável, afinal, é preciso conhecer as leis antes de se prevenir algo.

Proteção dos ativos

Categorias de Controles

Os controles podem ser categorizados da seguinte forma:

Função de Controle

Controles projetados para proteger um sistema que esteja vulnerável. São divididos em controles preventivos e de detecção:

- **Controles preventivos** detêm as tentativas de exploração das vulnerabilidades através de procedimentos técnicos;
- **Controles de detecção** alertam as violações dos princípios de segurança ou tentativas de exploração das vulnerabilidades. Usam técnicas como: logs de auditoria, detecção de intrusão e monitoramento.

Camadas de Arquitetura

Esse controle é aplicado a uma ou mais camadas de arquitetura técnica de uma organização. Os possíveis modelos de camadas arquitetônicas podem incluir o seguinte:

- Política organizacional
- Intranets
- Redes externas
- Dispositivos de rede...
- Extranets
- Sistemas
- Zonas desmilitarizadas (DMZ)
- Aplicações

Categorias de Controles

Os controles são, por vezes, classificados pela estratégia de controle de risco, ou seja, das quais já conhecemos como de prevenção, mitigação ou transferência. Note que a estratégia de aceitação do risco não é uma opção aqui, uma vez que essa estratégia envolve a ausência de controles.

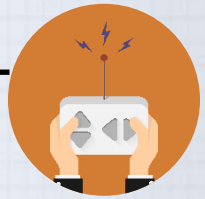
- Autorização
- Prestação de contas (Accountability)
- Privacidade
- Confidencialidade
- Integridade
- Disponibilidade
- Autenticação

Controles de risco que operam dentro de um ou mais dos princípios de segurança da informação comumente aceitos:

Controles de Riscos

A norma ISO/IEC 27002 informa sobre os controles dos riscos que, aqueles riscos onde a decisão de tratamento seja a de aplicar os controles apropriados, esses controles sejam selecionados e implementados para atender aos requisitos identificados pela análise/avaliação de riscos.

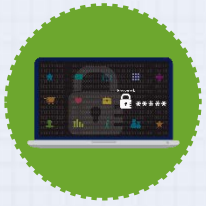
ISO/IEC 27002 ← **Outros conjuntos de controles existentes.** ← **Ou ainda, criados novos controles.**



"logging"

Legislação específica

Proteção à privacidade dos clientes



ou aquelas exercidas nos locais de trabalho

- Os **controles de segurança** da informação devem ser considerados na especificação dos requisitos e nos estágios iniciais dos projetos e sistemas.
- Caso isso não seja realizado, pode acarretar **custos adicionais e soluções menos efetivas**, ou mesmo, no pior caso, **incapacidade de se alcançar a segurança necessária.**
- **Nenhum conjunto de controles** pode conseguir uma **segurança completa**, e que uma ação gerencial adicional deve ser implementada...

Fontes de Requisitos de Segurança da Informação

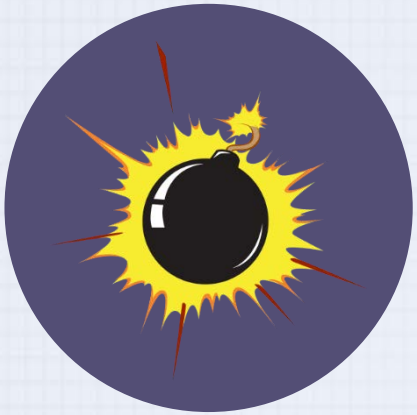
- A legislação vigente, com seus estatutos e cláusulas contratuais, os contratos firmados com parceiros, fornecedores e consumidores.

- A própria avaliação de riscos para a empresa, contando com os objetivos e estratégias de negócio da empresa – estratégias globais, com uma identificação das ameaças aos ativos, quais as vulnerabilidades, juntamente com uma estimativa das probabilidades de ocorrência de incidentes, e por fim, o impacto potencial a empresa.

- A terceira fonte é composta basicamente pelos objetivos e requisitos da própria empresa.

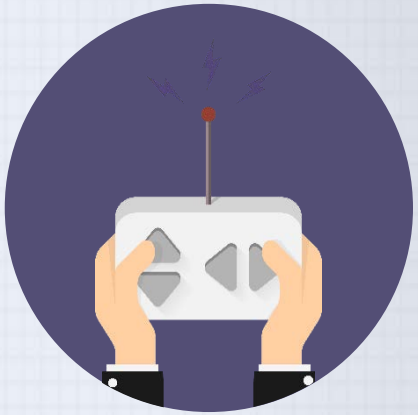
Seleção de Controle

Com Requisitos de Segurança da Informação



E riscos identificados

Decisões para o tratamento dos riscos tomadas



Convém que controles apropriados sejam selecionados e implementados

Conjunto de controles da norma ISO/IEC 27002

Novos controles podem ser desenvolvidos

- A seleção de controles de segurança da informação depende das decisões da organização;
- Baseadas nos critérios para aceitação de risco;
- Nas opções para tratamento do risco e no enfoque geral da gestão de risco aplicado à organização;
- Sujeito a todas as legislações e regulamentações nacionais e internacionais.

Seleção de Controle

Após a análise de Riscos, lembre-se que:

1º

O ideal é sempre manter um controle dos acessos e colocar controles a mais – ou mais direcionados – apenas quando for realmente necessário.

2º

As medidas que serão colocadas em funcionamento na empresa, para ajustar os controles que foram percebidos com a avaliação, devem ser bem balanceados:

- **Probabilidades de danos à empresa;**
- **E de acordo com o resultado dos problemas de segurança, causo faltem estes controles.**

Regras para a Seleção de Controle

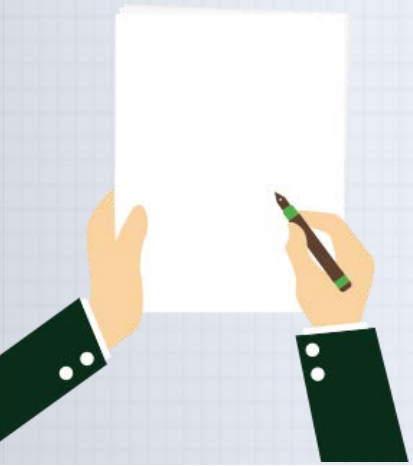
A seguir, algumas das regras básicas que ajudarão na seleção de estratégias de controle:

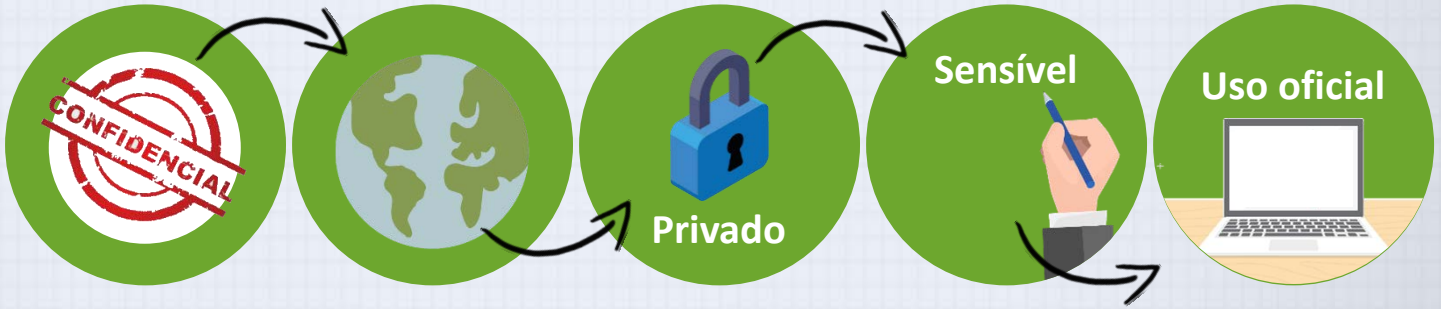
- Quando existir uma vulnerabilidade, deve-se implementar os controles de segurança para reduzir a probabilidade dela ser realmente explorada.
- Quando uma vulnerabilidade pode ser explorada, devem ser aplicados controles em camadas, para minimizar o risco ou evitar a ocorrência.
- Quando o ganho potencial do atacante é maior do que os custos do ataque: Aplique proteções para aumentar o custo do atacante, ou reduzir o ganho do atacante, usando controles técnicos ou organizacionais.
- Quando a perda potencial é substancial: Aplique controles de projeto para limitar a extensão do ataque, reduzindo assim o potencial de perda.

Avaliar o Valor dos Ativos de Informações

Os valores relativos são julgamentos comparativos, feitos para garantir que os ativos de informação mais valiosos, recebam a mais alta prioridade no gerenciamento do risco.

- Qual ativo de informação é o mais crítico para o sucesso da organização?
- Qual ativo de informação gera mais receita?
- Qual ativo de informação gera a maior rentabilidade?
- Que perda do ativo de informação seria o mais penoso ou causaria a maior responsabilidade?
- Qual ativo de informação é o mais caro para proteger?
- Qual ativo de informação é o mais caro de substituir?





Avaliar o Valor dos Ativos de Informações

Para desenvolver um modelo de Classificação de Dados, considere uma variedade de esquemas de classificação.

- **Os donos de dados devem classificar os ativos de informações das quais são responsáveis.**
- **Devem revisar essas classificações periodicamente para garantir que os dados ainda estejam classificados corretamente e os controles de acesso estão corretos.**

Alto

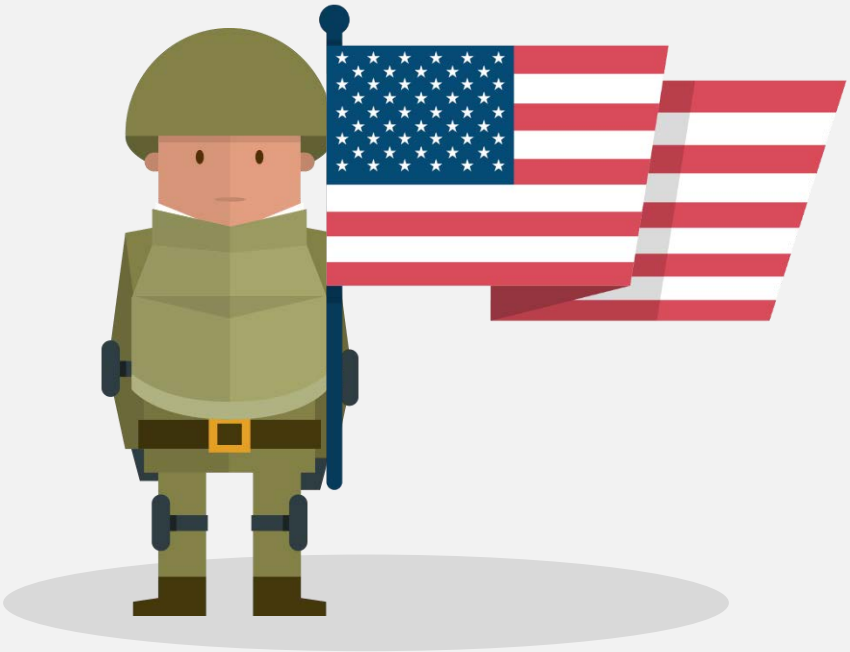
Médio

Baixo

Crítico

Avaliar o Valor dos Ativos de Informações

Esquema de classificação militar dos EUA. → **Ordem Executiva 12958**



- Dados não classificados;
- Dados sensíveis, mas não classificados;
- Dados confidenciais;
- Dados secretos;
- Dados extremamente secretos.

Avaliação dos Ativos

- Valor retido em relação aos custos de criação do próprio ativo de informação;
- Valor retido na manutenção do ativo de informação;
- Valor implícito no custo de substituição das informações;
- Valor para o fornecimento das informações;
- Valor adquirido do custo de proteção das informações;
- Valor para os proprietários;
- Valor da propriedade intelectual;
- Valor para os concorrentes;
- Perda de produtividade, enquanto os ativos de informação não estão disponíveis;
- Perda de receita, enquanto os ativos de informação não estão disponíveis.

Avaliação dos Ativos

Quanto custou para criar ou adquirir esta informação?

Quanto custaria para recriar ou recuperar esta informação?

Quanto custa para manter esta informação?

Quanto esta informação vale para a organização?

Quanto esta informação vale para a concorrência?

Avaliação dos Ativos

A próxima característica que a organização deve examinar é a perda potencial que pode ocorrer a partir da exploração da vulnerabilidade ou uma ocorrência de ameaça.

Quais danos poderiam ocorrer e qual o impacto financeiro que ele tem?

Qual é a expectativa de perda única para cada risco?

Qual seria o custo para recuperar do ataque, além do impacto financeiro de danos?

Estudos de Viabilidade e Análise de Custos e Benefícios

Antes de decidir sobre qual estratégia utilizar para uma vulnerabilidade específica, todas as informações sobre as consequências econômicas e não econômicas da vulnerabilidade enfrentada pelo recurso de informação, devem ser analisadas.

"Quais são as vantagens e desvantagens reais e percebidas de implementar um controle?"

Análise custo-benefício ACB (Cost Benefit Analysis - CBA)

É uma das abordagens mais comum para um projeto de controles e salvaguardas de segurança da informação, pois é através desta análise que será realizada a viabilidade econômica da implementação.

Avaliação do valor dos ativos de informação que devem ser protegidos

E a avaliação do valor perdido se esses ativos forem comprometidos.

Análise custo-benefício

Estudo de viabilidade econômica

Estudos de Viabilidade e Análise de Custos e Benefícios

Alguns dos itens que afetam o custo de um controle ou salvaguarda:

- Custos de desenvolvimento ou aquisição
- Custos com treinamento
- Custos da implementação
- Custos do serviço
- Custos de manutenção

O benefício do CBA é o valor que a organização reconhece, usando determinados controles, que evitam perdas associadas a uma vulnerabilidade específica.

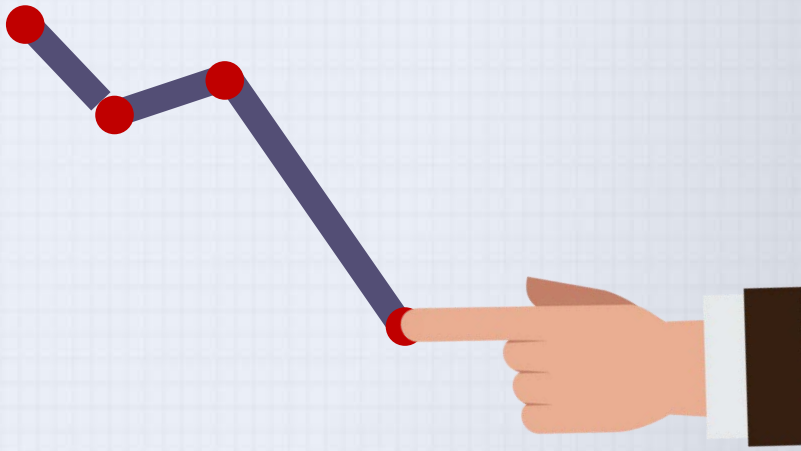
Estimativas de Perdas

Avaliação de Ativos

É o processo de atribuição de valor financeiro ou valor a cada ativo de informação.

- Envolve a estimativa de custos reais e percebidos associados à concepção;
- Desenvolvimento;
- Instalação;
- Manutenção;
- Proteção;
- Recuperação;
- Defesa.

- **Que danos poderiam ocorrer, e que impacto financeiro teria?**
- **O que custaria recuperar do ataque, além dos custos acima?**
- **Qual é a expectativa de perda única para cada risco?**



Expectativa de Perda Anual (EPA)

Expectativa de Perda Anual – EPA (*annualized loss expectancy – ALE*)

EPA = EPU x TOA

Expectativa de Perda Única - EPU (*Single Loss Expectancy - SLE*)

- **É baseado no valor que está associado com a perda mais provável de um ataque.**
- **É calculado com base no valor do ativo e a porcentagem esperada de perda.**

EPU = Valor do Ativo (VA) X Fator de Exposição (FE)

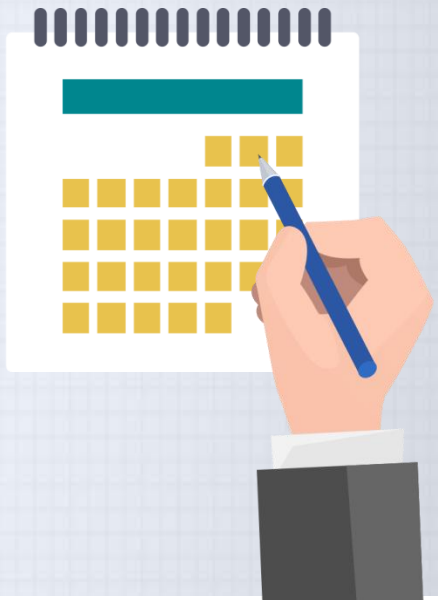
FE =

A perda percentual que ocorreria a partir de uma determinada vulnerabilidade.

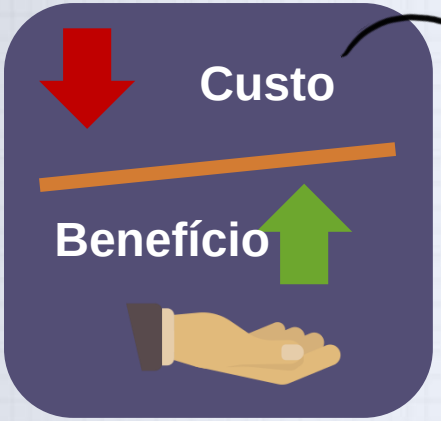
Taxa de Ocorrência Anua l – TOA (Annualized Rate of Occurrence – ARO)

Potencial total perdido por um risco.

Expectativa de Perda Anual – EPA (annualized loss expectancy – ALE) → **EPA = EPU x TOA**



Análise de Custo Benefício (ACB)



Análise de Custo Benefício – ACB *(Cost Benefit Analysis - CBA)*

É uma fórmula que vai determinar se o custo associado a uma alternativa de controle vale ou não a pena.

Custo Anual da Salvaguarda – CAS *(Annual Cost of the Safeguard – ACS)*

+

Resultado da Expectativa de Perda Anual - EPA:

A ACB = EPA (antes) - EPA (depois) – CAS

EPA (antes de controlar)

É a expectativa de perda anual do risco antes da implementação do controle.

EPA (pós-controle)

É a EPA examinada após o controle estar em vigor por um período de tempo.

Como resultado, quanto maior o valor resultante da ACB, segundo essa análise de custo-benefício, a aplicação dos controles e das técnicas de salvaguarda foi boa. Em contrapartida, um número mais baixo representa uma ação não muito satisfatória.

Retorno sobre o Investimento de Segurança (ROSI)

Custo Total de Propriedade – CTP
(Total Cost Ownership – TCO)

Retorno sobre o investimento
(ROI - Return on Investiment)

ROI

ROSI

Return on Security Investment

O **ROI** é definido como o lucro líquido de um investimento dividido pelo valor líquido dos ativos investidos.

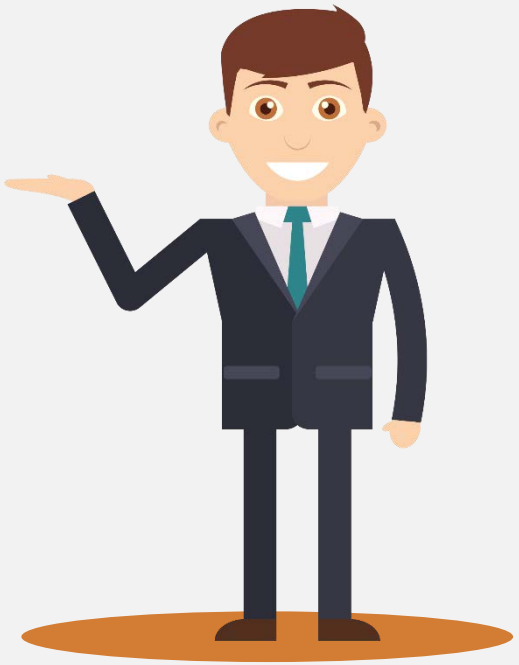
Avaliação dos riscos

Os controles mais eficazes:

- São aqueles que geram menos custos;
- Com um menor investimento;
- Tragam maiores receitas ou gerem maiores benefícios para a organização

Retorno sobre o Investimento de Segurança (ROSI)

- Qual é o valor da informação?
- Qual o valor perdido devido o impacto de um incidente?
- Qual é a probabilidade de um incidente que ocorrer?
- Qual é o custo para o reparo?
- Qual é o custo de implementação dos controles?
- Qual é o custo de manutenção dos controles?



ROSI = (Benefícios - Custos) / Custos

ROSI = [(Exposição ao Risco * % de Mitigação do Risco) – Custos] / Custos

ROSI = [EPA (antes) - EPA (depois) – Custos] / Custos

Caso de Negócios

- Identificar quais serão suas as opções ou alternativas.
- Avalie também a existência de outras possibilidades de redução de risco.
- Quais seriam os benefícios se os investimentos fossem alocados de forma diferente.
- Qual seria o ROI de um mesmo valor de investimento.

Os custos incluem os custos diretos e anuais da operação

Os benefícios incluem os lucros

Os benefícios subjetivos são a imagem

ROSI ≠ **ROI**

ICD - Indicadores Chave de Desempenho (KPI – Key Performance Indicators)

Caso de Negócios

Conformidade com os padrões da indústria através de um benchmarking;

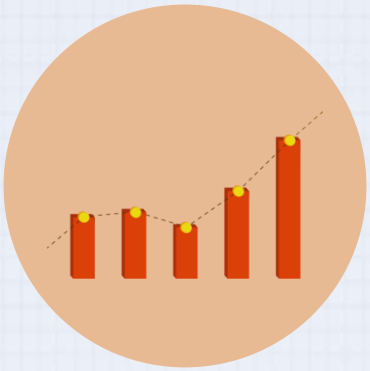
Investimentos necessários para manter o nível básico de segurança;

Com base em um melhor ROI;

Ajustado conforme a política da organização.

Outros Métodos de Viabilidade

Outros conceitos de viabilidade econômica



Uso de linha de base (*baseline*)

Referências (*benchmark*)

- **Análise de viabilidade organizacional;**
- **Viabilidade operacional (ou física);**
- **Viabilidade técnica;**
- **Viabilidade política.**

- **Benchmark;**
- **Baseline;**
- ***Due Care* e *Due Diligence*;**
- **Melhores Práticas de Negócios;**
- **Padrão Ouro.**

Benchmark

Referências (benchmark)

É o processo de busca e estudo das práticas utilizadas em outras organizações que produzem os resultados que você deseja em sua organização.

Duas medidas para comparar as práticas:

- Baseadas em métricas
- Baseadas em processos

As medidas baseadas em métricas são as comparações baseadas em padrões numéricos, tais como:

- Número de ataques bem-sucedidos;
- Horas de pessoal dedicadas à proteção de sistemas;
- Valores gastos em proteção;
- Quantidade de pessoal que atuam na segurança;
- Valor estimado das informações perdidas em ataques bem-sucedidos;
- Perda em horas de produtividade associada a ataques bem-sucedidos.

Benchmark

São geralmente menos focadas nos números e são mais estratégicas.

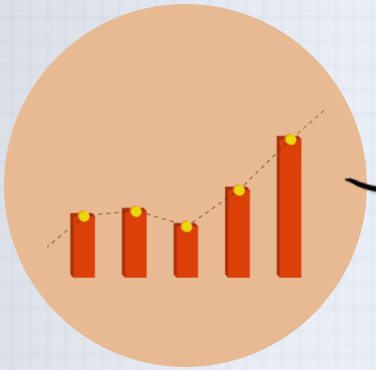
Medidas baseadas em processos

No domínio da segurança da informação, são utilizadas duas categorias de benchmarks:

- Padrões de devido cuidado e devida diligência (Due Care e Due Diligence);
- Melhores práticas.

Padrão-ouro é uma subcategoria de práticas que normalmente são vistas como "o melhor dos melhores", ou seja, The Best of The Best!

Baseline



É analisar as medidas em relação aos padrões estabelecidos.

Baseline

Princípios

- Implemente um conjunto limitado de controles para todos ativos. Cuidado com o excesso de controles, pois o custo e esforço de controles não podem ser maiores que o próprio ativo.
- Esteja apto a explicar e justificar a razão de implementar apenas esses controles nesses ativos. Lembre-se: use como ferramenta para isso a análise de impacto nos negócios;
- Realize uma avaliação de risco em todos os outros ativos e implemente controles extras apenas quando necessário.

Baseline

Considerar na sua avaliação de risco:

- Proteção de dado e privacidade de informação pessoal;
- Proteção dos registros organizacionais;
- Direitos de propriedade intelectual;
- Informação do documento de política de segurança;
- Alocação de responsabilidades de segurança da informação;
- Consciência da informação de segurança, educação e formação;
- Processamento correto das aplicações;
- Gerenciamento de vulnerabilidade técnica;
- Gerenciamento de continuidade de negócios;
- Gerenciamento de incidentes de segurança da informação e melhorias.

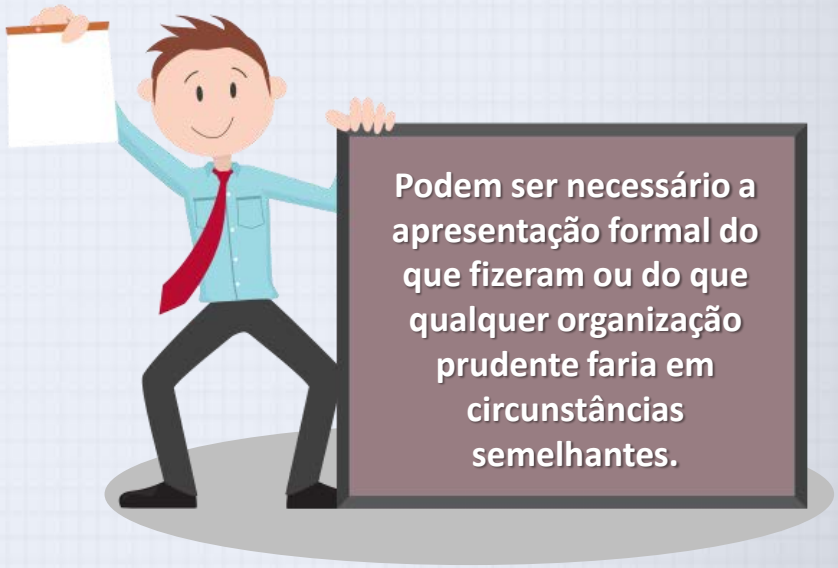
Due Care e Due Diligence

Padrão de devido cuidado

Padrão de devida diligência

São dois conceitos que ajudam a definir os padrões esperados para os requisitos de segurança.

- **O padrão de devida diligência (Due Diligence) é a demonstração que a organização é persistente em assegurar que os padrões implementados continuam a fornecer o nível de proteção necessário.**
- **O Due Diligence - ato de investigar e compreender os riscos que a empresa enfrenta.**
- **O Due Care – composto de medidas essenciais, que ajudarão na proteção da organização e dos seus recursos, contra possíveis riscos que foram identificados**



Melhores Práticas

ISO/IEC 27002:2013

As melhores práticas de segurança são aquelas que estão entre as melhores da indústria, equilibrando o acesso à informação com proteção adequada, mantendo ao mesmo tempo um grau sólido de responsabilidade.

Padrão-ouro

É um nível máximo de desempenho que demonstra uma liderança na indústria, alta qualidade e preocupação com a proteção da informação.

Aplicando Melhores Práticas

- Sua organização se parece com a organização que está implementando as melhores práticas?
- Sua organização está em uma área da indústria similar?
- Sua organização enfrenta desafios semelhantes?
- Sua estrutura organizacional é semelhante à organização da qual você está modelando as melhores práticas?
- Sua organização pode gastar recursos que estão de acordo com os requisitos das melhores práticas?
- Sua organização está em um ambiente de ameaça semelhante ao mencionado nas melhores práticas?

- **As organizações não falam entre si.**
- **Não há duas organizações idênticas.**
- **Melhores práticas são um alvo em constante movimento e mudanças.**
- **Simplesmente saber o que estava acontecendo há alguns anos atrás, não indica necessariamente o que deve ser feito agora.**

FAIR

Jack A. Jones

FAIR - Factor Analysis of Information Risk

Ajuda as organizações a entender, analisar e medir o risco da informação e, como resultado, a organização pode obter um gerenciamento de risco de informação mais rentável, com maior credibilidade.

- Uma taxonomia (define os grupos) para o risco de informação;
- Nomenclatura padrão para termos de risco de informação;
- Uma estrutura para estabelecer critérios de coleta de dados;
- Escalas de medição para fatores de risco;
- Um mecanismo computacional para calcular riscos;
- Uma construção de modelagem para analisar cenários de risco complexos.

FAIR

A análise FAIR básica compreende 10 fases em quatro etapas:

- **Etapa 1** - Identificar os componentes de um cenário:
  - ✓ 1. Identificar o ativo em risco.
  - ✓ 2. Identificar a comunidade de ameaças.

- **Etapa 2** - Avaliar a frequência de eventos de perda *(LEF - Evaluate Loss Event Frequency):*
  - ✓ 3. Estimar a frequência de evento de ameaça provável *(TEF - Threat Event Frequency).*
  - ✓ 4. Estimar a capacidade de ameaça *(TCap -Threat Capability).*
  - ✓ 5. Estimar a força do *controle (CS - Control Strength)*
  - ✓ 6. Derivar vulnerabilidades *(Vuln - Vulnerability).*
  - ✓ 7. Derivar a frequência doss eventos de perda Evento *(LEF - Derive Loss Event Frequency).*

- **Etapa 3** - Avaliar a magnitude da perda provável (PLM - Probable Loss Magnitude):
  - ✓ 8. Estimar a perda do pior caso.
  - ✓ 9. Estimar a perda provável.

- **Etapa 4** - Derivar e Articular o Risco
  - ✓ 10. Derivar e articular riscos.

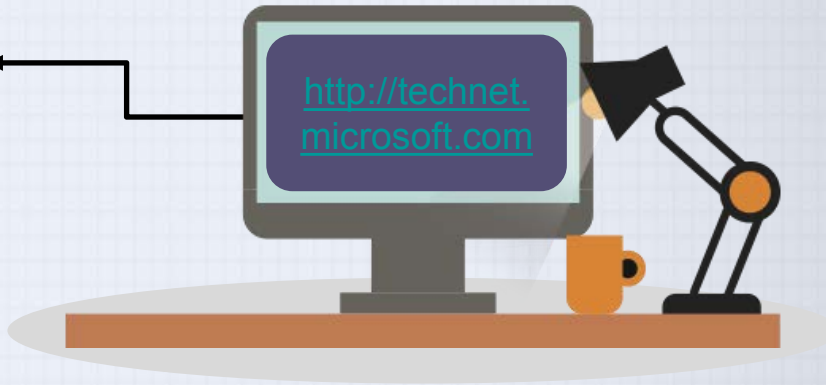
Abordagem de Gerenciamento de Riscos da Microsoft

Microsoft

Guia de Gerenciamento de Risco de Segurança:

Afirma que o gerenciamento de riscos não é um assunto independente e, portanto, deve fazer parte de um programa de governança geral para permitir que a comunidade organizacional e gerencial avaliem as operações da organização, tomem decisões melhores e mais informadas.

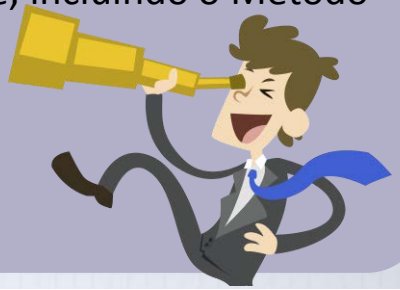
- **Abrangente**
- **Facilmente escalável**
- **Repetível**



Priorizar e gerenciar riscos de segurança

1. **Avaliação do risco;**
2. **Realização de apoio à decisão;**
3. **Implementação de controles;**
4. **Medir a eficácia do programa.**

Fornecem uma visão geral de um programa que é semelhante aos métodos apresentados anteriormente, incluindo o Método **OCTAVE.**



Método OCTAVE

O C T A V E

Operationally Critical Threat, Asset, and Vulnerability Evaluation

Método Operacionalmente Crítico de Ameaça, Ativos e Avaliação de Vulnerabilidade

http://www.cert.org/octave

É uma metodologia de avaliação de risco da segurança da informação, que permite às organizações equilibrar a proteção de ativos críticos de informação com os custos de fornecer controles de proteção e detecção.

Permite que uma organização faça uma avaliação em relação às boas práticas de segurança conhecidas e aceitas, para que, em seguida, estabeleça uma estratégia de proteção e um plano de mitigação de riscos de segurança da informação.

Método OCTAVE

Há três variações do método OCTAVE:

- O método OCTAVE original, que constitui a base para (knowledge) o corpo de conhecimento OCTAVE. Foi projetado para grandes organizações com 300 ou mais usuários.
- OCTAVE-S, para organizações menores, com cerca de 100 usuários.
- OCTAVE-Allegro, uma abordagem simplificada para a avaliação e garantia da segurança.

Outras Normas e Métodos

ISO 27000 → **Padrão para desempenho da Gestão de Riscos** → **ISO/IEC 27005**

http://www.27000.org/iso-27005.html

- **Avaliação do risco de segurança da informação;**
- **Tratamento do risco de segurança da informação;**
- **Aceitação do risco de segurança da informação;**
- **Comunicação de risco de segurança da informação;**
- **Acompanhamento e revisão dos riscos da segurança da informação.**

Outras Normas e Métodos

enisa
European Network and Information Security Agency

- **Agência Europeia para a Segurança das Redes e da Informação** - usa 22 atributos diferentes e fornece um utilitário em seu site que permite aos usuários comparar métodos ou ferramentas de gerenciamento de risco.
- **O site http://is027001security.com**, patrocinado pela IsecT, Ltd. que descreve mais de 60 métodos de gerenciamento de risco: (http://www.is027001security.comlhtml /faq.html # RiskAnalysis)

Pronto para o próximo?

Curso Preparatório para Certificação
Em Gestão de Segurança da Informação Avançada – Baseada na ISO/IEC 27002:2013

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 6

Controles Organizacionais

Resumo

Ao final deste módulo você terá conhecimento sobre os controles organizacionais.

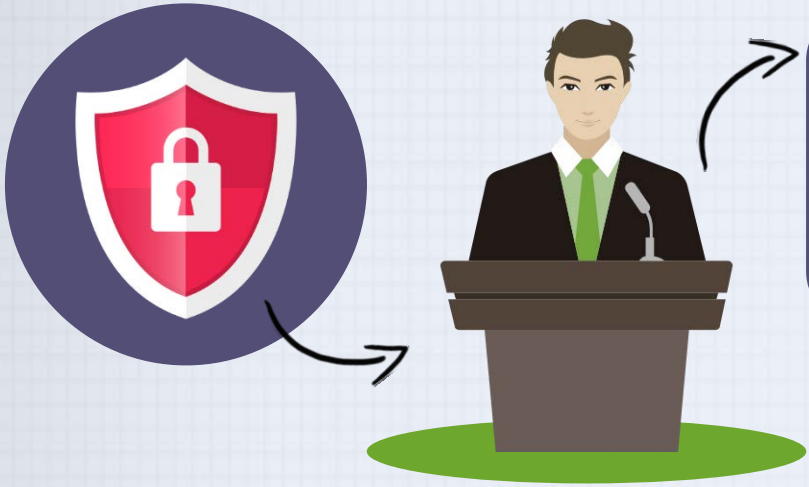
Saberá desenhar políticas e procedimentos de segurança da informação.

Implementar uma campanha de conscientização na organização...

Implementar o gerenciamento de incidentes de segurança de informação...

Implementar atribuições e responsabilidades para segurança da informação.

Porque uma Política?



As políticas desenvolvidas e implementadas adequadamente permitem que o Programa de Segurança da Informação funcione quase perfeitamente dentro do local de trabalho.

- **A política nunca deve entrar em conflito com a lei;**
- **A política deve ser capaz de se útil em tribunal, se contestada;**
- **A política deve ser devidamente apoiada e administrada.**

Porque uma Política?

- Não se deve acreditar que a única razão para o desenvolvimento de políticas seja simplesmente evitar um litígio. É importante enfatizar a natureza preventiva da política.

- Para informar os colaboradores sobre o que é e o que não é um comportamento aceitável na organização.

- Trata-se de um esforço para melhorar a produtividade dos colaboradores e evitar situações potencialmente embaraçosas.

Políticas, Padrões e Práticas

As políticas exigem constante modificação e manutenção. Para produzir uma política completa de Segurança da Informação, a gerência deve definir três tipos de política de segurança da informação:

Política de um programa de segurança da informação organizacional ou empresarial

Políticas de segurança de informações específicas por problemas

Políticas de segurança de informações específicas por sistemas

Introdução a Política de Segurança da Informação

Deve ser redigida de forma clara para que seja apresentada à direção da empresa.

Deve sempre estar ligada às estratégias de negócio da organização.

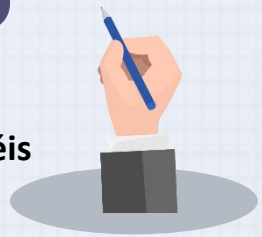
Estar de acordo com as regulamentações, legislações e outros contratos.

Deve garantir que há meios para tratar as ameaças no momento atual e a longo prazo.

Deve conter as formas de lidar com imprevistos e exceções.

Política de segurança da informação

Nomear e indicar os papéis gerais e específicos.



Deve ser autoexplicativa.

Políticas de Segurança da Informação

Prover uma orientação e suporte a direção da organização quanto à segurança da informação, de acordo com os requisitos do negócio, com as leis e regulamentações relevantes.

A implementação deve ocorrer primeiramente em "alto nível", com a definição de uma política de segurança da informação a ser aprovada pela direção.

1. **Controle de acesso;**
2. **Classificação de informações;**
3. **Segurança física e do ambiente;**
4. **Tópicos ligados ao usuário final;**
5. **Backups;**
6. **Transferência de informações;**
7. **Proteções contra malwares;**
8. **Gerenciamento de vulnerabilidades;**
9. **Criptografia;**
10. **Segurança da comunicação;**
11. **Privacidade e proteção de informações pessoais;**
12. **Relações com fornecedores.**

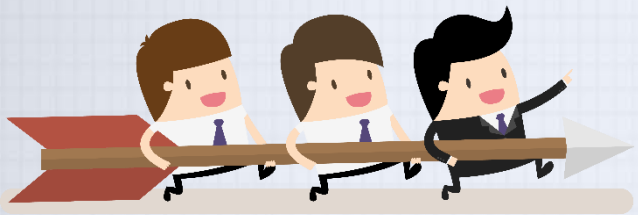
Políticas de Segurança da Informação

- Precisam ser revisadas em intervalos pré-determinados ou sempre que mudanças significativas ocorrerem no contexto, para garantir eficácia, adequação e disponibilidade.
- A revisão deve incluir oportunidades de melhorias e as respostas à modificações do ambiente organizacional, circunstâncias de negócio, mudanças técnicas e legais.

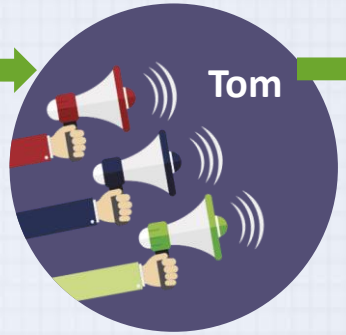
Existem algumas abordagens comuns para a criação e gerenciamento de uma Política de Segurança da Informação específica:

- Criar um número de documentos independentes da Política de Segurança da Informação, cada um adaptado a um assunto específico;
- Criar um único documento abrangente da Política de Segurança da Informação que vise cobrir todas as questões;
- Criar um documento modular da Política de Segurança da Informação que unifica a criação e administração de políticas, mantendo os requisitos de cada questão específica.

Política de Segurança da Informação Organizacional



Direção Estratégica



Atribuir as responsabilidades para as várias áreas da segurança da informação.

Orientar as necessidades de desenvolvimento, implementação e gerenciamento do programa de segurança da informação.

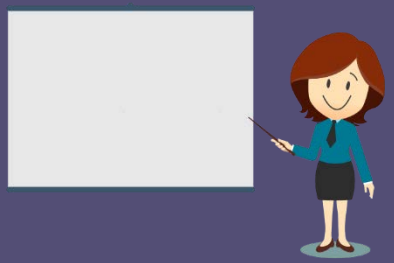
Políticas de Segurança da Informação Organizacional (PSIO) – ELEMENTOS:

- Uma visão geral da filosofia corporativa sobre segurança;
- Informação sobre a estrutura da organização de segurança da informação e indivíduos que cumprem o papel de segurança da informação;
- Responsabilidades de segurança que são compartilhadas por todos os membros da organização;
- Responsabilidades de segurança que são exclusivas para cada função dentro da organização.

Política de Segurança da Informação Organizacional

Uma PSIO deve conter também alguns componentes, como:

Declaração de Propósito



Elementos de segurança da tecnologia da informação

Necessidade de Segurança da Tecnologia da Informação

Referência a Outras Normas e Diretrizes de Tecnologia da Informação

Responsabilidades e Funções de Segurança da Tecnologia da Informação

Exemplo de um PSIO

Proteção da Informação

Uso de Informações

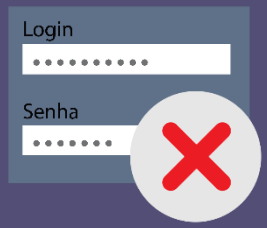
Manipulação de Informação, Acesso e Uso

Isenção de Responsabilidade de Danos contra os Dados e Programas

Conflitos Legais

Violação de Direito

Revogação de Privilégios de Acesso



Padrões de segurança de informações específicos de um setor

Uso de Políticas e Procedimentos de Segurança da Informação

Exigibilidade de Controles de Segurança

Comunicar e Reavaliar

As empresas adotam nomes similares para POLÍTICA:

- **Normas**
- **Regras**
- **Diretrizes**

Apresentar de forma assimilável a todos os colaboradores da organização, através, por exemplo, de sessões de treinamento

É importante criar um calendário de reavaliação da política e rever as medidas caso aconteça mudanças importantes.

Isto serve para avaliar se ainda está tudo funcionando corretamente, se ainda é adequado manter como está, ou se é hora de mudar alguma coisa.

Políticas, Documentos, Procedimentos e Processos

Política → **É um conjunto de medidas, estas medidas podem ter processos e procedimentos diferentes.**

Política → É a regra que se aplica.

Procedimento → É "como" se faz.

Política é diferente de procedimentos. → **O procedimento é uma forma bem explicada de fazer alguma atividade ou um processo.**

EX.: Política de segurança que descreve sobre a privacidade dos funcionários.

- Um procedimento nem sempre precisa estar documentado. **"Procedimento documentado".**
- Um **processo** é um conjunto de atividades que normalmente estão relacionados.
- Um **documento** é onde está escrito o procedimento, o processo ou a política da empresa.
- A Política de Segurança da Empresa é um Documento que contém os Processos e Procedimentos de um Sistema de Gerenciamento de Segurança da Informação (SGSI).

Exemplos de Políticas

- Política de segurança da informação;
- Política de controle de acesso;
- Política de classificação da informação;
- Política de dispositivo móvel;
- Política para teletrabalho (*teleworking*);
- Uso de redes e serviços de redes;
- Política no uso de controles criptográficos;
- Política de mesa e tela limpa;
- Política que proíbe o uso de software não autorizado;
- Política de Backup;
- Política de retenção de gravações;
- Política sobre quais tipos de software os usuários devem ou podem instalar;
- Política para uso de instalações de comunicação;
- Política de desenvolvimento seguro;
- Política de segurança da informação para relações com fornecedores;
- Política de conformidade IPR *(Intellectual property rights)* – Direitos Propriedade Intelectual;
- Política para manutenção das condições de licença;
- Política para eliminação ou transferência de software;
- Política para proteção da privacidade de dados.

Desenvolvendo Procedimentos

Não é necessário criar um procedimento específico para absolutamente tudo na empresa.

É importante redigir um procedimento para algo que poucas pessoas conhecem.

- Se estes profissionais se ausentarem e a empresa mantiver atualizado este "manual" ou procedimento, o ambiente de produção não sofrerá interrupções ou quedas de qualidade.
- Quando o processo é muito complicado e o erro pode ser custoso, a criação do procedimento faz total sentido.
- Quando o processo é muito longo e exige etapas bem elaboradas.

Processo de Continuidade de Negócio

Processo de Continuidade de TI

O grande desafio está em criar um número mínimo de procedimentos que sejam comum a todos.

Exemplos de Procedimentos

- Procedimento para contatos com autoridades;
- Procedimentos para casos de perda ou roubo de dispositivos móveis;
- Procedimentos para prevenção de disputas de direitos de Propriedade Intelectual;
- Procedimentos para backup e continuidade de negócios;
- Procedimentos para planejamento, relatórios, registros, manuseio evidências forense, avaliação e resposta na segurança da informação;
- Procedimentos para manuseio e classificação de informação;
- Procedimentos para manuseio de ativos e mídia;
- Procedimentos para eliminação e descarte de mídias;
- Procedimentos para transferência física de mídia;
- Procedimentos de autorização (exemplo, como a verificando de identidades);
- Procedimentos para proteger o acesso a conexões e serviços da rede;
- Procedimentos para prevenir o uso não autorizado de IDs administrativos;
- Procedimentos seguros para login;
- Procedimentos de autorização para programas utilitários;
- Procedimentos de acesso para programar códigos de fonte/bibliotecas;
- Procedimentos para uma mudança;
- Procedimentos para sistema de controle de mudança;
- Procedimentos para gerenciamento de sistema;
- Procedimentos para trabalhar em áreas seguras;

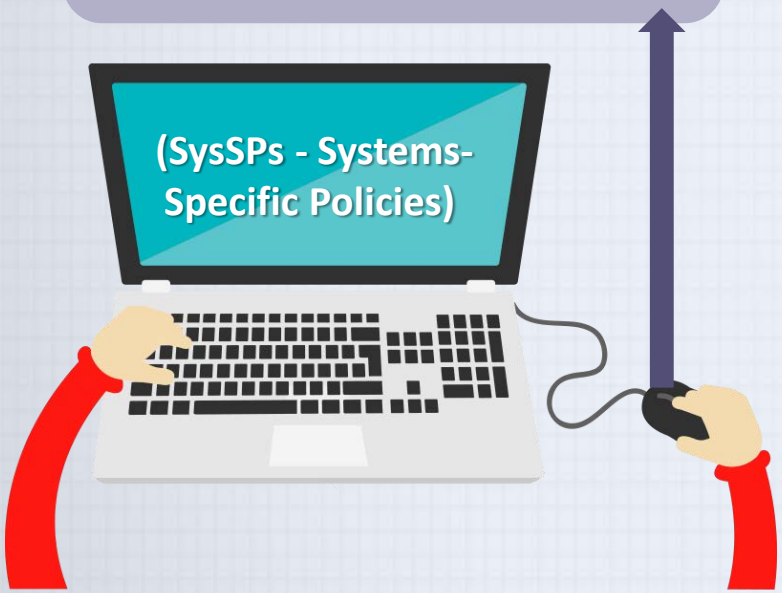
Exemplos de Procedimentos

- Procedimentos para proteger equipamentos;
- Procedimentos operacionais;
- Procedimentos de reiniciação e recuperação;
- Procedimentos de monitoramento;
- Procedimentos para lidar com proteção de malware;
- Procedimentos de backup e restauração;
- Procedimentos para instalação de software em sistemas operacionais;
- Procedimentos para reação a incidente de informação
- Procedimentos para gerenciamento de equipamentos em rede ;
- Procedimento para transferência de informação;
- Procedimentos para garantir rastreabilidade e não repúdio (repúdio é uma garantia que evita o autor negar algo que ele fez);
- Procedimentos para aplicação de controle e integridade;
- Procedimentos para desenvolvimento seguro;
- Procedimentos para a proteção de dados de teste;
- Procedimentos para monitorar aderência dos fornecedores às políticas;
- Procedimentos para garantir o nível exigido de continuidade para a segurança;
- Procedimentos para armazenagem e manuseio (para proteção de gravações);
- Procedimentos para proteção de privacidade.

Políticas Específicas de Sistema

Ou combinando esses dois tipos de conteúdo SysSP em um único documento de política.

Guia de Gerenciamento e Especificações Técnicas.



Guia de Gerenciamento:

É criado pela gerência para orientar a implementação e configuração da tecnologia, bem como abordar o comportamento das pessoas na organização de forma a apoiar a segurança da informação.

Especificações Técnicas do SysSPs:

Enquanto um gerente pode trabalhar com um administrador de sistemas para criar diretiva de gerenciamento, conforme especificado anteriormente, no **Guia de Gerenciamento**, o administrador do sistema pode precisar criar um tipo diferente de diretiva para implementar a diretiva de gerenciamento.

Política de Segurança Específica

Uma política de segurança específica eficaz deve:

- Articular as expectativas da organização sobre como o sistema em questão deve ser usado;
- Documentar como o sistema baseado em tecnologia é controlado; identificar os processos e autoridades que fornecem esse controle;
- Servir para indenizar a organização em relação a responsabilidade pelo uso inapropriado ou ilegal do sistema de um funcionário.

A Política específica de cada organização deve:

- Endereçar os sistemas específicos baseados em tecnologia;
- Exigir atualizações frequentes;
- Conter uma declaração sobre a posição da organização sobre uma questão específica.

Política de Segurança Específica

Os tópicos de uma política específica podem incluir:

- Correio eletrônico
- Utilização da Internet
- Configurações mínimas específicas em computadores para defesa contra *worms* e vírus
- Proibições contra hackear
- Testes dos controles de segurança da organização
- Uso de equipamento de fotocópia
- Uso de tecnologias de telecomunicações
- Uso de equipamentos pessoais em redes de empresas
- Utilização doméstica dos equipamentos de TI de propriedade da empresa

Componentes de uma Política de Segurança Específica

- Declaração de Propósito:
  - ✓ Escopo e a Aplicabilidade;
  - ✓ Definição de Tecnologia;
  - ✓ Responsabilidades.
- Acesso e o Uso Autorizado de Equipamentos
  - Acesso do usuário
- Uso correto e responsável
- Proteção da privacidade
- Uso Proibido de Equipamento:
  - ✓ Mau uso;
  - ✓ Uso Criminal;
  - ✓ Materiais ofensivos ou de assédio;
  - ✓ Direitos autorais, licenciamento ou outras proteções de Propriedade Intelectual;
  - ✓ Outras restrições.
- Gerenciamento de Sistemas:
  - ✓ Gerenciamento de Materiais Armazenados;
  - ✓ Monitoramento do empregador;
  - ✓ Proteção contra vírus;
  - ✓ Segurança física;
  - ✓ Criptografia.

Componentes de uma Política de Segurança Específica

- **Violações da Política:**
  - ✓Procedimentos para relatar violações;
  - ✓Sanções por Violações.
- **Revisão e Modificação de Políticas:**
  - ✓Revisão Agendada da Política;
  - ✓Procedimentos para Modificação.
- **Limitações de Responsabilidade:**
  - ✓Declarações de Responsabilidade;
  - ✓Outras isenções.

Organização da Segurança da Informação

ISO/IEC 27002

Sugere a o estabelecimento de uma organização interna.

É estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação da segurança da informação dentro da organização.

Distribuição das responsabilidades e funções dentro da segurança da informação.

Pode ser aplicado um controle para garantir que todas as responsabilidades pela segurança da informação estejam claramente definidas e todas as funções estejam atribuídas previamente.

Organização da Segurança da Informação

Exemplo: Não pode ser concedida a uma pessoa a permissão de acesso à informação, se ela não tiver este direito. Nem delegar um segredo de negócio a alguém com perfil não confiável ou apto para isso.

- As reponsabilidades devem estar claramente definidas e os processos, além de bem detalhados, devem ser seguidos, incluindo os procedimentos.
- Deixar claro as responsabilidades pelas atividades do gerenciamento dos riscos de segurança da informação e definir a aceitação dos riscos residuais.
- Formalizar a organização interna da segurança da informação através da criação de um **manual**.
- Definir as responsabilidades locais para a proteção dos ativos e o tratamento frente a um incidente.
- É ideal que todos os documentos estejam sempre juntos. Os níveis de autorização de acesso às informações devem estar bem definidos e documentados.

Diretrizes para o Desenvolvimento de Políticas

1 Projetar e desenvolver a política, ou ainda, redesenhar e reescrever uma política desatualizada.

2 É estabelecer processos de gerenciamento para perpetuar a política dentro da organização, exigindo aderência às boas práticas de negócios.

Planejado

Financiado

Gerenciado

Para garantir que ele seja concluído dentro do prazo e do orçamento esperado.

SecSDLC - Secure Software Development Lifecycle - o Ciclo de Vida de Desenvolvimento de Software Seguro.

4 fases

- **Investigação;**
- **Análise;**
- **Desenho;**
- **Implementação;**
- **Manutenção.**

SecSDLC - Ciclo de Vida de Desenvolvimento de Software Seguro

Fase de Investigação

Durante essa fase a equipe de desenvolvimento de políticas deve completar as seguintes atividades:

- Obter apoio da alta administração;
- Suportar e se envolver ativamente na gestão de TI, especificamente o CIO;
- Articular claramente as metas;
- Participação dos colaboradores corretos nas comunidades de interesse afetadas pelas políticas recomendadas;
- A equipe deve incluir representantes de outras áreas como o Jurídico, Recursos Humanos e usuários finais ...
- A equipe precisará de um *Sponsor* (responsável) pelo projeto com autoridade suficiente para realizar os objetivos dele;
- A equipe também precisará de um gerente de projeto capaz de acompanhar o projeto até a sua conclusão;
- Obter uma descrição detalhada do escopo do projeto de desenvolvimento de políticas e de estimativas sólidas para o custo e o prazo do projeto.

SecSDLC - Ciclo de Vida de Desenvolvimento de Software Seguro

Fase de Análise

A fase que deve incluir as seguintes atividades:

Uma nova, ou atualização da avaliação de risco ou de auditoria de TI, documentando as necessidades atuais de segurança da informação.

Reunião de muitos materiais de referência essenciais, incluindo quaisquer políticas existentes, além dos itens mencionados acima.

Fase de Desenho

Deve incluir as seguintes atividades:

- Um projeto e um plano informando como as políticas serão distribuídas;
- Especificar qualquer ferramenta automatizada utilizada para a criação e gestão dos documentos de política;
- Revisão dos relatórios de análise de viabilidade com base nos melhores custos e benefícios.

SecSDLC - Ciclo de Vida de Desenvolvimento de Software Seguro

Fase de implementação

A equipe de desenvolvimento de políticas zelará pela redação das políticas. Os recursos disponíveis para isso podem incluir:

- Conteúdo na Internet;
- Sites do governo;
- Literatura profissional;
- Diversos autores;
- Consultores profissionais;
- Certifique-se de que as políticas podem ser executadas;
- A distribuição de políticas nem sempre é tão simples como se pode pensar;
- A política efetiva deve ser escrita em um nível de leitura razoável e tentando minimizar jargões técnicos e terminologias de gerenciamento.

Fase de manutenção

Durante a fase de manutenção, a equipe de desenvolvimento de políticas irá monitorar, manter e modificar a política conforme necessário para garantir que ela permaneça efetiva, de forma que seja usada como uma ferramenta para atender as ameaças em constante mudança.

ISPME – Abordagem Fácil

- Coleta de materiais de referência;
- Definição de um Framework (estrutura ou modelo) para Políticas;
- Preparação de uma Matriz de Cobertura;
- Tomar decisões de desenho de Sistemas Críticos;
- Estruturar o processo de revisão, aprovação e execução.

- Publicar as Políticas na Intranet ou equivalente;
- Desenvolver um questionário de autoavaliação;
- Desenvolver testes para determinar se os colaboradores compreendem as políticas;
- Atribuir coordenadores de Segurança da Informação;
- Treinar coordenadores de Segurança da Informação;
- Preparar e entregar um curso básico de segurança da informação;
- Desenvolver políticas de segurança de informações de aplicativos específicos;
- Atribuir custódia e propriedade da Informação;
- Estabelecer um Comitê de Gerenciamento de Segurança da Informação;
- Desenvolver um documento de arquitetura de segurança da informação.

Checklist ISPME

- ✓ Realizar uma avaliação de risco ou auditoria de tecnologia da informação para determinar as necessidades de Segurança da Informação (SI);
- ✓ Esclarecer o que significa a palavra "política" dentro de sua organização;
- ✓ Assegurar que as funções e responsabilidades relacionadas com a SI estejam claras;
- ✓ Convencer a gestão que é aconselhável manter as políticas de SI documentadas;
- ✓ Identificar os colaboradores da alta administração que aprovarão o documento final de SI, além de identificar todos os revisores influentes;
- ✓ Coletar e ler todo o material existente internamente sobre conscientização de SI;
- ✓ Conduzir uma breve pesquisa interna a fim de reunir ideias das partes interessadas, para incluir em uma nova (ou atualizada) política de SI;
- ✓ Examinar outras políticas emitidas pela sua organização, como as da gestão de Recursos Humanos, para identificar o formato, o estilo e as referências;
- ✓ Identificar o público-alvo que receberá o conteúdo da política de SI e determinar se eles receberão um documento separado ou uma página no site;
- ✓ Determinar até que ponto o público é alfabetizado, informado e receptivo às mensagens de segurança;
- ✓ Decidir se outros esforços de conscientização devem ocorrer antes que as políticas de SI sejam publicadas;

Checklist ISPME

- ✓ Usar as ideias da avaliação de risco e preparar e comunicar as políticas através de uma mensagem;
- ✓ Determinar como o conteúdo da política será divulgado, observando os constrangimentos e implicações de cada meio de comunicação;
- ✓ Revisar os processos de avaliação de conformidade para garantir que todos possam trabalhar sem problemas com o novo documento;
- ✓ Determinar se a quantidade de mensagens é muito alta para serem tratadas de uma só vez, e, caso afirmativo, identificar diferentes categorias de conteúdo que serão publicadas em momentos diferentes;
- ✓ Ter um esboço dos tópicos que serão incluídos no primeiro documento revisto por várias partes interessadas;
- ✓ Com base nos comentários das partes interessadas, rever o esboço inicial e preparar um primeiro rascunho;
- ✓ Ter o primeiro rascunho de documento revisto pelas partes interessadas com reações iniciais, sugestões de apresentação e ideias de implementação;
- ✓ Rever o projeto em resposta aos comentários das partes interessadas;
- ✓ Solicitar aprovação da política da alta direção;
- ✓ Desenvolver um plano de conscientização que use o documento de política como uma fonte de ideias e requisitos;
- ✓ Redigir as lições aprendidas e o que precisa ser corrigido....

SP 800-18: Guia para Desenvolvimento de Planos de Segurança

NIST 800-18

- **Políticas** são **documentos vivos** que mudam e crescem constantemente, por isso, devem ser divulgadas, distribuídas, lidas, entendidas, acordadas. Em resumo: geridas.

As políticas devem ter:

- Uma pessoa responsável pelas revisões;
- Um cronograma de revisões;
- Um método para fazer recomendações para revisões;
- Datas de revisão.

Pronto para o próximo?

Curso Preparatório para Certificação
Em Gestão de Segurança da Informação Avançada – Baseada na ISO/IEC 27002:2013

Área de Aprendizagem

www.pmgacademy.com

Official Course

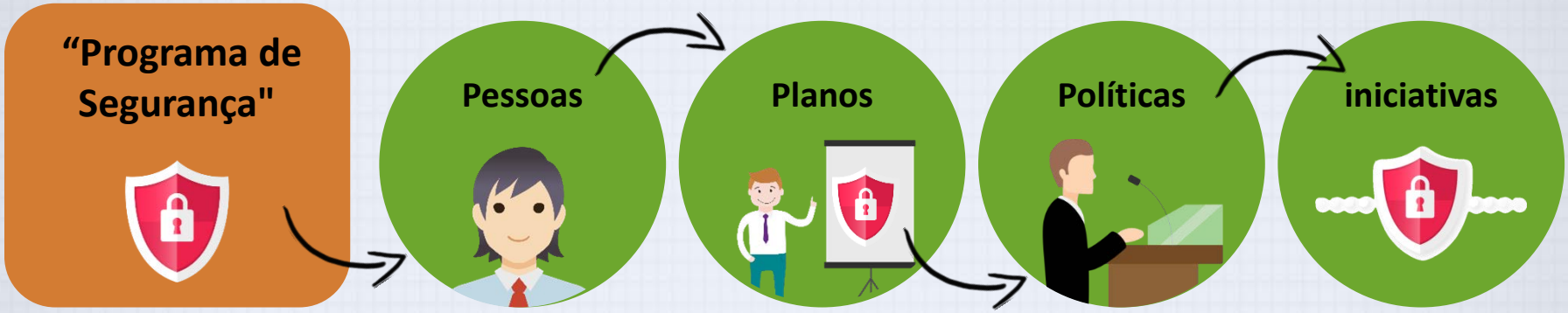
Módulo 7

Programa de Segurança

Resumo

- Como definir uma política de segurança da informação e compreender o seu papel central num programa bem sucedido de segurança da informação.
- Como desenvolver, implementar e manter vários tipos de políticas de segurança da informação.
- Explorar as diversas abordagens para a segurança da informação e fornecer uma explicação dos componentes funcionais de um programa de segurança da informação.
- Planejar um programa de segurança da informação com base em seu tamanho e outros fatores; bem como a forma de avaliar os fatores internos e externos que influenciam as atividades e a organização.
- Identificar e descrever os títulos e funções típicas desempenhadas no programa de segurança da informação.
- Abordar temas como um programa de educação, treinamento e conscientização sobre segurança.

Programa de Segurança



Variáveis:

- Cultura organizacional;
- Tamanho;
- Orçamento com o pessoal envolvido na segurança;
- Orçamento em segurança.

Funções na Segurança da Informação

Critérios:

- Controle da organização;
- Lei da oferta e a demanda dos diferentes níveis de habilidades e experiência.

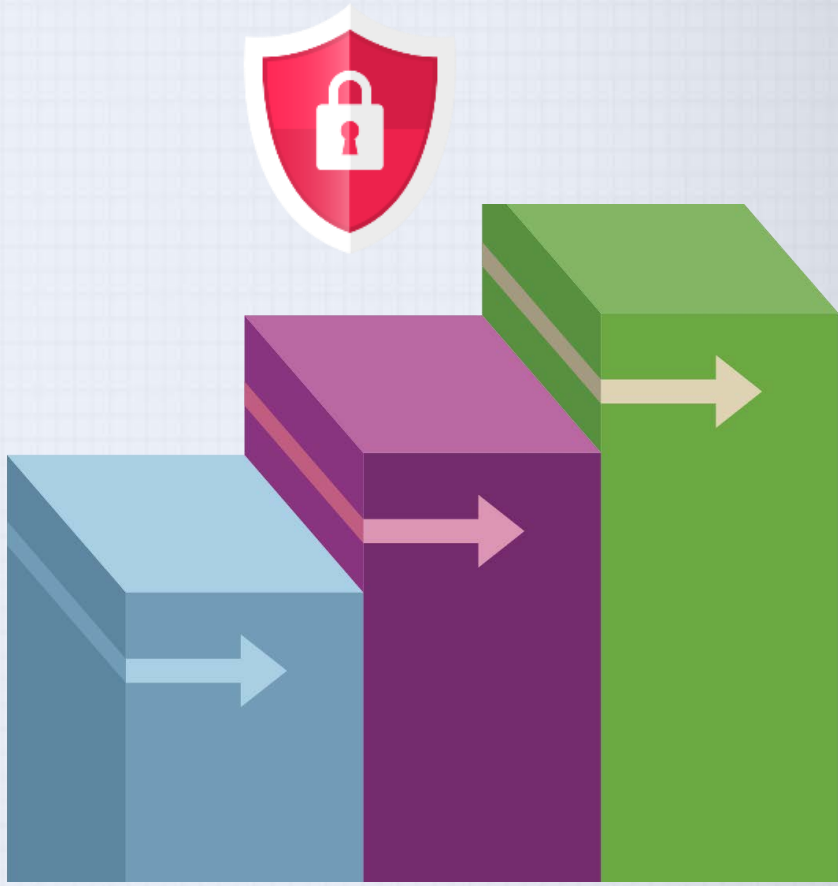
EX.:

Profissionais experientes em ERP na década de 1990.

Programadores **COBOL** experientes no início do século XXI, devido a preocupações com questões relacionadas ao *bug* do milênio.

Qualificações e Requisitos

- A comunidade de gestores em geral deve aprender mais sobre os requisitos e qualificações para ambas posições de segurança da informação e TI;
- A alta administração deve aprender mais sobre as necessidades de orçamento da equipe de segurança da informação.
- As comunidades de TI e de gestão geral devem conferir à função de segurança da informação a principal responsável pela segurança da informação com um nível adequado de influência e prestígio.

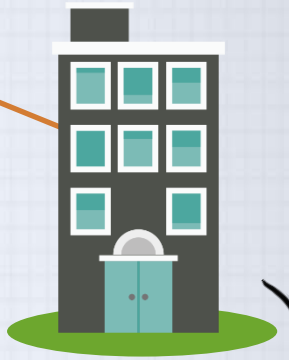


Qualificações e Requisitos

- Compreender como as organizações são estruturadas e operadas;
- Reconhecer que a segurança da informação é uma tarefa de gerenciamento...;
- Trabalhar bem com as pessoas em geral;
- Reconhecer o papel da política na orientação dos esforços de segurança;
- Compreender o papel essencial da educação e da formação em relação a segurança da informação;
- Perceber as ameaças enfrentadas por uma organização;
- Entender como os controles técnicos podem ser aplicados para resolver problemas específicos;
- Demonstrar familiaridade com as principais tecnologias de informação;
- Compreender a terminologia e os conceitos de TI e da Segurança da Informação.

Posições na Área de Segurança da Informação

- Rede;
- Programação;
- Administração de banco de dados;
- Administração de sistemas.



As organizações podem promover um maior profissionalismo na disciplina de segurança da informação, definindo claramente suas EXPECTATIVAS e estabelecendo DESCRIÇÕES EXPLÍCITAS DE CARGOS.

As três áreas da Segurança da Informação são:

As que definem;	As que constroem;	As que administram.

- Os definidores fornecem as políticas, diretrizes e padrões.
- Os controladores são os verdadeiros técnicos, que criam e instalam soluções de segurança.
- As pessoas que operam e administram as ferramentas de segurança e de monitoramento de segurança...

Estrutura da Organização

Definição dos **papéis** e **responsabilidades** das pessoas envolvidas.

Isto implica que esses termos sejam descritos em:

- Manuais de RH
- Contratos de trabalho
- Manuais de funcionários
- Descrições de cargos e salários; e etc.

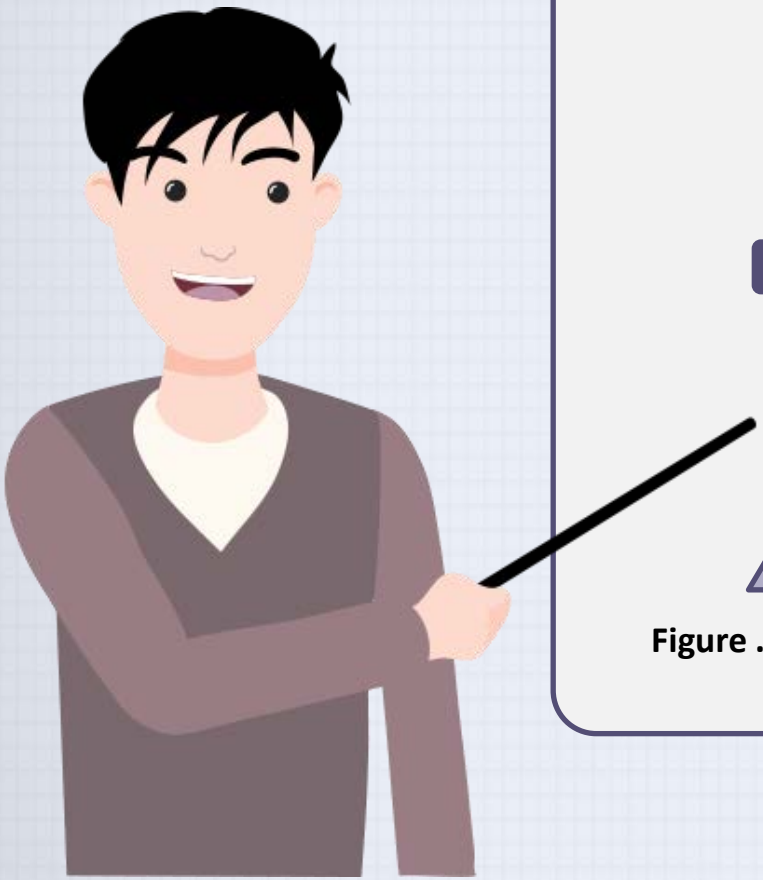
É projetar a governança da segurança da informação, incluindo suas relações de trabalho com outras funções relacionadas e com a alta administração.

O líder precisa ter visão estratégica, empatia, capacidade de se comunicar efetivamente com outros gerentes sêniores, integridade pessoal e, claro, competência profissional na disciplina de gestão.

1ª O nível de abstração: estratégia, tática ou operacional.

2ª Considera as disciplinas envolvidas.

Nível de Abstração da Organização



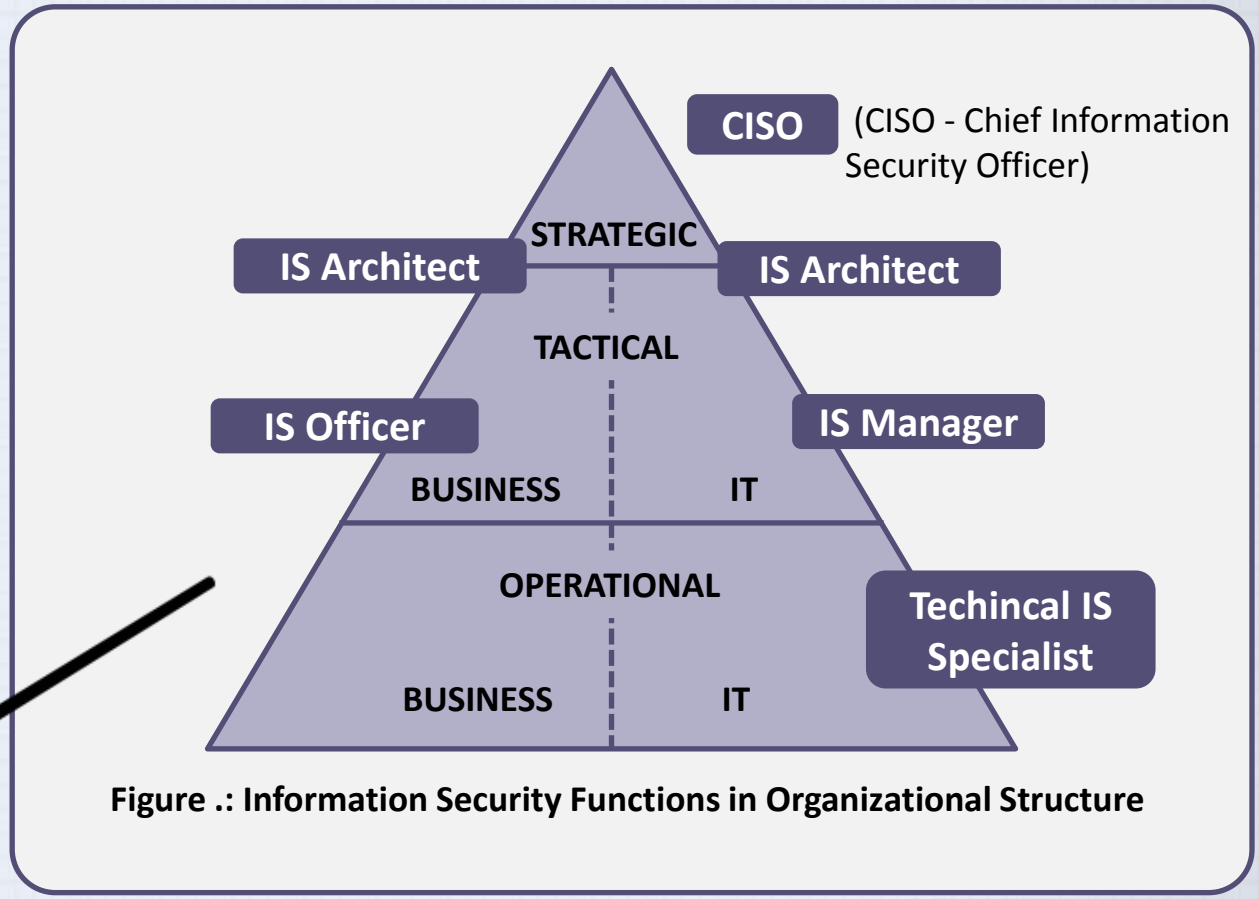


Figure .: Information Security Functions in Organizational Structure

Funções e Títulos de Segurança da Informação

Diretor de Segurança da Informação (CISO)

Gerentes de segurança

Administradores e analistas de segurança

Técnicos de segurança

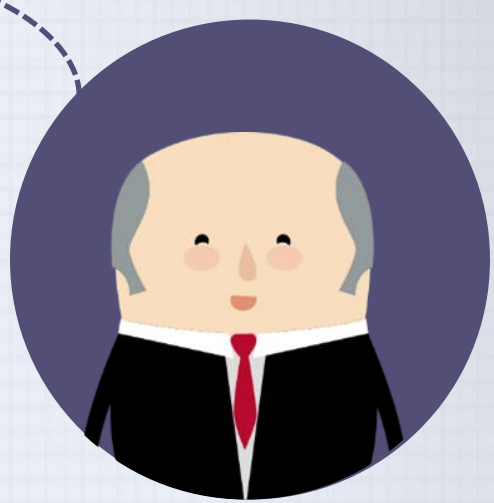
Funcionário de segurança

Há a necessidade de treinamento especializado.

Central de Serviços

CISO

É considerado o chefe da Segurança da informação na organização.



O CISO geralmente não está em uma posição de nível executivo e frequentemente relata ao CIO.

Devem estar familiarizados com todas as áreas de segurança da informação, incluindo tecnologia, planejamento e política.

Deverá elaborar ou aprovar uma série de políticas de segurança da informação.

Ele trabalha com o CIO no planejamento estratégico, desenvolve planos táticos e trabalha com gerentes de segurança no planejamento operacional.

É o porta-voz da equipe de segurança e é responsável pelo programa geral de segurança da informação.

Desenvolve orçamentos de segurança da informação com base no financiamento disponível e toma decisões ou recomendações sobre compras, implementação de projetos e tecnologia, recrutamento, contratação e demissão de pessoal de segurança.

Gerente de Segurança

- **São responsáveis pela operação diária do programa de segurança da informação.**
- **Executam os objetivos identificados pelo CISO e resolvem questões identificadas pelos técnicos.**
  - Desenvolvimento de políticas;
  - Avaliação de riscos;
  - Planejamento de contingência;
  - Planejamento operacional e tático para a função de segurança.
- **Trabalham em conjunto com gerentes de outros departamentos.**
- **Tem a função de contratar e demitir recursos humanos, atuar na operações, no controle do ambiente e no projeto de segurança física.**

Administradores de sistemas são tecnicamente proficientes na tecnologia usada pelos sistemas que trabalham. São responsáveis por garantir que os sistemas sejam usados de acordo com as políticas da organização. Podem ter algumas funções de gestão, mas não são responsabilizados como gerentes.

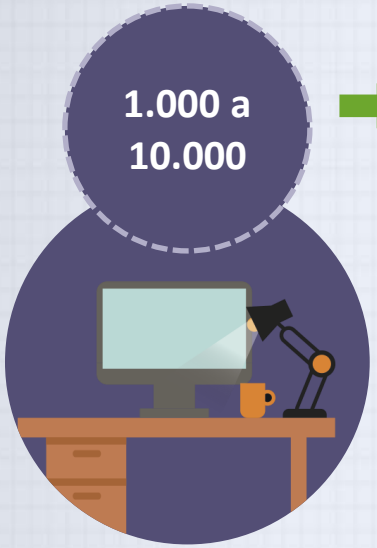
Técnicos de Segurança

- São as pessoas tecnicamente qualificadas que configuram firewalls e IDSs, implementam software de segurança, diagnosticam e solucionam problemas e coordenam-se com os administradores de sistemas e administradores de rede para garantir que a tecnologia de segurança seja devidamente implementada.

- Devem ser especializados, focar em um grupo de segurança principal (firewalls, IDS, servidores, roteadores e software), e depois se especializar em pacotes de software ou hardware específicos dos fornecedores deste tipo.

- Os técnicos de segurança que desejam subir na hierarquia da empresa devem expandir horizontalmente o seu conhecimento técnico e obter uma compreensão geral da organização da segurança da informação, bem como todas as áreas técnicas.

Segurança em Grandes Organizações



Tendem a formar grupos internos para enfrentar desafios de longo prazo, mesmo que já lidem com operações de segurança do dia-a-dia.

- Os orçamentos de segurança tendem a crescer mais rápido do que os orçamentos de TI. Mesmo com um enorme orçamento, o valor médio por usuário é ainda menor do que qualquer outro tipo de organização.

- A abordagem da segurança deve amadurecer, integrando o planejamento e a cultura na política.

- Elas tendem a gastar substancialmente menos em segurança (apenas cerca de **5% do orçamento total de TI** em média) criando problemas em toda a organização.

- Cultura;
- Do tamanho;
- Do orçamento disponível.

Outras Posições

Grupo de Segurança da Informação:

- Gerente de departamento Segurança da Informação (InfoSec);
- Administrador do sistema de controle de acesso;
- Consultor Internai de InfoSec;
- Engenheiro de InfoSec;
- Especialista em documentação de InfoSec;
- Planejador de contingência da InfoSys;
- Coordenador Local de InfoSec.

Outras Posições

Grupo de TI:

- Diretor de informação;
- Analista de Negócios / Analista de Sistemas;
- Programador de sistemas;
- Programador de aplicações de Negócios;
- Gerente de Operações de Computador;
- Operador de computador;
- Analista de garantia de qualidade de Sistemas;
- Analista de Central de Serviços ou Help Desk;
- Gerente de arquivos / registros;
- Gerente de telecomunicações;
- Administrador de sistemas / administrador de rede;
- Administrador de site / administrador do site de comércio;
- Administrador de banco de dados;
- Gerente de administração de dados.

Outras Posições

- Gerente do departamento de segurança física;
- Especialista em proteção de ativos físicos;
- Guarda e segurança física;
- Profissional de manutenção de escritório;
- Gerente de departamento de auditoria interna;
- Auditor de processamento de dados;

Grupo de negócios em geral:

- Advogado especialista em propriedade...;
- Gerente de departamento de recursos humanos;
- Consultor de recursos humanos;
- Recepcionista;
- Administrador de contrato de terceirização;
- Treinador interno;
- Gerente do departamento de seguros...;
- Analista de Seguros e gerenciamento de riscos;
- Planejador de contingência de negócios;
- Gerente de Relações Públicas;
- Diretor financeiro;
- Agente de compra;
- Diretoria Executiva.

Áreas de Segurança

Para grandes organizações é recomendado separar as funções em quatro áreas:

1. Funções desempenhadas por unidades de negócio não tecnológicas, fora do domínio da tecnologia da informação, como as áreas de gerenciamento, tais como:

EX.: Departamentos Legais, de Treinamento, etc.

2. Funções desempenhadas por grupos de TI fora da área de segurança da informação como áreas de gerenciamento, tais como:

- Administração de segurança de sistemas;
- Administração de segurança de rede;
- Autenticação centralizada.

3. Funções desempenhadas pelo departamento de segurança da informação, atuando como um serviço ao cliente para a organização e seus parceiros externos, como:

- Avaliação de risco;
- Planejamento;
- Teste de sistemas;
- Medição;
- Resposta a incidentes;
- Avaliação de vulnerabilidade.

4. Funções desempenhadas no escopo de um departamento de segurança da informação com obrigação de atender:

- Política; Conformidade e Gerenciamento de riscos

Áreas de Segurança

Que verifica se as funções de segurança da informação são adequadamente executadas em algum lugar dentro da organização.

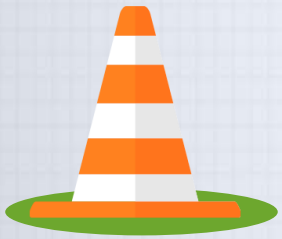
A implantação do pessoal de segurança em tempo integral depende de uma série de fatores, incluindo a sensibilidade da informação que deve ser protegida, os regulamentos da indústria e a rentabilidade geral da empresa.

CISO (Chief Information, Security Officer)

Segurança em Médias Organizações

Orçamento menor, ou seja, aproximadamente 11% do orçamento de TI.

Deve confiar na ajuda da equipe de TI para por em prática os planos de segurança. Sua capacidade de definir políticas, lidar com incidentes de forma regular e efetivamente alocar recursos são, em geral, piores do que qualquer outro grupo.



- Cerca de 70% das organizações deste porte sofreram danos por violações de segurança...
- ... Um aumento de 48% em relação às pequenas organizações.
- Podem ser grandes o suficiente para implementar a abordagem multicamadas de segurança.

Segurança em Pequenas Organizações

10 e 100

- E possui um modelo organizacional de TI centralizado e simples.
- Gasta desproporcionalmente mais em segurança, quase 20% do orçamento total de TI.

Seguem pouco uma política formal, planejamento ou medidas de segurança, e geralmente terceirizam sua presença na Web ou operações de comércio eletrônico, por exemplo.

Treinamento de segurança e conscientização é comumente realizado em uma base 1-em-1, ou seja, o administrador de segurança fornecendo aconselhamento diretamente aos usuários, conforme necessário.

Quaisquer políticas provavelmente serão políticas específicas de tratamento de problemas.

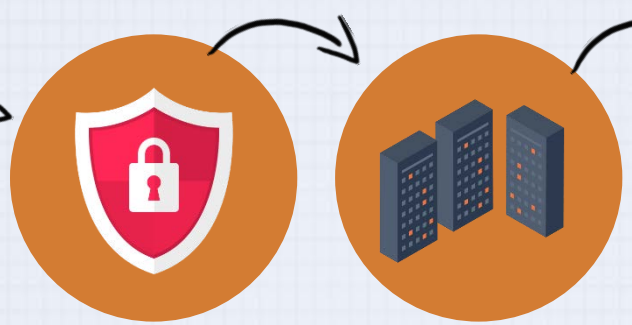
O planejamento formal é geralmente parte do planejamento de TI conduzido pelo CIO.

Vantagem: pequenas organizações evitam algumas ameaças justamente em virtude do seu tamanho.

Ameaças de pessoas que têm informações da organização também são menos prováveis em um ambiente onde cada funcionário sabe tudo dos outros funcionários.

Alocando a Segurança da Informação Dentro de uma Organização

Grandes organizações



Que reporta diretamente ao executivo de TI, ou CIO.

O desafio é projetar uma estrutura com relatórios para o programa Segurança da Informação que equilibre as necessidades de cada uma das comunidades de interesse.

- O gerente de segurança de nível médio deve reportar diretamente ao CEO, ou outro executivo tão alto na hierarquia organizacional, quanto possível.
- Os gerentes de outras unidades organizacionais também precisarão ter uma relação confiável com a função de segurança da informação ou de um vínculo estratégico com ela.

Alocando a Segurança da Informação Dentro de uma Organização

- **Opção 1:** A Segurança da Informação reportando ao Departamento de Tecnologia da Informação.
- **Opção 2:** A Segurança da Informação reportando a um Departamento de Segurança amplamente definido.
- **Opção 3:** A Segurança da Informação reportando ao Departamento de Serviços Administrativos.
- **Opção 4:** A Segurança da Informação reportando ao Departamento de Gerenciamento de Riscos.
- **Opção 5:** A Segurança da Informação reportando ao Departamento de Planejamento e Estratégia.
- **Opção 6:** A Segurança da Informação reportando ao Departamento Legal.

Alocando a Segurança da Informação Dentro de uma Organização

- **Opção 7:** Auditoria Interna;
- **Opção 8:** Help Desk;
- **Opção 9:** Contabilidade e Finanças através da TI;
- **Opção 10:** Recursos Humanos;
- **Opção 11:** Gerenciamento de Instalações;
- **Opção 12:** Operações.

Segurança em Recursos Humanos

Funcionários

Ao contratar um profissional de segurança da informação, certificar-se que ele tem competências necessárias e se é suficientemente confiável para desempenhar a sua tarefa.

Partes Externas

Estabelecer procedimentos, critérios e limitações onde envolve pessoas que tenham acesso aos recursos e ativos.

- Entender suas responsabilidades;
- Estarem em conformidade com seus papéis;
- De acordo com a ética da empresa;
- Regulamentações, leis;
- Questões de privacidade;
- Proteção da informação de identificação do pessoal.

As obrigações contratuais: assinatura de termos de confidencialidade ou de não divulgação, e detalhes das ações a serem tomadas no caso de desrespeito dos requisitos de segurança da informação.

Um código de conduta pode ser usado para estabelecer as responsabilidades de segurança da informação...

Segurança na Contratação e Demissão

Solicitar a todos os funcionários e partes externas que estão sendo contratados que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.

- instruídas
- conscientizadas
- treinadas
- motivadas

Antes de obter acesso às informações sensíveis ou aos sistemas de informação.

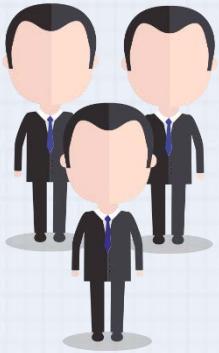
É interessante criar um canal de notificação, de forma anônima, para reportar quaisquer violações que ocorram nas políticas e procedimentos de segurança da informação.

Segurança na Contratação e Demissão

- É essencial que as cláusulas da Política de Informação estejam vigentes – e comunicadas - mesmo após as demissões ou encerramento de contrato é essencial que utilizando como apoio acordos de confidencialidade e os termos e condições de trabalho.
- A função de Recursos Humanos é geralmente responsável por todo processo de demissão e trabalha junto com o gestor do colaborador que está saindo da empresa para gerir os aspectos relevantes dos procedimentos de segurança da informação.
- No caso de um prestador de serviço fornecido por uma parte externa, este processo é feito pela parte externa de acordo com o contrato entre a organização e a parte externa.

Políticas e Práticas com o Empregado

CIO



Gestores de Segurança da Informação

Devem estabelecer um diálogo com a **equipe de RH** para que as questões de segurança da informação façam parte do processo de contratação.

- Quando uma entrevista inclui uma visita ao local, deve se evitar o acesso a sites seguros e restritos.
- Os novos funcionários devem receber como parte de sua orientação, informação detalhada sobre a segurança da informação.
- Quando estiverem prontos para começar a trabalhar, devem ser informados sobre os componentes de segurança, sobre seus direitos e responsabilidades.
- As organizações devem realizar as atividades de conscientização e treinamentos de segurança periodicamente para manter a segurança na mente dos funcionários e minimizar seus erros.

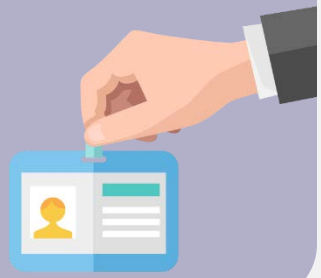
Verificação de Segurança

Uma verificação de antecedentes deve ser realizada antes que a organização ofereça uma vaga ao candidato, independentemente do nível de emprego.

Verificação de Segurança

Alguns dos tipos comuns de verificações de antecedentes são os seguintes:

- Verificações de identidade



- Verificações de educação e de credencial

- Verificação de emprego anterior

- Verificações de validade da referência e integridade das fontes de referência

- Histórico de remuneração do trabalhador

- História criminal

- História com processo civil

- Histórico de crédito

- Histórico médico

- Histórico com droga

- Registros de automóveis, suspensões e outros itens registrados

Contrato de Trabalho

O contrato de trabalho torna-se um importante instrumento de segurança.

O funcionário deve concordar por escrito.

- Estes contratos e acordos devem estar em vigor no momento da contratação, porque depois que já estiverem trabalhando corre-se o risco dos funcionários não assinarem.
- As organizações devem incorporar componentes de segurança da informação nas **avaliações de desempenho.**
- Os colaboradores prestam muita atenção nestas avaliações de desempenho, e ao incluir tarefas de segurança da informação nestas avaliações, os motivará ainda mais a terem cuidado ao executar certas tarefas.
- As organizações são obrigadas por lei a proteger informações confidenciais. Esta responsabilidade também se estende aos clientes, pacientes e qualquer pessoa com quem a organização tem relações comerciais.

Questões na Demissão

A principal delas é a continuidade da proteção de toda a informação à qual o funcionário teve acesso.

Questões na Demissão

Quando um funcionário deixa uma organização, as seguintes tarefas devem ser executadas:

- O acesso do ex-funcionário aos sistemas da organização deve ser desativado.
- O antigo funcionário deve devolver todas as mídias removíveis.
- Os discos rígidos do ex-funcionário devem ser protegidos.
- Os bloqueios aos arquivos devem ser alterados.
- As fechaduras das portas do escritório devem ser trocadas.
- O acesso do crachá do ex-funcionário deve ser revogado.
- Os bens pessoais do ex-funcionário devem ser removidos das instalações.
- O ex-funcionário deve ser escoltado das instalações.

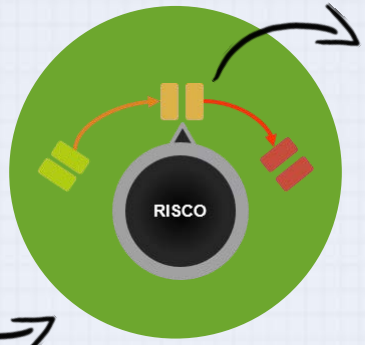
Além de realizar essas tarefas, muitas organizações realizam uma revisão geral para lembrar ao empregado de quaisquer obrigações contratuais, tais como acordos de não divulgação.

O empregado deve ser lembrado que o descumprimento das obrigações contratuais pode levar a uma ação civil ou criminal.

Métodos Para o Desligamento

Funcionário deixa a instalação imediatamente

Aviso Prévio



Dois métodos para lidar com o desligamento:

- Saída hostil (geralmente involuntária), incluindo rescisão, redução de pessoal, demissão ou desistência.
- Saída amigável (voluntária) devido aposentadoria, promoção ou realocação.

Em qualquer circunstância, as informações usadas pelos funcionários que partem, devem ser inventariadas, seus arquivos armazenados ou destruídos e todos os bens retornados.

Segregação de Funções

Segregação de Função

- Ajuda a reduzir o risco do uso incorreto, erro acidental ou proposital, das informações, ou seja, dos ativos de uma empresa.
- É o princípio básico de um sistema de controle interno que consiste na separação de funções, nomeadamente de autorização, aprovação, execução, controle e contabilização das operações.

- **Os colaboradores devem ter competências para cumprir com as tarefas a eles atribuídas. Assim, o essencial é que sejam treinadas, continuamente, para que se mantenham atualizadas.**

- Responsável por todo desenvolvimento e aplicação do plano de segurança da informação.
- Identificar quais controles usar e como apoiar estes controles.
- A responsabilidade pela pesquisa e implementação dos controles são dos gestores de cada área.

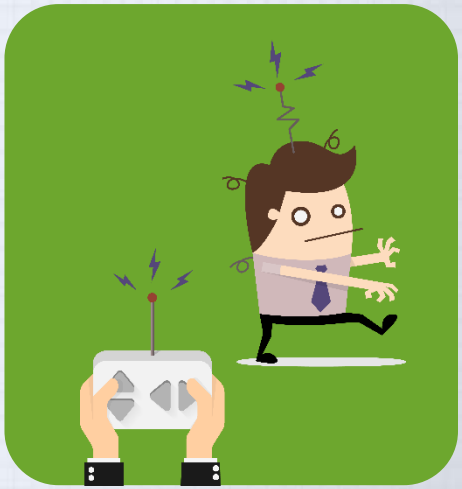
Gerente de Segurança da Informação

Considerações na Segregação de Funções

- **Para empresas menores, pode ser complicado segregar as funções, isto porque há poucas pessoas, mas de qualquer forma, ainda é preciso aplicar o principio básico, de modo que seja funcional.**

Evitar que um profissional mantenha os direitos liberados para acessar, modificar ou usar os ativos da empresa, principalmente se ele puder fazer isto sem ser rastreado, sem autorização ou sem ser detectado.

A segregação de funções pode ser usada para dificultar a violação da confidencialidade, integridade ou disponibilidade de informações.



Considerações na Segregação de Funções

Práticas de Segurança Pessoal

- Na qual todas as tarefas críticas possam ser realizadas por várias pessoas.
- A **rotação de tarefas** e a **rotação de trabalho** garantem que nenhum funcionário esteja executando ações que não possam ser revisadas por outro funcionário.

Rotação de tarefas

- Exige que cada funcionário seja capaz de realizar o trabalho de pelo menos outro funcionário.

Controle em Pares

Requer que duas pessoas revisem e aprovem o trabalho de cada um antes que a tarefa seja considerada completa.

Rotação de trabalho ou *Job Rotation*

- As chances de que duas pessoas sejam capazes de colaborar com êxito para o mau uso de um sistema são muito menores do que as chances de uma pessoa fazer.

Práticas de Segurança Pessoal

Sistema RAID Humano

- Cada empregado deve ser obrigado a tirar férias.

- Limitar o acesso à informação.
- Os funcionários devem ser capazes de acessar apenas as informações de que necessitam, e apenas pelo período necessário para executar suas tarefas.

Princípio do Privilégio Mínimo

- Assegura que não ocorra nenhum acesso desnecessário aos dados.

Segurança de Terceiros

- Pessoas que não são funcionários muitas vezes têm acesso a informações sensíveis.
- As relações com essas pessoas devem ser cuidadosamente geridas para evitar que as ameaças aos ativos da informação se materializem
- São muitas vezes expostos a uma gama de informações e podem não estar sujeitos às obrigações contratuais ou políticas gerais que são aplicados aos outros funcionários.

- Encerrar o relacionamento com o temporário.
- Encerrar o contrato com a empresa prestadora de serviços.
- Garantir que os funcionários que supervisionam os trabalhadores temporários
- Não devem sacrificar a segurança da informação.

Segurança de Terceiros

- Consultores têm seus próprios requisitos de segurança e obrigações contratuais.
- Seus contratos devem especificar seus direitos de acesso a informações e instalações.
- Lembre-se sempre de aplicar o princípio do privilégio mínimo ao trabalhar com consultores.
- Parceiros de Negócios, criados através de alianças estratégicas com outras organizações para trocar informações ou desfrutar de alguma outra vantagem mútua.

Conscientização

Nível da Conscientização

- **É preciso criar mecanismos e campanhas de conscientização dos usuários, considerando alguns fatores a respeito:**
- Usuários não gostam de ter privilégios reduzidos;
- É preciso motivação para seguir novas políticas;
- A falha geralmente não está na técnica e sim em sua aplicação;
- Atividades integradas à rotina funcionam melhor.

Aspectos devem ser considerados em um programa de conscientização:

- Conhecimento, ou seja, deve entender as regras;
- Atitude, ou seja, as pessoas devem ter uma disposição para cooperar;
- Comportamento, ou seja, obedecer as regras.

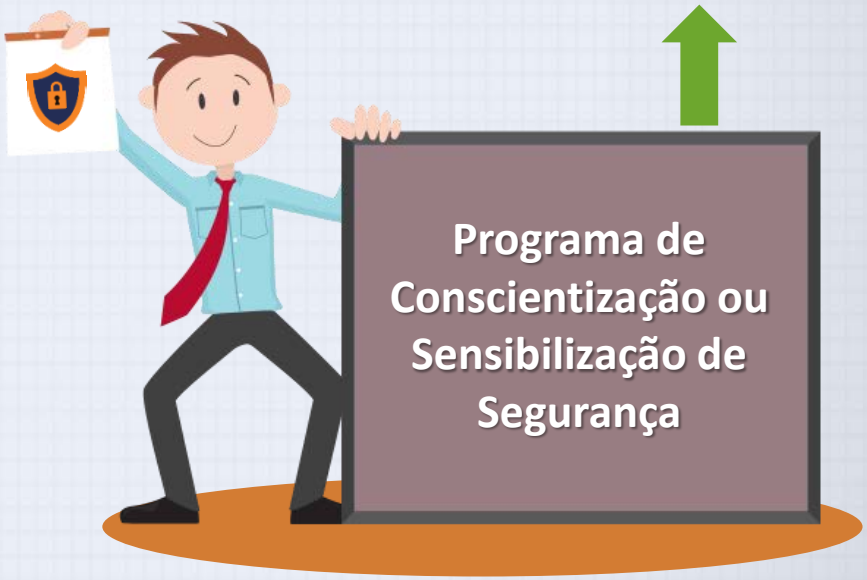
Garantir o envolvimento de executivos e das lideranças através de veículos de comunicação interna, uso de procedimentos de RH, políticas de sanções e punições etc.

Programa de Conscientização de Segurança

- Concentre-se nas pessoas tanto como parte do problema e da solução.
- Abster-se de usar jargão técnico.
- Use todos os locais disponíveis para acessar todos os usuários.
- Definir pelo menos um objetivo chave de aprendizado, declará-lo claramente ...
- Mantenha as coisas claras.
- Não sobrecarregue os usuários com demasiados detalhes ou um volume de informações.
- Ajudar os usuários a entender suas funções da Segurança da Informação e como uma...
- Aproveitar os meios de comunicação internos para entregar mensagens.
- Tornar o programa de conscientização formal.
- Fornecer boas informações antecipadamente, ao invés de informações perfeitas tardiamente.

(1) Preparar o terreno para uma formação e capacitação, mudando as atitudes organizacionais para perceber a importância da segurança e as consequências adversas de seu fracasso; e

(2) Lembrar os usuários dos procedimentos a serem seguidos.



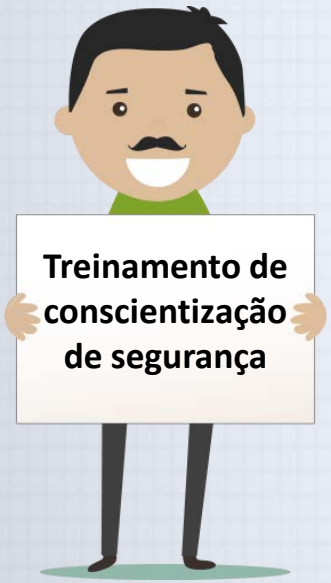
Componentes de Conscientização

- **É projetado para modificar qualquer comportamento do colaborador que põe em perigo a segurança das informações da organização.**

As atividades de sensibilização podem ser minadas se a gestão não servir como um bom exemplo.

Programas de treinamento e conscientização eficazes tornam os colaboradores responsáveis por suas ações.

Aclimatação



Vídeos

Cartazes e banners

Palestras e conferências

Treinamento em computador

Boletins informativos

Folhetos e panfletos

Mensagens em copos de café, canetas, lápis, camisetas

Quadros de avisos

Engenharia Social

Qualquer colaborador deve ser treinados para identificar a Engenharia Social e saber como identificar quem pode ter acesso a qual ativo.

Empregados devem entender e seguir as políticas da empresa sobre o que eles podem ou não podem divulgar sobre ela em uma rede social.

- **É preciso informar os limites permitidos para cada informação.**
- **É possível criar informações padrão, para barrar este tipo de investida.**
- **Isso só será possível se for explicado os motivos de ter controles de segurança; é preciso explicar e conseguir a cooperação de cada um.**
- **Quem usa engenharia social estabelece uma relação de confiança com um empregado da empresa.**

Divulgando a Mensagem de Segurança

Newsletters ou Boletim de Segurança

- **É a maneira mais econômica de disseminar informações de segurança. Podem ser na forma impressa, e-mail, ou pela intranet.**
- **O objetivo é manter a ideia de segurança da informação na cabeça dos usuários e estimulá-los a se preocuparem com a segurança.**

Boletins podem incluir:

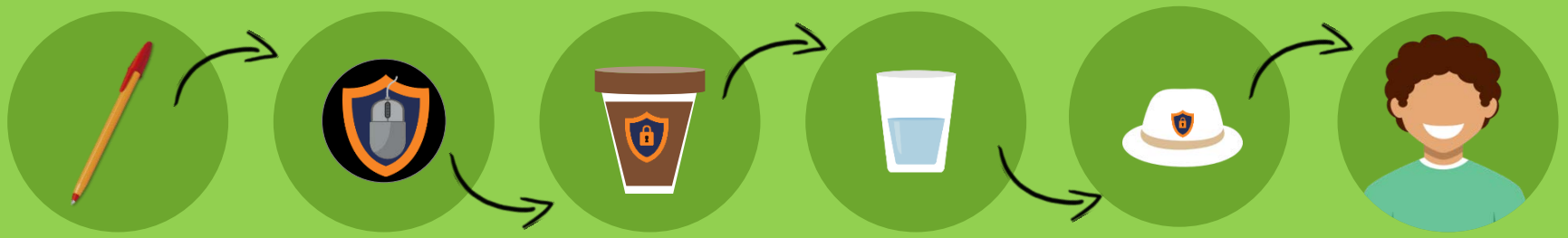
- Resumos das políticas-chave;
- Resumos de notícias importantes;
- Um calendário de eventos de segurança;
- Anúncios relevantes para a segurança da informação;
- How-To's (como fazer).

Itens para se ter um bom cartaz:

- Variar o conteúdo e mantê-los atualizados;
- Mantê-los simples, mas interessantes;
- Um calendário de eventos de segurança;
- Anúncios relevantes;
- Fornecer informações sobre denúncia.

Divulgando a Mensagem de Segurança

Trinkets são objetos simples que são usados para comunicar uma mensagem importante, que podem não custar muito unitariamente, mas quando distribuídos em toda a organização, podem se tornar caros.



- Veja o que já está fora do site.
- Planeje com antecedência.
- Mantenha o tempo mínimo de carregamento da página;
- Obtenha feedback.
- Não assuma nada e verifique tudo antes.
- Invista tempo promovendo seu site.

Acordos de Confidencialidade

Acordos de confidencialidades e os acordos de não divulgação.

Têm a finalidade de proteger a informação de forma regular.

É essencial que sejam considerados os seguintes elementos:

- Uma definição da informação a ser protegida;
- Tempo de duração esperado de um acordo;
- Ações requeridas quando um acordo está encerrado;
- Responsabilidades e ações dos profissionais que assinam os documentos...;
- Proprietário da informação, segredos comerciais e de propriedade intelectual...;
- Uso permitido da informação confidencial e os direitos do signatário para usar a informação;
- Direito de auditar e monitorar as atividades que envolvem as informações confidenciais;
- Processo para notificação e relato de divulgação não autorizada ou violação das confidenciais;
- Termos para a informação ser retornada ou destruída quando da suspensão do acordo;
- Ações esperadas a serem tomadas no caso de uma violação deste acordo.

Educação e Treinamento em Segurança da Informação

Partes Externas **Funcionários**

Devem receber treinamento, educação e conscientização apropriados, e atualizações regulares das políticas e procedimentos, conforme estabelecido em um programa de conscientização em segurança da informação.

Programa de Conscientização.

Alinhado com as políticas e procedimentos da segurança da informação.

Conter atividades regulares e repetidas, principalmente para atingir novos funcionários e partes externas.

Presencial | **À distância** | **Na web** | **Autodidata** | **e outros**

Educação e Treinamento em Segurança da Informação

Considerar as lições aprendidas dos incidentes reais na própria organização e incluir procedimentos de segurança da informação básicos.

Não focar apenas no “o quê” e “como”, mas também no “porquê”.

Aplicar uma espécie de processo disciplinar formal e assegurando um tratamento justo e correto aos suspeitos de cometer violações.

Programas de Educação, Treinamento e Conscientização

Uma vez estabelecido o local do programa de Segurança da Informação na organização, o planejamento dos Programas de Educação, Treinamento e Conscientização de segurança (PETC) começa.

PETC

Projetado para reduzir a incidência de violações acidentais de segurança por funcionários, contratados, consultores, fornecedores e parceiros de negócios.

Melhorar o comportamento dos funcionários;

Permitir que a organização responsabilize os funcionários por suas ações.

Programas de Educação, Treinamento e Conscientização

Educação em segurança → **Treinamento em segurança** → **Conscientização sobre segurança**

- Criar conhecimentos aprofundados, conforme necessário, para conceber, implementar ou operar programas de segurança para organizações e para os sistemas;
- Desenvolver habilidades e conhecimentos para que os usuários possam realizar seus trabalhos enquanto usam os sistemas com mais segurança;
- Aumentar a consciência da necessidade de proteger os recursos do sistema.

Educação em Segurança

Os funcionários sem experiência do departamento de segurança da informação devem ser encorajados a usar um método de educação formal.

- Programas híbridos de tecnologia da informação / segurança surgiram para preencher a lacuna da falta de educação focada em segurança da informação.
- A instituição que tem um currículo formal em segurança da informação deve mapear cuidadosamente os resultados de aprendizagem esperados.
- Este mapa de conhecimento pode ajudar os potenciais estudantes avaliarem os programas de segurança da informação, identificar as competências...
- Como muitas instituições não têm um quadro de referência para as qualificações e conhecimentos que são necessários para uma determinada área de trabalho, muitas vezes eles se referem às certificações oferecidas nesse campo.
- Uma vez identificadas as áreas de conhecimento, elas são agregadas em domínios, a partir das quais podem ser criados cursos individuais.

Treinamento de Segurança

Existem dois métodos para personalizar o treinamento para os usuários. O primeiro é por fundo funcional:

- Usuário geral;
- Usuário gerencial;
- Usuário técnico que pode ser dividido por:
  - ✓ Categoria de Emprego;
  - ✓ Função de trabalho;
  - ✓ Produto de tecnologia.

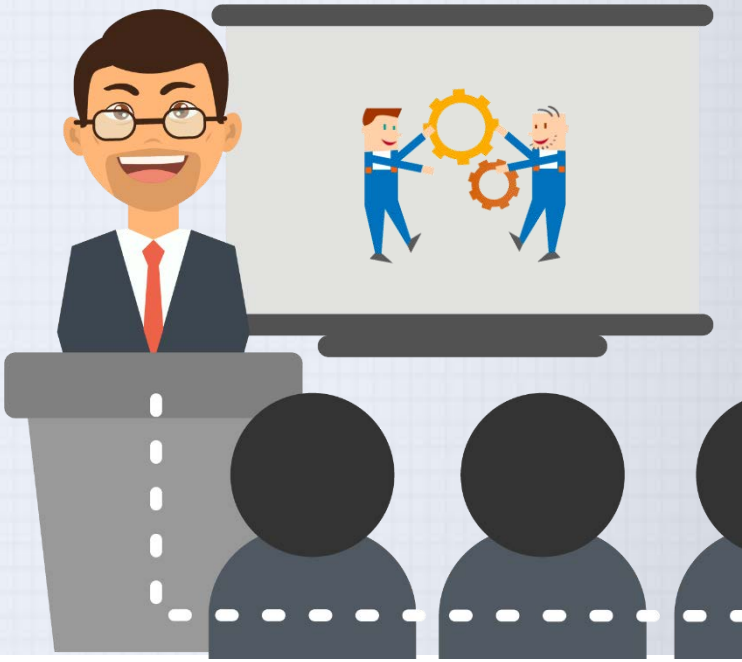
O segundo é por nível de habilidade:

- Novato;
- Intermediário;
- Avançado.

Técnicas de Treinamento

- Os bons programas de treinamento, independentemente do método de entrega, aproveitam as mais recentes tecnologias de aprendizagem e as melhores práticas.
- O treinamento, às vezes, não é necessário para todos, por isso, esperar até que haja um grupo suficientemente grande para uma classe, pode custar às empresas perda de produtividade.
- O uso de módulos curtos, orientados à tarefas, disponíveis durante a semana normal de trabalho, que acabam sendo cursos imediatos e consistentes.

- Individual;
- Treinamento Baseado em Computador *(CBT - Computer-Based Training);*
- Grupo de Suporte ao Usuário;
- Auto-Estudo sem computador (*Self-Study*).
- Classe formal e presencial;
- Treinamento à Distância / Seminários na Web;
- Treinamento *On-the-Job;*



Seleção do Pessoal para o Treinamento

Programa local de treinamento

Um departamento de educação

Uma empresa para o treinamento externo

Contratar um instrutor profissional

Organizar e conduzir treinamento interno

- **Etapa 1:** Identificar o escopo do programa, metas e objetivos;
- **Etapa 2:** Identificar a equipe de treinamento;
- **Etapa 3:** Identificar público-alvo;
- **Etapa 4:** Motivar a gerência e os funcionários;
- **Etapa 5:** Administrar o programa;
- **Etapa 6:** Manter o programa;
- **Etapa 7:** Avaliar o programa.

Pronto para o próximo?

Curso Preparatório para Certificação
Em Gestão de Segurança da Informação Avançada – Baseada na ISO/IEC 27002:2013

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 8

Controles Técnicos

Resumo

Terá conhecimento sobre os controles técnicos.

Saberá explicar a proposta da arquitetura de segurança.

Explicar a importância dos elementos de segurança na infraestrutura de TI.

Vai adquirir conhecimento sobre os controles técnicos, relações com empregados e de continuidade de negócios.

Entenderá como recomendar acesso a controles técnicos.

Recomendar controles de segurança para o ciclo de vida do emprego, favorecer o desenvolvimento e o teste de um plano de continuidade de negócios.

Criação ou validação de um framework de segurança.

Plano de Segurança de Informações que descreve os controles existentes e identifica outros controles de segurança necessários.

Um framework é o esboço do plano mais completo, que é a base para o desenho, seleção e implementação de todos os controles de segurança subsequentes.

Introdução

É uma disciplina emergente que combina os esforços de pessoas, políticas, educação, treinamento, conscientização, procedimentos e tecnologia para melhorar a Confidencialidade, Integridade e Disponibilidade dos ativos de informações de uma organização.

Os **CONTROLES TÉCNICOS** por si só não podem garantir um ambiente de TI seguro, mas são parte essencial dos Programas de Segurança da Informação.

Gerenciar o desenvolvimento e uso de controles técnicos requer conhecimento e familiaridade com a tecnologia que os capacita.

Devem ser combinados com políticas sólidas, educação, treinamento e conscientização.

Os controles técnicos podem permitir a aplicação de políticas onde o comportamento humano é difícil de regular.

Introdução

Mecanismos de segurança técnicos incluem:

- Controles de acesso;
- Firewalls;
- Proteção dial-up;
- Sistemas de detecção de intrusão;
- Ferramentas de análise e análise propriamente dita;
- Sistemas de criptografia.

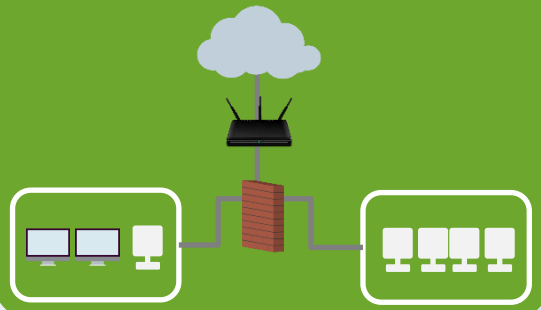
Exemplos de Controles Técnicos

Lembre-se a lista pode ser muito maior do que esta:

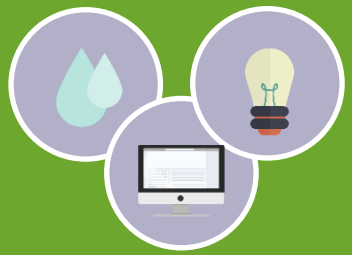
Controles contra os Malware

Registro de eventos

Segregação nas redes



Suporte aos *Utilities*



Gerenciamento de Chave

Gerenciamento de vulnerabilidades técnicas

Controles Técnicos

CONTROLES TÉCNICOS devem tratar especificamente da proteção contra ataques, códigos maliciosos, etc., através do uso de controles como a CRIPTOGRAFIA e outras técnicas.

Campanha de Conscientização sobre Segurança

Não será o suficiente para fazer com que todos os usuários da empresa estejam mais seguros.

A organização deve manter uma rotina de verificação, atualização de bons software antivírus, antimalwares, firewall e outros.

Estabelecer um canal de comunicação mais "dedicado", da qual será usado quando existirem atividades de alto risco.

- Conhecer as falhas existentes.
- Quando for configurar, parametrizar um sistema em homologação.

Não podem ficar sem controles:

Senhas | **Tokens** | **Certificados**

Infraestrutura

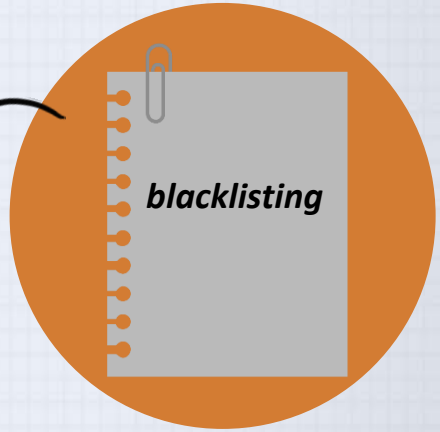
Funcionalidades dos principais itens na infraestrutura, que contribuem para a proteção dentro do escopo de segurança da informação:

- **Roteador** ou um **firewall** são um filtro em uma porta de entrada. Podem atuar como um só ou combinar os controles;
- O **roteador** é que divide as redes e encaminha ou bloqueia o tráfego.
- O **firewall** analisa os pacotes de dados e, depois, decide se o pacote é perigoso ou não.
- Um **gateway** solicita identificação aos usuários da rede e só depois que permite o acesso.
- O **firewall** pode só inspecionar os "pacotes“ e ler a lista de permitidos e bloqueados, ou pode identificar “estados específicos” de pacotes, permitindo apenas aqueles que são necessários a algum processo.
- O **firewall de camada de aplicação** interpreta melhor os argumentos e regras de protocolos e pacotes, e pode reconhecer códigos maliciosos e bloquear suas entradas.
- Os **servidores de e-mail** garantem que as mensagens fiquem armazenadas mesmo depois de serem excluídas pelos usuário, em alguns casos, e ficam sob o controle dos administradores.
- Os **servidores de aplicação** contêm os dados da organização e dos sistemas que são usados para acessar os dados.
- Em **redes wireless ou cabeadas** é usado filtragem de endereços MAC aliada a criptografia. Já as **redes sem fio**, requerem criptografia e autorização para serem um pouco mais seguras.
- A **rede WPA2** ainda pode ser considerada segura.

Proteção Contra Códigos Maliciosos

A organização precisa implementar controles para detectar, prevenir e recuperar, para se proteger contra códigos maliciosos, mais um adequado programa de conscientização do usuário.

- Uma lista de softwares permitidos a acessar o sistema, malware, etc.
- Avalie ainda a instalação de dois ou mais tipos de software de controle contra códigos maliciosos de diferentes fornecedores.



- Uma lista de softwares permitidos a acessar o sistema, controles associados a proteção contra a importação de arquivos e softwares de redes externas...
- Controles que visam reduzir vulnerabilidades que possam ser exploradas por códigos maliciosos...

- **EX.:** Por meio do gerenciamento de vulnerabilidades técnicas e que possibilitem conduzir análises críticas regulares dos softwares e dados dos sistemas que suportam processos críticos de negócio.

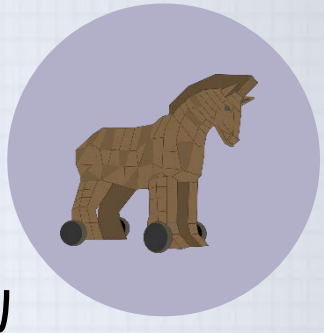
Proteção Contra Códigos Maliciosos

- Instalar e atualizar regularmente os softwares de detecção e remoção de códigos maliciosos;
- A VARREDURA POR CÓDIGOS deve ocorrer nos arquivos recebidos através de redes ou qualquer mídia de armazenamento, correio eletrônico, páginas web ou download.
- Uma avaliação pode ser feita em diversos locais;
- Definir os procedimentos e responsabilidades para tratar da proteção de código malicioso nos sistemas...
- Preparar planos de continuidade do negócio adequados para a recuperação em caso de ataques por códigos maliciosos...
- Coletar regularmente informações. EX.: Por assinaturas de listas de discussão e visitas a sites informativos sobre novos códigos maliciosos...
- Os gestores devem garantir que fontes confiáveis, sejam utilizadas para diferenciar boatos de notícias reais, sobre códigos maliciosos. Lembre-se: Isolar os ambientes onde impactos catastróficos possam ser gerados.

Controles Contra Malware

Malware

- **spyware**
- **adware**
- **phishing**
- **vírus**
- **Cavalos de Tróia**
- **worms**
- **rootkits**
- **ramsoware**



Podem danificar dados e/ou aplicativos ou roubar informações através dos navegadores.

Todos aqueles Sistemas - tanto hardware quando software - que detectam códigos maliciosos dependem de assinaturas que representam códigos previamente encontrados do malware ou detectam comportamento malicioso do próprio malware.

Falso-positivos

- É o resultado de arquivo comum que é detectado por um sistema *antimalware,* como se fosse alguma praga escondida em seu computador, apesar de não oferecerem perigo algum.

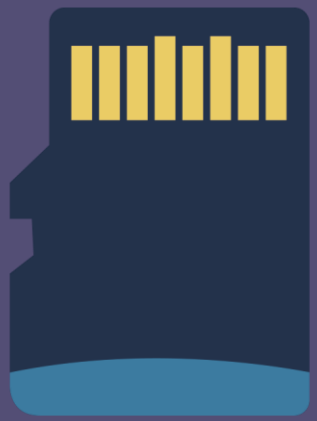
Controles Contra Malware

Malware

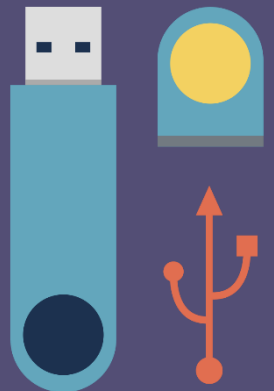
Backdoor **(portas dos fundos)**

Logic bomb **(bombas lógicas)**

Mas na maioria das vezes o computador da vítima é contaminado simplesmente por visitarem websites infectados.



Cartão de memória



Pendrives

Cópias de Segurança

Importante que, regularmente, sejam realizadas e testadas as cópias de segurança das informações, softwares e imagens do sistema, conforme a Política de Geração de Cópias de Segurança.

Plano de Backup

- Incluir os registros exatos das cópias de segurança e dos procedimentos de restauração da informação...
- Precisam ser armazenadas em uma local distante o suficiente para escapar dos danos de um possível desastre no local principal...
- As mídias de backup devem ser testadas regularmente para garantir que são confiáveis no caso do uso emergencial...
- Em situações onde a confidencialidade é importante, é essencial que cópias de segurança sejam protegidas com criptografia.

A Importância do Backup

Criar uma rotina de backup é indispensável, tanto para fazer o backup, quanto para restaurar em caso de necessidade.

Tríade: Confidencialidade e Integridade e Disponibilidade.

BACKUP - Pode ser feito até em um HD externo, ou outra forma de armazenamento externo, independente da mídia usada, faça regularmente uma checagem neste backup.

- Questione se durante os procedimentos de segurança da informação estão sendo seguidos ou se durante um problema nos serviços, é possível retornar ao trabalho e, principalmente, em quanto tempo.
- Realize o backup diariamente, como uma rotina automática, mantendo, idealmente, pelo menos os backups da última semana à disposição e com rápido acesso, e principalmente, armazene em local externo ao servidor.
- Faça um backup com as informações mais importantes para a empresa.
- Crie um passo a passo fácil de seguir.
- Inclua um processo de restauração e de teste, avaliando sempre o tempo dos mesmos.

Orientação Para Backup de Informação

- O fato de ser feito um backup diariamente não significa que a organização e seus dados estão protegidos, pois a questão primordial é a restauração.
- O problema é ser capaz de restaurar todas as informações relevantes sempre que há uma perda de dados, sob qualquer circunstância, com o espaço de tempo necessário.

- Entender quanto tempo se leva para restauração;
- Entender quais sistemas devem ser restaurados;
- Disponibilidade para fazer a restauração;
- Conhecimento dos colaboradores a respeito das atividades de restauração;
- Software exigido para fazer a restauração;
- Procedimentos de restauração descrevendo as atividades necessárias;
- Procedimentos testados após a restauração, para decidir se o ambiente pode voltar a ficar operacional.

Controle de Acesso

Uma empresa que possui uma senha de acesso para determinada função, que só os gerentes podem liberar, mas que por algum motivo é repassada a outros usuários em um determinado momento.

- Quem define o valor da informação é o dono desta informação.
- Os proprietários dos ativos que devem definir as regras de controle de acesso.

Controles lógicos - incluem acesso de sistemas, rede, etc.

Acessos físicos - são os que impedem uma pessoa de entrar em uma sala, por exemplo.

O Trabalho Remoto e Dispositivos Móveis

- Garantir que seja mantida a segurança das informações em ambos os casos (trabalho e do dispositivo).
- Os dispositivos móveis devem estar cobertos por cuidados que assegurem o não comprometimento das informações da empresa.
- É preciso pensar em ações que cubram seu uso em ambientes desprotegidos.

✓ Os registros dos dispositivos móveis;

✓ O que é necessário para a proteção física (seguros, capas, ...)

✓ Que seja protegido contra a instalação de softwares não autorizados;

✓ Os requisitos para as versões dos softwares e os caminhos do sistema;

✓ As restrições para os tipos de conexão aos serviços de informação;

- Deve ter um controle de acesso através de elementos como Identificação, Autenticação e Autorização;
- Criptografia e recursos contra códigos maliciosos;
- Bloqueio contra exclusão, desativação ou mesmo um bloqueio externo, seja ele acidental ou proposital;
- Precisam ter um mecanismo de backups;
- E cuidar quanto ao uso dos serviços web e aplicações dentro da web.

O Trabalho Remoto e Dispositivos Móveis

Autenticação

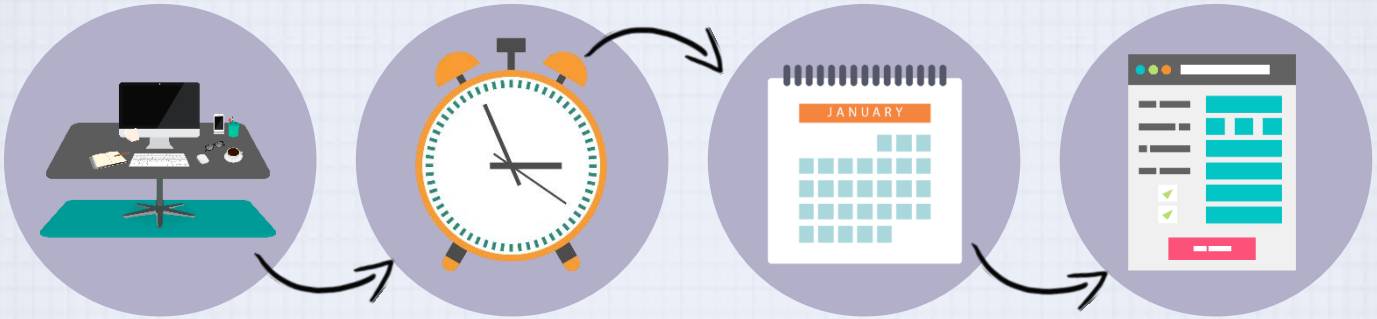
Criptografia

Seguros podem ser feitos e deve ter um plano em caso de roubo.

Quem usar estes dispositivos precisa ser treinado, saber o uso correto e as consequências do uso incorreto.

Requisitos no Trabalho Remoto

O trabalho remoto é todo aquele que é feito fora do escritório padrão.

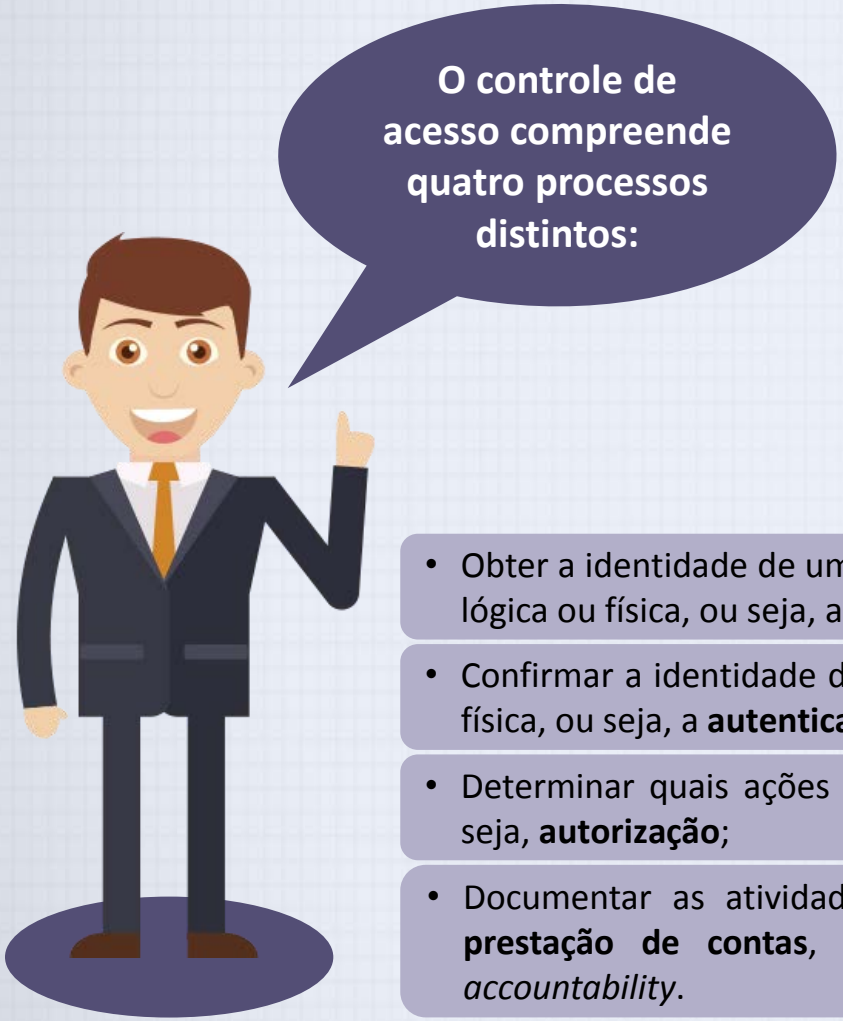


- Detectar os métodos de acesso que o funcionário deve usar;
- Fornecer meios seguros para este acesso;
- Pensar se vale a pena fazer um seguro do equipamento;
- Planejar ações quando um funcionário deixar a empresa;
- Definir se ele vai devolver o equipamento, como serão retiradas as permissões e os acessos etc

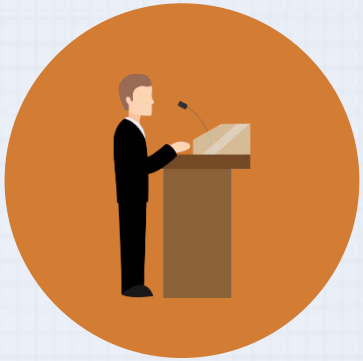
Requisitos no Trabalho Remoto

- É preciso manter uma forma de acesso virtual nas estações de trabalho.
- Criar uma forma para que o sistema acessado não seja processado nem armazenado no computador do usuário
- Verificar a integridade das redes domésticas, os requisitos ou restrições na configuração dos serviços usados em rede sem fio.
- Criar políticas e procedimentos que evitem disputas sobre direitos de propriedade intelectual – os direitos autorais – de quem trabalha em equipamentos de propriedade particular.
- Criar mecanismos que permitam o acesso remoto aos equipamentos de propriedade particular.
- Pode ser necessário um acesso remoto para verificar a segurança do equipamento em algum momento ou mesmo durante uma investigação.
- Verificar os acordos de licenciamento de software que a empresa precisa usar e checar os requisitos de proteção contra vírus e ajustes de firewall.

Elementos do Controle de Acesso



Política de Controle de Acesso:



Determina como os direitos de acesso são concedidos a entidades e grupos.

- Obter a identidade de uma entidade através de uma solicitação de acesso a uma área lógica ou física, ou seja, a **identificação**;
- Confirmar a identidade desta entidade que busca obter acesso a uma área lógica ou física, ou seja, a **autenticação**;
- Determinar quais ações essa entidade pode realizar nessa área física ou lógica, ou seja, **autorização**;
- Documentar as atividades do indivíduo e dos sistemas autorizados, ou seja, a **prestação de contas**, porém usualmente usamos o termo em inglês como *accountability*.

Identificação

A IDENTIFICAÇÃO é um mecanismo que fornece informações sobre uma entidade que ainda não foi verificada, chamada de SOLICITANTE (que deseja obter acesso a um recurso).

O ID ou o IDENTIFICADOR deve ter um valor exclusivo que pode ser mapeado para uma entidade dentro do domínio de segurança, que está sendo administrado.

Algumas organizações usam **identificadores compostos,** com a finalidade de se obter **identificadores exclusivos** dentro do domínio de segurança.

Para se obter acesso à informação, no caso, um sistema, o usuário deve identificar-se com algo que ele possui, ou através de um conhecimento, tal como um USUÁRIO e SENHA ou ainda, algo que usuário é, tal como a BIOMETRIA. Com mais de dois: AUTENTICAÇÃO FORTE.

Autenticação

É o processo que valida a suposta identidade do solicitante. Ele garante que a entidade que solicita o acesso é a verdadeira.

- **Algo que você sabe**, por exemplo, senhas e palavras-chave;
- **Algo que você tem**, como tokens criptográficos e cartões inteligentes com ou sem a fotografia do dono;
- **Algo que você é**, e isso incluem as impressões digitais, impressões de palma da mão, topografia de mão, geometria da mão, escaneamento da retina e íris, etc.;
- **Algo que você produz**, como o reconhecimento de voz e de assinatura.

Certas áreas críticas ou físicas requerem níveis de acesso mais altos e, portanto, usam uma autenticação forte, ou seja, como mencionado, pelo menos dois mecanismos diferentes de autenticação, geralmente algo que você tem e algo que você sabe.

Autenticação de dois fatores

Autorização

A autorização para acessar estes ativos deve ser regida por um processo seguro.

Tipos de acesso também devem ser controlados

Estes direitos de acesso devem ser acoplados ao papel de alguém na organização;

Um cuidado especial ao ser dado proteção contra leitura.

As senhas devem:

- Não consistir em palavras encontradas no dicionário;
- Serem longas e conterem caracteres de toda a lista alfanumérica;
- Mudar com regularidade.

Processo de Autorização

A autorização pode ser tratada de três maneiras:

- Autorização para cada usuário autenticado.
- Autorização para membros de um grupo, da qual o sistema é autenticado;
- Entidades de uma lista associadas a um grupo que concede acesso aos recursos com base nos direitos de acesso deste grupo.
- Autorização em vários sistemas, em que um sistema central de autenticação e autorização verifica a identidade da entidade e concede um conjunto de credenciais à entidade verificada.

Login único *(SSO – Single Sign-On)* ou de login reduzido

***Lightweight Directory Access Protocol* - LDAP**

Prestação de Contas

Prestação de Contas ou Accountability

Assegura que todas as ações em um sistema possam ser atribuídas a uma identidade autenticada.

Pesquisar → **Modificar dados** → **Autorização para aumentar o nível dos privilégios** → **Pesquisar ou modificar dados que estejam além de seu nível de acesso**

- É realizada através da implementação de logs do sistema e de logs de banco de dados, além de uma auditoria desses registros.
- Registros de sistemas - registros mantidos por um sistema específico que foi configurado para registrar informações específicas, como tentativas de acesso com falha e modificações de sistema.

Uso dos *logs*

- detecção de intrusão
- determinar causa-raiz de uma falha do sistema
- simplesmente rastreamento do uso de um recurso específico.

Prestação de Contas

Menos privilégio: os colaboradores recebem acesso a uma quantidade mínima de informação, proporcional pelo o que é desempenhado em suas funções;

Necessidade de conhecimento: limita o acesso a informação do que é exigido para executar seus trabalhos;

Segregação de funções: mais de um colaborador é responsável por um determinado ativo, processo ou tarefa.

Controles de Acesso

Controle de Acesso → **Controle Técnico** → **Controle Físico**

Controle Organizacional

Controle de Acesso endereça questões sobre a admissão de um usuário em uma área confiável da organização.

Podem incluir sistemas de informação, áreas fisicamente restritas, como salas de informática, e até mesmo a organização na sua totalidade.

Consiste de uma combinação de políticas, programas e tecnologias.

Obrigatórios (MACs - Mandatory Access Control)

- Usam um esquema de classificação de dados que classifica cada coleção de informações.

Nos controles de acesso baseados em rede, por exemplo, os usuários recebem uma matriz de autorizações para determinadas áreas de acesso.

Lista de controle de acesso (ACL - Access Control List).

Controles de Acesso

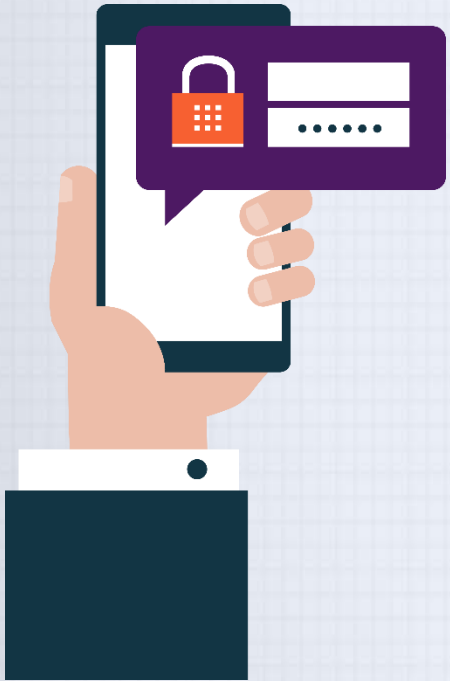
- **Necessidade de conhecer:** permissão para acessar as informações que são necessárias para trabalhar.

- **Necessidade de uso:** permissão para acessar os recursos como equipamentos conforma a sua função.

Controles de Acesso Discricionário

Controles Discricionários

São os controles livres de condições, de restrições. É uma política de controle de acesso determinada pelo **proprietário do recurso**, como um arquivo.



Controles Baseados em Função

- São vinculados à função que um usuário específico realiza em uma organização

Controles Baseados em Tarefas

- Podem ser baseados em listas mantidas, assuntos ou objetos.
- São vinculados a uma atribuição ou responsabilidade específica.

Controles de Acesso Discricionário

Controles de Acesso Discricionário (DACs - *Discretionary Access Control*)

São implementados a critério ou opção do usuário de dados.

Os usuários podem permitir o acesso sem restrições ou podem permitir que as pessoas, ou conjuntos de pessoas específicas, acessem esses recursos.

Protegendo a Confidencialidade

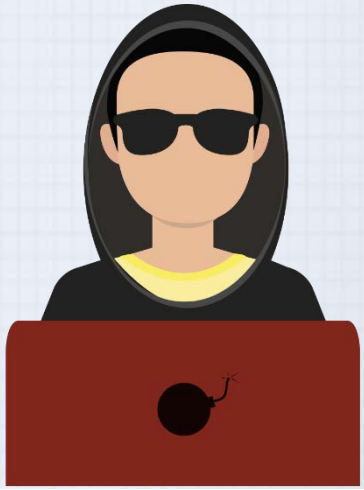
Identificação

Autorização do usuário

Acessos subsequentes devem ser baseadas na lista de controle de acesso ACL - *Access Control List*

- **Faz com haja um tipo de “embaralhamento” da informação.**

- **Vai exigir algum tipo de chave digital, seja simétrica ou assimétrica, que faz a criptografia e descriptografia da informação.**

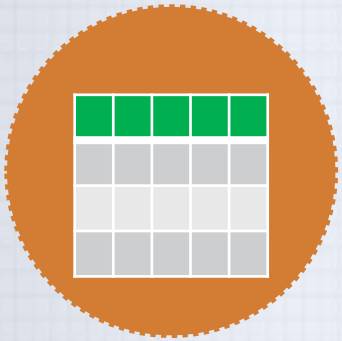


Listas de Controle de Acesso - ACL

Listas de Controle de Acesso (ACLs)

- Listas de acesso de usuário;
- Matrizes;
- Tabelas de capacidade.

- **Podem controlar o acesso a sistemas de armazenamento de arquivos, aos objetos ou outros dispositivos de comunicação de rede.**



Matriz ou tabela

- Especifica quais objetos e usuários ou grupos de usuários podem acessar.
- Identifica claramente quais privilégios devem ser concedidos a cada usuário ou grupo de usuários.

Granularidade

- Pode variar de sistema para sistema.
- Permitem aos administradores restringi o acesso de acordo com o usuário, computador, tempo, duração ou mesmo um arquivo específico.

Listas de Controle de Acesso - ACL

ACLs regulam:

- Quem pode usar o sistema;
- Que usuários autorizados podem acessar;
- Quando usuários autorizados podem acessar o sistema;
- De onde usuários autorizados podem acessar o sistema;
- Como os usuários autorizados podem acessar o sistema.

Os administradores definem privilégios de usuário, como:

- Leitura;
- Escrita ou gravação;
- Criação;
- Modificação;
- Exclusão;
- Comparação;
- Cópia.

Outras Formas de Controle de Acesso

CONTROLES DE ACESSO DEPENDENTES DO CONTEÚDO:

Como o nome sugere o acesso a um conjunto específico de informações pode depender do seu conteúdo.

INTERFACES RESTRITAS DE USUÁRIO:

Alguns sistemas são projetados especificamente para restringir as informações que um usuário individual pode acessar.

ISOLAMENTO TEMPORAL (baseado no tempo):

Em alguns casos, o acesso à informação é limitado por uma restrição de hora-de-dia.

Outras Formas de Controle de Acesso

Acesso

Centralizado

Descentralizado

- **O nível de centralização adequado a uma dada situação vai variar de acordo com a organização e o tipo de informação protegida.**
- **Quanto menos crítica é a informação, mais os controles tendem a ser descentralizados.**
- **Quando ativos críticos de informação estão sendo protegidos, o uso de um conjunto de ferramentas de controle de acesso altamente centralizado é indicado.**
- **RADIUS e o Kerberos.**

Categorias de Controle de Acesso

Categorias de Controle de Acesso

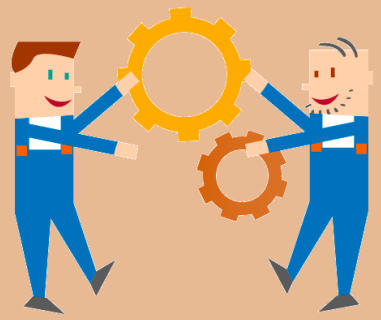
Série de Publicações Especiais do NIST (http://csrc.nist.gov/publications/PubsSPs.html)

Gerenciamento:

Controles que abordam os processos de segurança desenhados por pessoas do nível estratégico, incorporados nas práticas de gestão da organização e rotineiramente usados por administradores de segurança para projetar, implementar e monitorar outros sistemas de controle;

Operacional (ou administrativo):

Controles que lidam com funções operacionais de segurança, que foram integrados nos processos diários da organização;



Técnico:

Controles que suportam as questões táticas de um programa de segurança e que foram implementados como mecanismos reativos para atender às necessidades imediatas da organização, uma vez que respondem às realidades de um ambiente técnico.

Controles de Rede

Comunicações

- Roteador;
- Firewall;
- Porta de entrada (Gateway);
- Zona desmilitarizada (DMZ);
- Servidores de E-mail / Web / Antivírus / DNS;
- Sistema de detecção de intrusão (IDS);
- Sistema de prevenção de intrusão (IPS).

Processamento de Informação

- Servidores de arquivos;
- Servidores de aplicação;
- Servidores contendo outros serviços Client/Server.

Transmissão

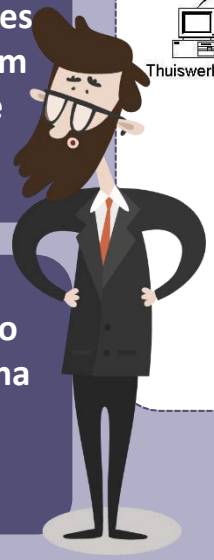
- Rede LAN a cabo;
- Rede LAN sem fio (wireless).

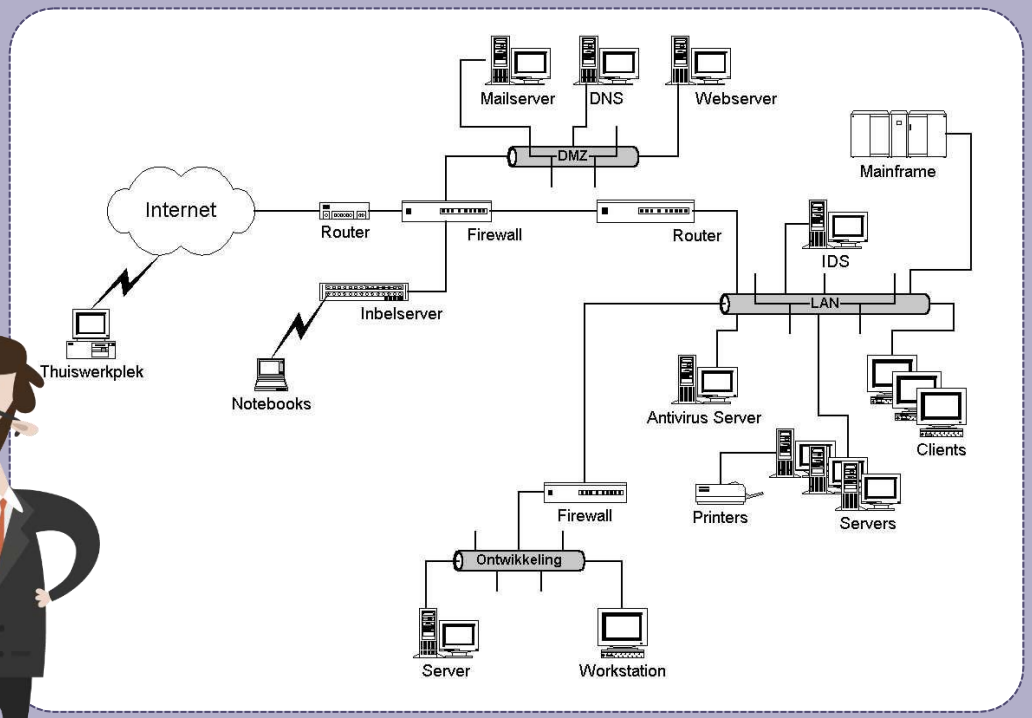
Controles de Rede

- **O CONTROLE pode ser feito através de um roteador dividindo a rede ou com base na faixa de endereço, bloqueando ou liberando o acesso.**

- **Um FIREWALL analisa os pacotes de dados e decide, com base em uma lista de regras, se permite esses pacotes na rede ou não.**

- **Um GATEWAY que vai um passo além: ele só permite usuários na rede após a identificação e autorização.**





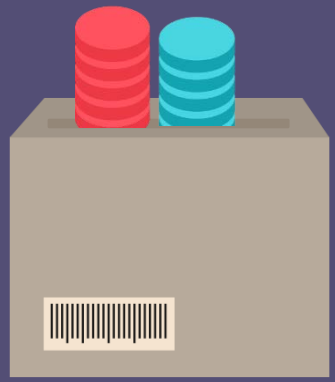
Gerenciamento dos Logs

Verifique se há espaço suficiente para armazenamento dos logs gerados pelas atividades.

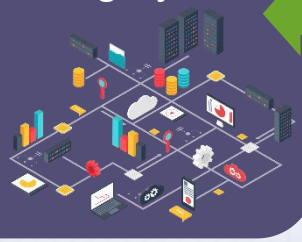
As configurações desta sobreposição de registro devem ser configuradas para o sistema.

Os sistemas de log podem copiar os registros para outro local ou removê-los definitivamente após um período para liberar espaço.

Existe uma discordância em relação ao tempo de armazenamento destes logs. Por isso, algum plano deve estar em vigor para lidar com esses arquivos.



O registro de arquivos deve ser criptografado quando armazenados, para evitar a divulgação não desejada caso o armazenamento de log seja comprometido.



Uma vez que os dados do registro tenham sobrevivido à sua utilidade, ele deve ser destruído com segurança.

Avaliando a Biometria

Taxa de Falso Negativo (Tipo I):

- Percentagem de usuários autorizados que tem acesso negado. A rejeição de um usuário autorizado não representa uma ameaça à segurança, mas apenas um empecilho, no entanto, muitas vezes não é visto como um problema grave até que o aumento da taxa seja alto o suficiente para irritar os usuários.

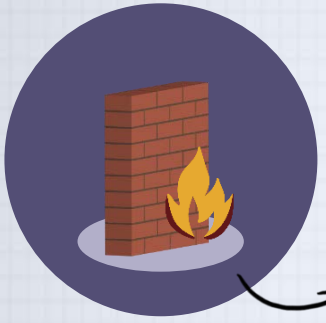
Taxa de Falso Positivo (Tipo II):

- Percentagem de usuários não autorizados a quem é concedidoo acesso. É a taxa de aceitação de usuários fraudulentos ou não, que têm acesso aos sistemas ou áreas como resultado de uma falha no dispositivo biométrico. Essa falha representa uma grave violação de segurança.

Taxa de Erro de Crossover:

- O ponto em que o número de falsos negativos se iguala aos falsos positivos. É o resultado ideal para sistemas baseados em biometria. Estes resultados são usados para comparar vários dados biométricos e podem variar de acordo com o fabricante. Um dispositivo biométrico que fornece uma equiparação de 1% é considerado superior a um dispositivo com um cruzamento de 5%.

Firewalls – 1ª e 2ª Geração



É qualquer dispositivo que impeça um tipo específico de informação de se mover entre o mundo exterior - conhecido como rede não confiável - e o interno - conhecido como a rede confiável.

- Pode ser um sistema separado;
- Um serviço rodando em um roteador;
- Servidor existente;
- Uma rede separada contendo vários dispositivos.

1ª Firewalls de Filtragem de Pacotes

- São dispositivos simples de rede que filtram os pacotes, examinando cada cabeçalho dos de entrada e saída.
- Podem seletivamente filtrar pacotes com base em valores no cabeçalho dele, aceitando ou rejeitando conforme necessário.
- Podem ser configurados para filtrar com base no endereço IP, tipo de pacote, solicitação de porta e / ou outros elementos.

2ª Firewalls de Nível de Aplicativo

- Consiste em computadores dedicados, mantidos separados do primeiro roteador de filtragem (roteador de borda);
- Configuração: o servidor Proxy, ao invés do servidor Web, é exposto ao mundo externo a partir de um segmento de rede chamado DMZ (zona desmilitarizada), uma área intermediária entre uma rede confiável e uma rede não confiável.

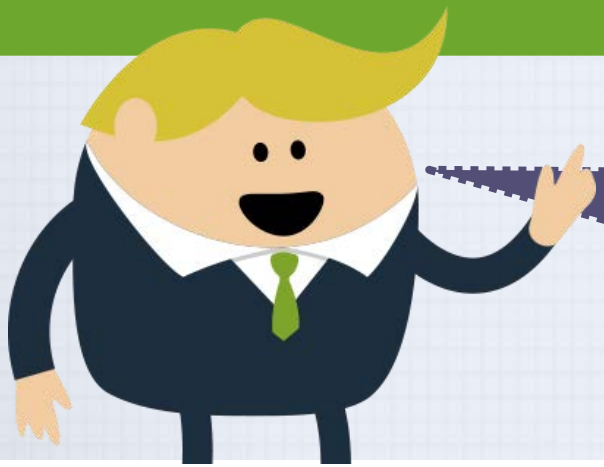
Firewalls – 3ª e 4ª Geração

3ª Firewall de Filtragem Multiestado ou *Stateful Inspection*

- As tabelas de estado rastreiam o estado e o contexto de cada pacote trocado, gravando qual equipamento enviou qual pacote e quando.
- Se este tipo de firewall receber um pacote de entrada que não esteja em sua tabela de estado, então, ele consulta a lista de ACL para determinar se permite o pacote passar.

4ª Firewall de Filtragem Dinâmica de Pacotes

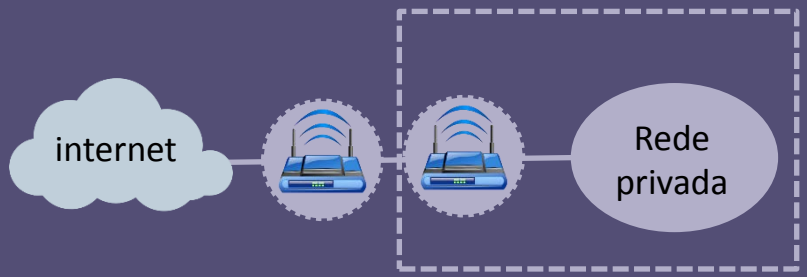
- Permite que apenas um pacote específico com uma origem, um destino e um endereço de porta específico passe pelo firewall.
- Ele faz isso por entender como o protocolo funciona, abrindo e fechando as portas no firewall com base nas informações contidas no cabeçalho do pacote.



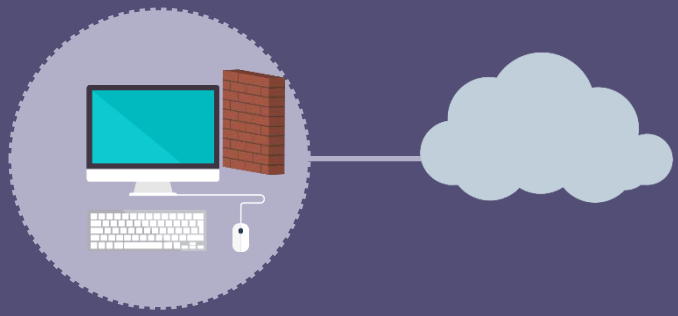
Os Filtros de Pacotes Dinâmicos são uma forma intermediária, entre Filtros de Pacotes Estáticos tradicionais e Aplicativos Proxy.

Arquitetura de Firewall

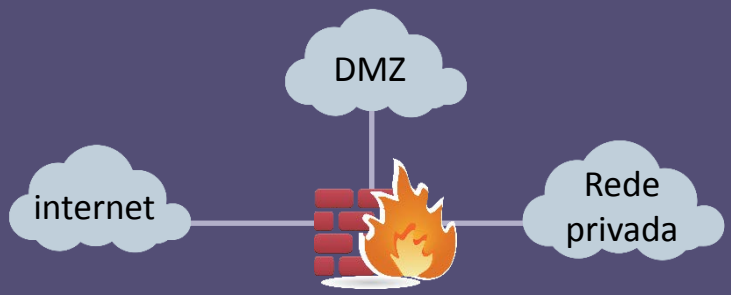
Roteadores de filtragem de pacotes



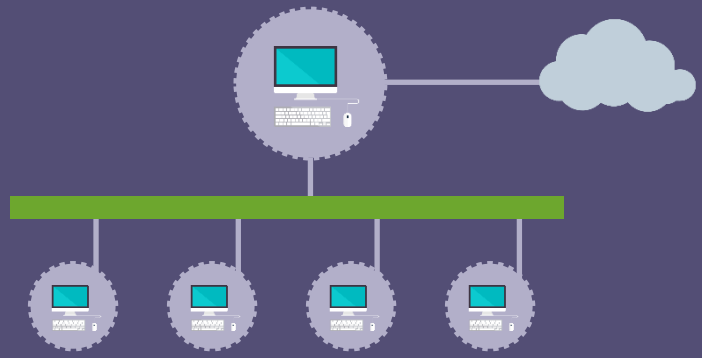
Firewalls com host selecionado



Firewalls de Blindados com DMZ



Firewalls host *dual-homed*



Selecionando o Melhor Firewall

1. Que tipo de tecnologia de firewall oferece o equilíbrio certo entre proteção e custo para as necessidades da organização?
2. Que características estão incluídas na arquitetura de firewall com um preço inicial?
3. Como é fácil configurar e configurar o firewall?
4. O firewall candidato pode se adaptar à crescente rede da organização?

- São conhecidos todos os fatores de custo?
- Quais recursos estão disponíveis com um custo extra?
- Quão acessíveis são os técnicos da equipe especializada que podem configurar o firewall com competência?

Gerenciando Firewall

- **Cada regra de firewall deve ser cuidadosamente elaborada;**
- **Colocada na lista com uma sequência apropriada, depurada e testada;**
- **Essa sequência de regras assegura que as ações mais intensivas sejam executadas após as mais restritivas, reduzindo assim o número de pacotes que passam por um exame intenso.**

Gerenciando Firewall

- Executam nada mais do que foram programados, eles não têm uma inteligência como esperam alguns profissionais.
- Lidam estritamente com os padrões que foram definidos.

São projetados para funcionar dentro dos limites da capacidade de hardware e, portanto, só podem responder a padrões de eventos que acontecem em uma sequência esperada e simultânea.

Gerenciando Firewall

- Falta de treinamento;
- Os firewalls são muito diferentes;
- Responsável pela segurança;
- Tarefas diárias de administração.

Práticas no Uso de um Firewall

- Todo o tráfego da rede confiável deve ser permitido.
- O dispositivo de firewall jamais deve estar acessível diretamente da uma rede pública, assim como quase todo o acesso é negado aos usuários internos.
- É permitido o envio e recebimento de dados SMTP *(Simple Mail Transport Protocol)* pelo firewall, porém, devem ser roteados por um gateway SMTP.
- Todos os dados ICMP *(Internet Control Message Protocol)* devem ser negados.
- O acesso Telnet (emulação de terminal) a todos os servidores internos através de redes públicas deve ser bloqueado.
- O acesso Telnet (emulação de terminal) a todos os servidores internos através de redes públicas deve ser bloqueado.

Sistemas de Detecção de Intrusão

Sistemas de Detecção de Intrusão de Segurança da Informação (IDSs - Information Security Intrusion Detection Systems).

Eles não servem apenas para detectar intrusão, mas também para impedir que o intruso ataque a organização.

Muitos IDSs podem ser configurados para notificar administradores via e-mail e através de *pagers*.

- **Interrompem o ataque;**
- **Alteram o ambiente de segurança reconfigurando dispositivos de rede;**
- **Alteram o conteúdo do ataque. Ex.: Remove o arquivo infectado de um e-mail.**

Rede	Host	Métodos de Detecção
Proteger os ativos de informações de rede.	Proteger o servidor ou host.	• Baseado em Assinatura; • Baseado em Anomalias Estatísticas.

Tipos de IDS

IDS baseado em Rede

- Monitoram o tráfego da rede e, quando ocorre uma condição predefinida, notificam ao administrador.
- Procuram padrões de tráfego de rede para indicar um ataque de negação de serviço ou uma série de pacotes relacionados que podem indicar uma varredura de portas.
- Combinam estratégias de ataque conhecidas e desconhecidas, através de uma base de conhecimento, para determinar se um ataque realmente ocorreu.

Já que esses sistemas produzem muito mais leituras de falso-positivos, do que os IDSs baseados no host, por estarem tentando ler e interpretar o padrão de atividade da rede, a fim de determinar o que é ou não normal.

Tipos de IDS

IDS Baseado em Assinatura ou em IDS Baseado em Conhecimento

- Examina o tráfego de dados para algo que corresponde às assinaturas, que compreendem aos padrões de ataque preconfigurados e predeterminados.

- **Problema:** as assinaturas devem ser continuamente atualizadas.
- **Fraqueza:** o período em que os ataques ocorrem.

- Se os atacantes são lentos e metódicos, podem ser facilmente detectados através do IDS, uma vez que as suas ações podem não corresponder à uma assinatura que inclua fatores baseados, por exemplo, na duração dos eventos.

- Coleta os dados de um tráfego normal e estabelece um padrão.
- Periodicamente e com base em métodos estatísticos, as amostras das atividades na rede são comparadas com as amostras de linha de base.
- Quando a atividade é diferente dos parâmetros de linha de base (conhecidos como nível de clipping), o IDS notifica o administrador.

IDS Baseado em Anomalias Estatísticas ou em Comportamento

Gerenciando IDS

Não remove ou nega acesso a um sistema por padrão, a menos que esteja programado para executar a ação, ele meramente registra os eventos que o acionam.

Devem ser configurados usando conhecimento técnico, de negócios e de segurança, para diferenciar entre circunstâncias de rotina e ameaças baixas, moderadas ou graves.

Configurado corretamente pode traduzir um alerta de segurança em diferentes tipos de notificação. Caso contrário, pode gerar sobrecarga de informações.

Gerenciador Corporativo Consolidado

***(Consolidated Enterprise Manager* - CEM)**

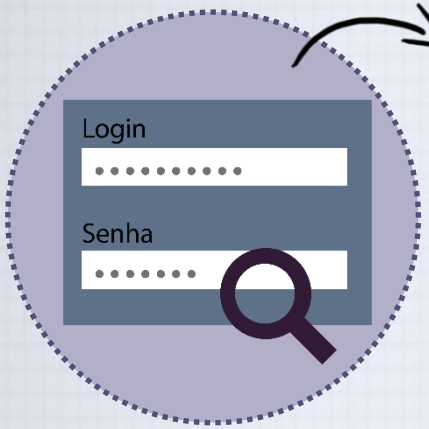
Agentes

Software que reside em um sistema que gera e armazena relatórios, que são usados para um servidor gerenciar.

O **CEM** não apenas coleta as respostas de todos os IDSs, atuando como uma estação central de monitoramento, mas também pode ser usado para identificar esses tráfegos e intrusões entre sistemas.

Software que permite que o profissional de segurança colete os dados de vários IDSs, Baseados em Host e Baseados Rede, e procure por padrões em sistemas e subredes.

Política de Senhas



Caso o recurso de AUTENTICAÇÃO, independente do sistemas, não permita distinguir o conteúdo permitido de senha, há a necessidade de conscientização dos usuário para se evitar senhas que contenham:

- **Data de nascimento**
- **De casamento**
- **Aniversário da mãe**
- **Pai**
- **Amigo**
- **De qualquer outras pessoa**

Engenharia Social

- **Evitar o nome do próprio usuário.**
- **Do seu bicho de estimação.**
- **De um ator, cantor, escritor, ou qualquer outro ídolo.**

Alguns sistemas usam estes dados como uma segunda camada de autenticação.

Política de Senhas

As senhas não devem ser fáceis de lembrar, nem de falar. O correto é que sejam criadas a partir de uma ordem aleatória.

Que não sejam uma palavra real, que possa ser testada, porque os programas que quebram senhas por força bruta, sempre usam palavras de dicionário.

Use maiúsculas, minúsculas, números, caracteres especiais e até espaços, quando quiser uma senha realmente segura.

E, se for escrever, que seja em um lugar de difícil acesso. Preferencialmente, mude constantemente, porém, de forma moderada, planejada, de acordo com o risco que a descoberta da senha possa representar.

Proteção de Acesso Remoto

Conexões dial-up ou com linhas alugadas.

Hoje, os firewalls são usados para proteger a conexão entre uma organização e a Internet (rede pública).

O mesmo nível de proteção é necessário para proteger as conexões, ao usar redes privadas, que permitem acesso dial-up.

Conectividade VPN

war-dialer

Programa de discagem automática que descobre quem atende a um chamado telefônico, se uma pessoa, uma secretária eletrônica ou um modem**. Se um modem:** ele faz uma anotação do número e, em seguida, move para o próximo número de destino. Então, tenta invadir a rede através da conexão de modem identificada usando uma variedade de técnicas.

RADIUS

CHAP - ***Challenge Handshake Authentication Protocol***

RADIUS e TACACS

O acesso dial-up não seguro representa exposição substancial ao ataque.

RADIUS ---------- **TACACS**

RADIUS - *Remote Authentication Dial-In User Service* (Serviço de Usuário de Discagem Autenticação Remota)

- Centraliza o gerenciamento da autenticação dos usuários, colocando a responsabilidade pela autenticação de cada usuário de um servidor RADIUS central.

- Servidor de acesso remoto *(RAS - Remote Access Server)* recebe uma solicitação para uma e passa a solicitação junto com credenciais do usuário para o servidor RADIUS. O RADIUS então valida as credenciais.

O *Terminal Access Controller Access Control System* (TACACS)

- Funciona de forma semelhante e é baseado em uma configuração cliente / servidor. As organizações que continuam a oferecer acesso remoto dial-up devem lidar com uma série de problemas árduos:

- Determinar quantas conexões dial-up a organização tem.
- Controlar o acesso a inúmeros modens autorizados.
- Use call-back (retorno de chamada) sempre que possível.
- Utilizar a autenticação de tokens se for possível.

Gerenciando Conexões Dial-up

Ferramentas de Análise

- Lista com vários sites de hackers marcados;
- Procurar discussão de novas vulnerabilidades;
- Novas técnicas de proteção e técnicas de roubos favoritas.

Footprinting

- É uma pesquisa organizada de endereços da Internet.

Fingerprinting

- Faz um exame sistemático de todos os endereços Internet da organização (recolhidos durante a fase de *Footprinting*).

- Produz uma análise de rede de forma detalhada que fornece informações úteis sobre os alvos do ataque planejado. Para obter o conhecimentos no uso destas ferramentas, o profissional precisará de muita educação e treinamentos específico.

Coletam as informações que um invasor precisa para ter sucesso.

Proteção de Redes Sem Fio

Certifique-se de que a área de cobertura de uma rede Wi-fi cobre apenas uma área pretendida, mas que não seja suficientemente grande que permita que áreas externas recebam um sinal da rede sem fio.

WEP (*Wired Equivalent Privacy*)

WPA (*Wi-Fi Protected Access*)

- **Fornecem um nível básico de segurança para impedir o acesso não autorizado ou uma escuta indevida.**

Tem falhas relacionadas a criptografia fundamental, que resultam em vulnerabilidades, que podem ser exploradas facilmente.

É o padrão da indústria, criado pela Wi-Fi Alliance.

Há problemas de compatibilidade com WAPs mais antigos.

Mas existem fornecedores de recursos WAP que aumentam as soluções de autenticação, criptografia e taxa de transferência.

Proteção de Redes Sem Fio

Wi-Max, ou WirelessMAN

- Essencialmente uma melhoria na tecnologia desenvolvida para telefones celulares e modems.

IEEE 802.16

- Padrão industrial para comunicações sem fio de curto alcance entre dispositivos.
- O link de comunicação sem fio Bluetooth pode ser explorado por qualquer pessoa dentro da faixa de aproximadamente 30 pés, a menos que sejam implementados controles de segurança adequados.
- Não autentica as conexões, mas ele implementa algum grau de segurança quando os dispositivos acessam determinados serviços.

Bluetooth

Port Scanners

Utilitários de varredura de portas (ou scanners de portas - Port Scanners).

- Técnicas de *fingerprint* - computadores ativos em uma rede;
- Portas e serviços ativos;
- Funções cumpridas nessas máquinas;
- E outras informações úteis.

Uma porta é um canal de rede ou ponto de conexão em um sistema de comunicação de dados.

- Protocolo de rede TCP / IP, os números de porta TCP e UDP.
- Existem 65.536 números de portas em uso.

- **Portas bem conhecidas:** de O até 1023.
- **Portas registradas:** de 1024 a 49151
- **Portas dinâmicas e privadas:** de 49152 a 65535.

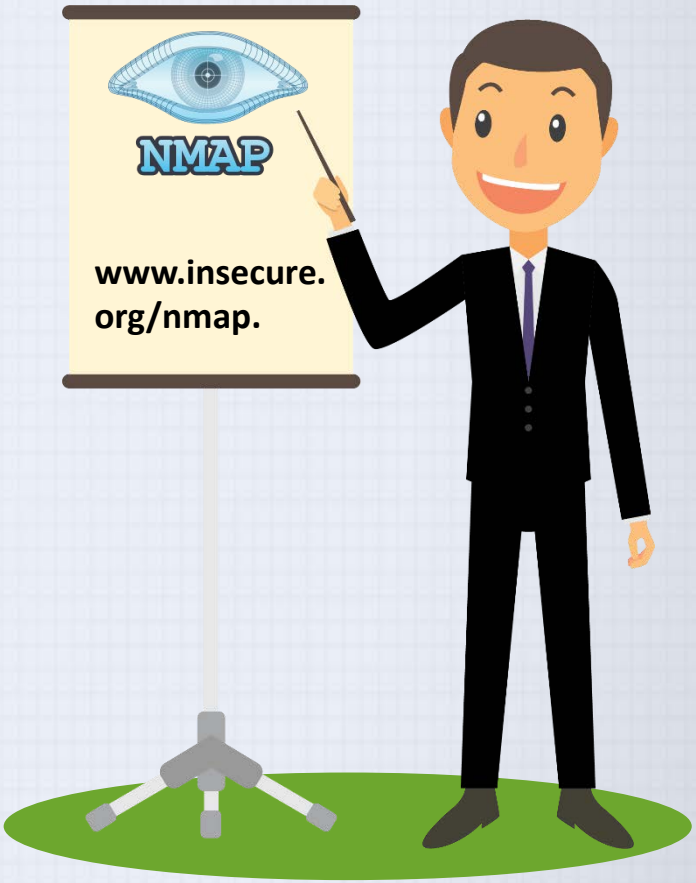
- **REGRA GERAL:** proteger todas as portas e remover do serviço todas as portas que não necessárias para funções essenciais.

Vulnerability Scanners e Packet Sniffers

Scanners de Vulnerabilidade *(Vulnerability Scanners)* ≠ **Scanners de Portas**

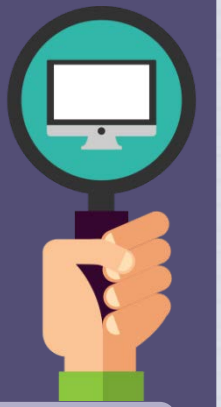
- Porque estes são capazes de explorar as redes por informações muito detalhadas.
- Identificam nomes e grupos de usuários expostos.
- Mostram compartilhamentos abertos de rede abertas.
- E expõem problemas de configuração e outras vulnerabilidades de um servidor.

- **GFI LANguard Network Scanner;**
- **IBM ISS;**
- **IBM Foundstone - uma divisão da McAfee.**



Vulnerability Scanners e Packet Sniffers

É uma ferramenta de rede que coleta e analisa cópias de pacotes da rede.



Espionar o tráfego da rede.

- **Estar em uma rede da própria organização;**
- **Estar sob a autorização direta dos donos da rede;**
- **Ter o conhecimento e o consentimento dos usuários;**
- **Ter uma razão comercial justificável para fazê-lo.**

Filtros de Conteúdo e Trap and Trace

Filtro de Conteúdo

- **Software**
- **Dispositivo de Hardware**

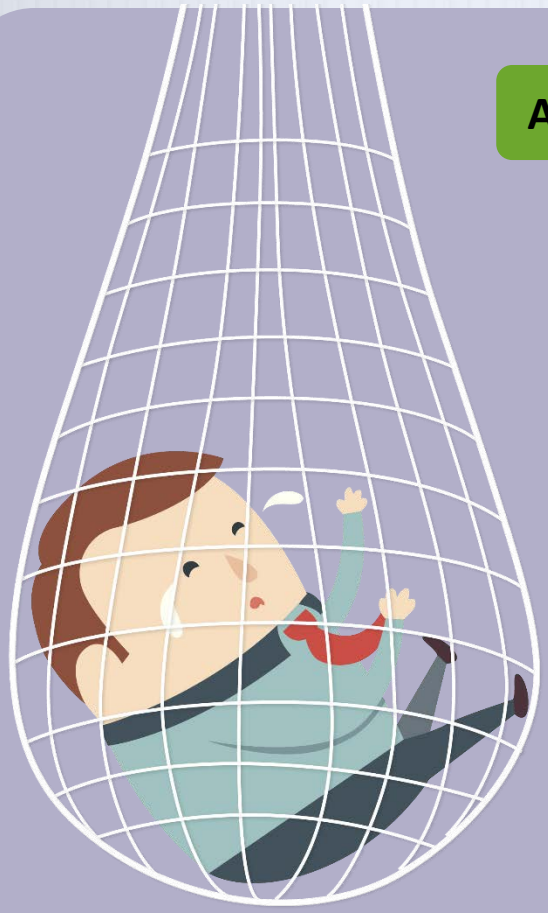
- Permite aos administradores restringir o conteúdo que entra em uma rede.
- Requer configuração extensa e atualização constante da lista de endereços de destinos aceitos ou endereços de e-mails restritos.

Restrição do acesso a sites

Restrição de e-mail spam

Garantem que colaboradores não usem recursos de rede inadequadamente.

Filtros de Conteúdo e Trap and Trace



Aplicações de Armadilha e Rastreamento (*Trape and Trace*)

Trap (armadilha)

- Descreve o desenho de um software para atrair os atacantes que estão em busca das áreas internas de uma rede.

Trace (rastreamento)

- É um processo pelo qual a organização tenta determinar a identidade de alguém descoberto em áreas não autorizadas da rede ou sistemas.

Gerenciando Ferramentas de Análise e Scanning

Desenvolver um programa usando recursos internos, contratados ou de um provedor de serviços terceirizado.

Periodicamente varrer seus sistemas e redes, em busca de vulnerabilidades com as ferramentas que um hacker típico pode usar.

- Não são pessoas e, portanto, não simulam o comportamento mais criativo de um atacante humano;
- Apenas problemas previamente conhecidos podem ser detectados;
- Estão sujeitas a erros humanos;
- Estão propensas a erros, falhas e vulnerabilidades próprias;
- Você recebe o que você paga;
- Alguns governos, agências, instituições e universidades estabeleceram políticas ou leis que protegem o direito do usuário individual de acessar o conteúdo;
- O uso e a configuração da ferramenta devem obedecer a uma política explicitamente articulada e a política deve fornecer exceções válidas.

Termos da Criptografia

A criptografia é o processo que converte uma mensagem original, em uma que não pode ser compreendida por pessoas não autorizadas.

Criptologia

Criptografia

kryptos

Oculto

Graphein

Escrever

Criptoanálise

Analyein

Quebrar

Descreve os processos envolvidos na codificação e decodificação de mensagens para que outros não possam compreendê-las.

Processo de decifrar a mensagem original (ou plaintext) de uma mensagem criptografada (ou texto cifrado), sem conhecer os algoritmos e as chaves usadas para executar a criptografia.

Termos da Criptografia

- **ALGORITMO:** Método usado para converter uma mensagem não criptografada em criptografada.
- **CIPHER: T**ransformação dos componentes individuais não criptografados em criptografados.
- **CRIPTOGRAFIA OU CRIPTOGRAMA:** Mensagem criptografada ou codificada ininteligível, resultante de uma criptografia.
- **CRYPTOSYSTEM:** Conjunto de transformações necessárias para converter uma mensagem não criptografada em criptografada.
- **DECIFRAR:** Para descriptografar ou converter texto cifrado para texto simples.
- **ENCIPHER (decifrador):** Para criptografar ou converter texto simples em texto cifrados.
- **KEY (chave): I**nformação usada em conjunto com o algoritmo para criar o texto cifrado a partir do texto simples; Pode ser uma série de bits usados em um algoritmo matemático, ou o conhecimento de como manipular o plaintext (texto simples).
- **KEYSPACE:** Todo o intervalo de valores que podem ser usados para construir uma chave individual.
- **PLAINTEXT:** Mensagem original não criptografada que é criptografada e resulta de uma decodificação bem-sucedida.
- **STEGANOGRAPHY:** Processo de esconder mensagens, geralmente dentro de imagens gráficas.
- **FATOR DE TRABALHO:** Quantidade de esforço (geralmente expressa em horas) requerida para realizar a criptoanálise em uma mensagem codificada.

Criptografia Segundo a ISO/IEC 27002

1. Gerar chaves para diferentes sistemas e aplicações;
2. Obter certificações;
3. Distribuir chaves para entidades e pessoas, incluindo sua ativação quando forem recebidas;
4. Armazenar essas chaves, incluindo o acesso e autorização das mesmas por parte de usuários selecionados;
5. Modificar ou atualizar as chaves em relação a regras e algoritmos quando for necessário;
6. Lidar com chaves comprometidas;
7. Recuperar chaves perdidas ou corrompidas;
8. Destruir chaves após uso ou comprometimento;
9. Monitorar acessos e uso das chaves.

Criptografia Segundo a ISO/IEC 27002

Aspectos:

- Deve haver uma abordagem da direção em relação à criptografia e seu uso na organização, inclusive os princípios gerais sob os quais a informação do negócio deve ser protegida.

Riscos Averiguados:

- O nível de proteção deve ser definido, usando o tipo, o nível e a qualidade de algoritmo que melhor se adequa.
- O uso de criptografia para informações transmitidas via mobile ou mídias removíveis devem ser consideradas também.

- Medidas para proteção das chaves de criptografia e descriptografia em caso de perda ou comprometimento; definição de papéis e responsabilidades; gestão e geração eficiente das chaves de segurança; adoção de padrões na implementação.

Regulamentação de Controles de Criptografia

- As restrições à importação e/ou exportação de hardware e software de computador para execução de funções criptográficas.

- Restrições à importação e/ou exportação de hardware e software de computador que foi projetado para ter funções criptográficas embutidas.

- Restrições quanto ao uso de métodos obrigatórios ou discricionários de acesso, pelas autoridades dos países, à informação criptografada por hardware ou software, para fornecer confidencialidade ao conteúdo.

- Restrições no uso de criptografia.

Assessoria Jurídica

Controles de Criptografia

- **CONFIDENCIALIDADE**. Uso da criptografia para proteger informações críticas ou sensíveis, armazenadas ou transmitidas.

- **INTEGRIDADE**. Uso de assinaturas digitais e códigos de autenticação para verificar a autenticidade e integridade das informações transmitidas ou armazenadas.

- **AUTENTICAÇÃO**. Uso da criptografia para autenticar usuários e outras entidades requerendo a acesso a sistemas e recursos.

- **CHECAGEM**. Uso das técnicas de criptografia para criar evidências da ocorrência ou não ocorrência de eventos e ações.

- **Deve ser desenvolvida e implementada uma política para uso, proteção e ciclo de vida de chaves criptográficas.**
- **Precisa considerar os requisitos para implementação dessas chaves ao longo de todo o ciclo – desde sua geração, passando pelo armazenamento, recuperação, distribuição e até exclusão.**

Cifras Comuns

Algoritmos → **3 Funções de Cifras (ciphers):**

Substituição

- Substitui um valor por outro.
- **SUBSTITUIÇÃO MONO ALFABÉTICO:** usa somente um alfabeto.
- **SUBSTITUIÇÃO POLI ALFABÉTICO:** usa dois ou mais alfabetos.

Transposição

- Reorganiza os valores dentro de um bloco para criar o texto cifrado. Isso pode ser feito no nível de bit ou no nível de byte (caractere).

XOR

- O fluxo de bits é submetido a uma função **XOR booleana** contra algum outro fluxo de dados, normalmente um fluxo de chaves. XOR funciona da seguinte forma:

- **'0' XOR' com '1' resulta em '1'. (0 ^ 1 = 1)**
- **'0' XOR' com '0' resulta em '0'. (0 ^ 0 = 0)**
- **'1' XOR' com '0' resulta em '1'. (1 ^ 0 = 1)**
- **'1' XOR' com '1' resulta em '0'. (1 ^ 1 = 0)**

Cifras Comuns

Se os dois valores são os mesmos, você recebe **"0"**; Se não, você recebe **"1"**. Este processo é reversível. Ou seja, se você faz um **XOR** no texto cifrado com o fluxo de chaves, você obtém o texto sem formatação.

- **'0100 0001' Plaintext (texto simples);**
- **'0101 1010' Key strearn (fluxo de chave);**
- **'0001 1011' Ciphertext (texto cifrado).**

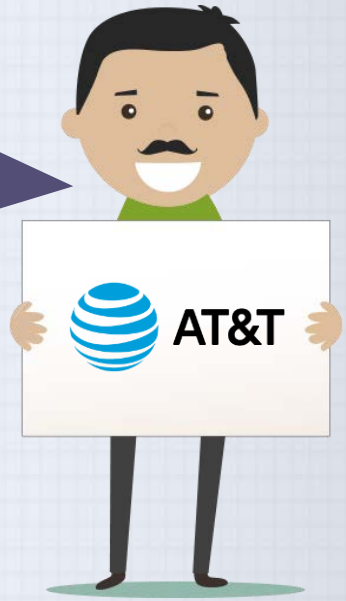
Cifras de Verman e Running Key Cipher

Vernam Cipher → **One-Time Pad (OTP)**

Cifra de uso único ou chave de uso único.

Os valores deste OTP são adicionados ao bloco de texto, e a soma resultante é convertida em texto.

Usa um conjunto de caracteres que são usados para operações de criptografia apenas uma vez e depois descartadas.



Book → **Running Key Cipher**

Método usado em textos, normalmente de um livro, com uma solução para descriptografar uma mensagem.

(1) saber qual livro usar

(2) lista de códigos representando o número da página, o número da linha e o número da palavra do plaintext.

Cifras de Verman e Running Key Cipher

Requerem o mesmo algoritmo e chaves das quais serão usadas para codificar e descodificar uma mensagem.

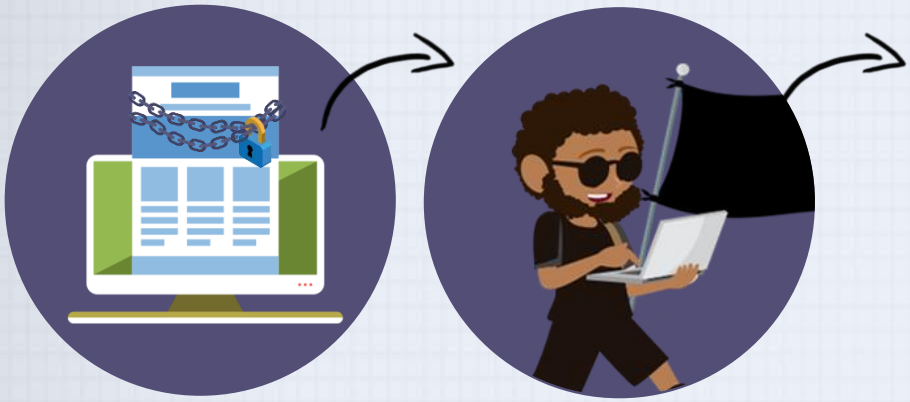
Criptografia de chave privada ou criptografia simétrica.

Criptografia

Criptografar é utilizar mecanismos que fazem a codificação da informação de um jeito que só quem é o dono, ou autorizado do dono, possa ler.

POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

Controles Criptográficos



Criptografia

Integridade → **Autenticidade**

Tokens **Certificados**

Outros tipos de assinaturas digitais

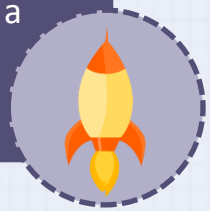
Há dois tipos de chaves de segurança:

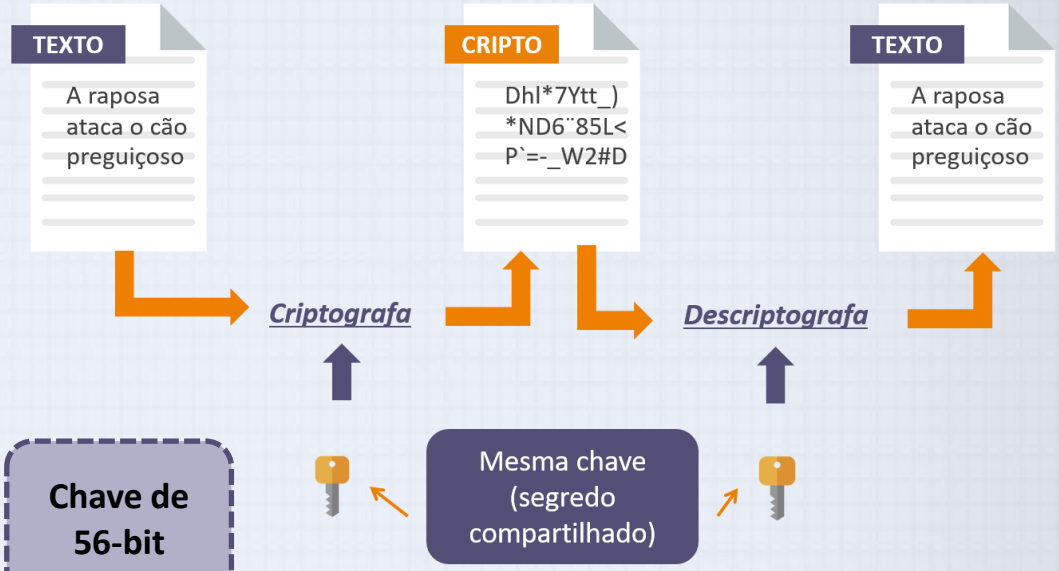
Pública

Privada

Criptografia Simétrica

Obter uma cópia da chave para o receptor, um processo que deve ser realizado fora do meio de comunicação utilizada para enviar e receber a mensagem para se evitar a interceptação.





Padrão de Criptografia de Dados (DES - Data Encryption Standard).

Chave de 56-bit

Foi substituído por:

Padrão Avançado de Encriptação (AES - Advanced Encryption Standard).

Criptografia Assimétrica

Ou criptografia de chave pública

Qualquer chave pode ser usada para criptografar ou descriptografar a mensagem.

A criptografar

descriptografar

PROBLEMA: ela requer quatro chaves para realizar uma única conversa entre duas partes.

Autoridade de Certificação (CA - Certification Authority)

criptografar

B

descriptografar

Criptografia Assimétrica

Pré-requisitos:

- O CA deve se certificar que a chave pública que alguém pede realmente pertence a parte que a está gerando.
- A matemática envolvida deve garantir 100% que sem as chaves privadas ninguém pode decifrar a mensagem de alguém que usa a chave pública correspondente para decifrar.

- Mantidas em absoluto segredo;
- Guardadas de forma segura contra perda;
- Revogadas quando uma violação acontece ou é suspeita;
- Únicas.

Assinatura Digital

Chave Privada

É um identificador único, que pode ser usada como uma assinatura eletrônica ou digital.

Funções Hash

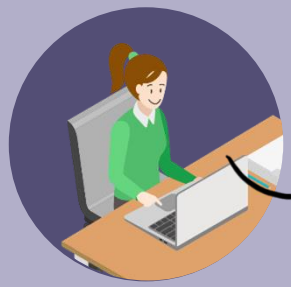
Garantirá que estas chaves possam ser usadas para provar a sua identidade e/ou integridade.

São algoritmos matemáticos que utilizam funções criptográficas conhecidas como MD5 (*Message-Digest algorithm 5*).

- Gerar um número relativamente pequeno de bits, que são inseridos como sufixos de uma grande quantidade de dados que serão transmitidos, acessados, lidos, armazenados, etc. ponto a ponto.

Assinatura Digital

Exemplo:



Maria gera um hash de um documento e criptografa

Chave privada

Para o João descriptografar este documento, ele utiliza um hash que usa a chave pública da Maria.

Chave Pública

É claro que isso só funciona quando a Maria mantém sua chave privada secreta e se há provas definitivas de que ela é realmente a "dona" de sua chave pública.

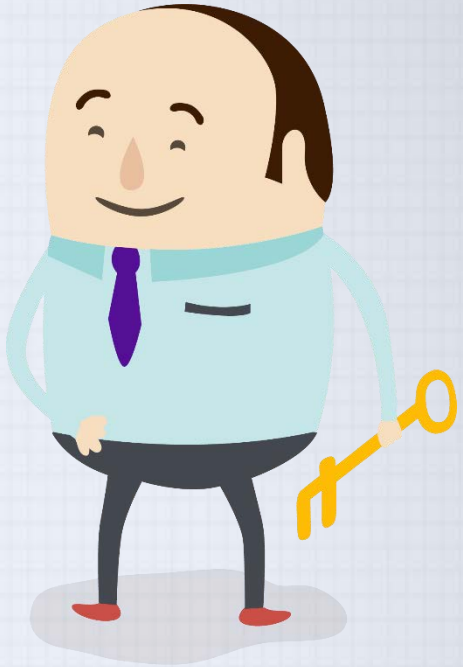
RSA (Rivest-Shamir-Aldeman)

- Popular sistema de criptografia de chave pública. Modelo proprietário.
- 1º algoritmo de chave pública desenvolvido para uso comercial.
- Integrado no Microsoft Internet Explorer e no Netscape Navigator.

RSA Encryption Scheme-Optimal Asymmetric Encryption Padding (RSAES-OAEP)

RSA Signature Scheme e o Apêndice - Probabilistic Signature Scheme (RSASSA-PSS).

Infraestrutura de Chave Pública

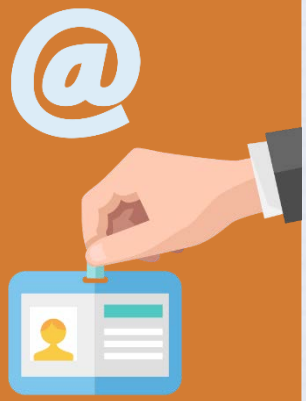


Chave Pública (*PKI - Public Key Infrastructure*)

É todo o conjunto de hardware, software e sistemas de criptografia necessários para implementar a criptografia de uma chave pública.

Sistemas PKI se baseiam em criptografia de chave pública e incluem os certificados digitais e autoridades de certificação.

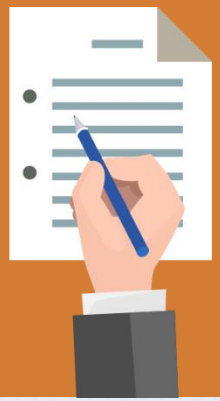
Autenticação



Integridade

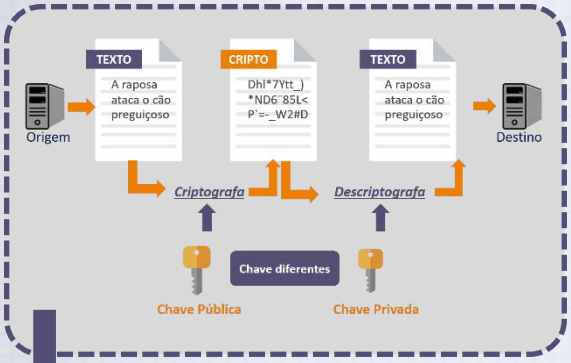
Confidencialidade

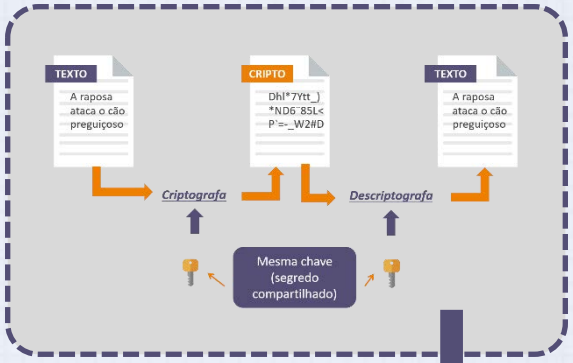
Autorização



Não rejeição

Sistema Híbrido de Criptografia





Sistema Híbrido

Baseado no método de troca de chaves Diffie-Hellman, que fornece uma maneira de trocar chaves privadas sem exposição a terceiros.

A criptografia assimétrica não exige a troca de chaves fora do canal usado para a troca da mensagem, ela pode ser usada para transmitir chaves simétricas em uma abordagem híbrida.

É mais eficiente do que a Criptografia Assimétrica para o envio de mensagens.

1. João cria a chave de sessão; **2.** Criptografa a mensagem; **3.** Recebe a chave pública de Maria. **4.** Usa sua chave pública para criptografar tanto a chave de sessão quanto a mensagem que já está criptografada. **5.** Transmite todo o pacote para Maria, que usa sua chave privada para descriptografar o pacote contendo a chave de sessão e a mensagem criptografada. **6.**Usa a chave de sessão para descriptografar a mensagem. **7.** Maria pode então continuar a conversa eletrônica usando apenas a chave de sessão simétrica mais eficiente.

João - Empresa XYZ

Maria - Empresa ABC

Usando Controles Criptográficos

Organizações com necessidade e capacidade de usar controles criptográficos, podem usá-los para apoiar seus negócios da seguinte forma:

- Confidencialidade e integridade do e-mail e seus anexos;
- Autenticação, confidencialidade, integridade e não repúdio das transações em e-commerce;
- Autenticação e confidencialidade de acesso remoto através de conexões VPN;
- Maior padrão de autenticação quando usado para complementar de sistemas de controle de acesso.

Segurança nos E-mails

Secure Multipurpose Internet Mail Extensions - S/MIME (Extensões de Correio da Internet Multipropósito e Segurança);

Privacy Enhanced Mail – PEM (Correio com Privacidade Reforçada);

Pretty Good Privacy – PGP (Privacidade Muito Boa).

Baseia-se na codificação MIME (*Multipurpose Internet Mail Extensions*) formando e adicionando criptografia e autenticação via assinaturas digitais baseadas em sistemas de criptografia de chave pública.

Sugerido pelo IETF (*Internet Engineering Task Force*) como um padrão que funciona com criptografia de chave pública. Usa criptografia de chave simétrica 3DES e RSA para troca de chaves e assinaturas digitais.

Desenvolvido por Phil Zimmerman, usa a IDEA Cipher, um algoritmo de criptografia de blocos de chave simétrica de **128 bits com blocos de 64 bits**, para a codificação de mensagens. Usa o RSA para troca de chaves simétricas e para suporte a assinaturas digitais. O PGP confia em um modelo de *"web of trust"* para compartilhar informações importantes com facilidade, embora com alguma perda no grau de controle e informação chave.

Segurança nos E-mails

Com o PGP

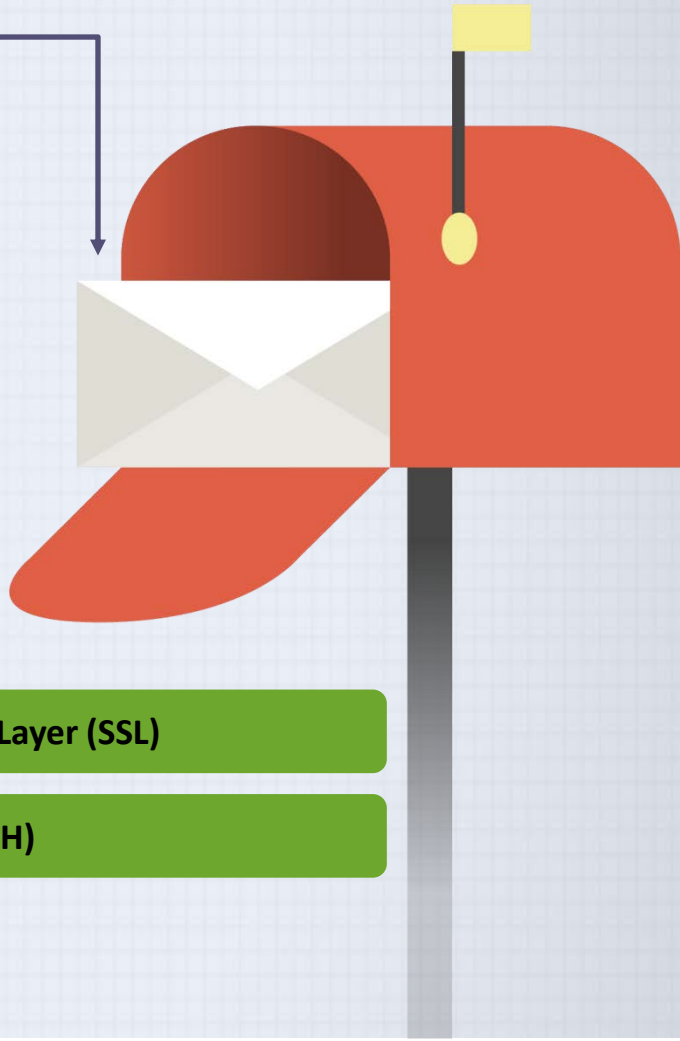
Então o USUÁRIO A presume ter uma relação de confiança com o USUÁRIO C, e pode trocar informações criptografadas com ele.

Protegendo a Web

PGP → PEM → S/MIME

Sistemas de Criptografia → Atividades da Web

Sites de comércio eletrônico



- Secure Electronic Transactions (SET)
- Secure Hypertext Transfer Protocol (SHTTP)
- IP Security (IPSec)
- Secure Sockets Layer (SSL)
- Secure Shell (SSH)

Protegendo a Web

Secure Electronic Transactions (SET)

- Desenvolvido pela **MasterCard e VISA** em 1997;
- Fornece proteção contra fraude em pagamento eletrônico.
- Criptografa as transferências de cartão de crédito com DES para criptografia e RSA para troca de chaves.

Secure Sockets Layer (SSL)

- Desenvolvido pela **Netscape** em 1994.
- Ele usa um número de algoritmos, mas depende principalmente de RSA para transferência de chaves e em IDEA, DES ou 3DES para transferência de dados baseada em chave simétrica criptografada.

Protocolo Seguro de Transferência de Hipertexto ou Secure Hypertext Transfer Protocol (SHTTP)

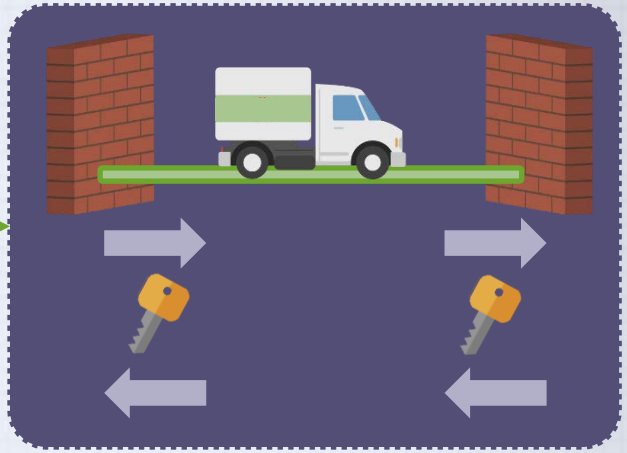
- É uma versão criptografada do HTTP, fornece transações de comércio eletrônico seguras, bem como páginas da Web criptografadas para transferência segura de dados pela Web, usando vários algoritmos diferentes.

Secure Shell (SSH)

- Fornece segurança para conexões de acesso remoto em redes públicas usando serviços de autenticação entre um cliente e um servidor e é usado para proteger ferramentas que usam a emulação de terminal, gerenciamento remoto e transferência de arquivos.

IPSec

IP Security (IPSec) — **1** — **IETF IP Protocol Security Working Group.**



Combina vários sistemas de criptografia diferentes, tais como:

- Intercâmbio de chaves Diffie-Hellman para derivar material-chave entre pares em uma rede pública;
- Criptografia de chave pública para a assinatura das trocas Diffie-Hellman para garantir a identidade das partes;
- Algoritmos de criptografia em massa, como DES, para criptografar os dados;
- Certificados digitais assinados por uma autoridade certificadora para atuar como cartões de identificação digital.

O protocolo de segurança IP em si, que especifica as informações a serem adicionadas a um pacote IP e indica como criptografar dados dos pacotes;

O Internet Key Exchange, que utiliza o intercâmbio de chaves assimétricas e negocia as associações de segurança.

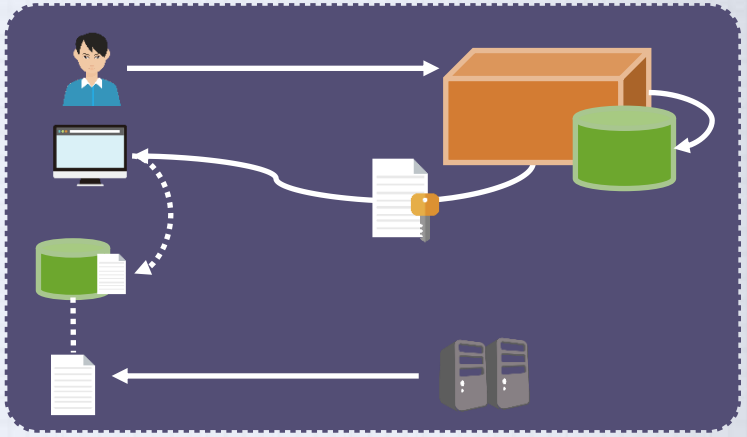
IPSec funciona em dois modos de operação: transporte e túnel.

TRANSPORTE: apenas os dados IP são criptografados, e não os próprios cabeçalhos IP.

TÚNEL: todo o pacote IP é criptografado e inserido e carregados em outro pacote IP.

Protegendo a Autenticação

É fornecer uma autenticação forte segura.



Kerberos

- Mantém um banco de dados contendo as chaves particulares de clientes e servidores.
- Supervisiona o processo de autenticação.
- Conhece essas chaves privadas e pode autenticar um nó de rede, seja no cliente ou no servidor.
- Gera chaves de sessão temporárias - isto é, chaves privadas dadas às duas partes em uma conversa.

Protegendo a Autenticação

- O **KDC (Key Distribution Center que gera e emite chaves de sessão)** conhece as chaves secretas de todos os clientes e servidores na rede.
- Inicialmente troca informações com o cliente e o servidor usando as chaves secretas.
- Autentica um cliente para um serviço solicitado em um servidor por meio do **TGS (Kerberos Ticket Granting Service, que fornece acessos para clientes que solicitam serviços)** e emite chaves de sessão temporárias para comunicações entre o cliente e o KDC, entre o servidor e o KDC e entre o cliente e o servidor.
- As comunicações ocorrem entre o cliente e o servidor usando as chaves de sessão temporárias.

http://ist.mit.edu.

Gerenciando Controles Criptográficos

Jamais perca as chaves;

Saiba com quem você está se comunicando;

Pode ser ilegal usar uma técnica específica de criptografia para se comunicar com algumas nações ou países;

Cada sistema criptográfico tem suas fraquezas;

Dê acesso apenas àqueles com uma necessidade real e comercial;

Ao colocar confiança em uma autoridade de certificação, pergunte "quem vigia os as autoridades de certificação?";

Não há segurança na obscuridade. Só porque um sistema é secreto não significa que é seguro.

Tratamento de Mídias

- ... o conteúdo de qualquer meio magnético reutilizável seja destruído, caso venha a ser retirado da organização;
- ... seja requerida a autorização para remoção de qualquer mídia da organização e mantido o registro dessa remoção como trilha de auditoria;
- Ser guardada de forma segura em um ambiente protegido, de acordo com as especificações do fabricante;
- Usar técnicas de criptografia para proteger os dados na mídia removível;
- Os dados devem ser transferidos para uma mídia nova antes de se tornar ilegíveis;
- Múltiplas cópias de dados valiosos devem ser armazenadas em mídias separadas;
- As mídias removíveis devem ser registradas;
- As mídias removíveis devem ser habilitadas apenas se houver uma necessidade do negócio;
- Onde houver necessidade do uso de mídia removível, a transferência da informação deve monitorada;
- Documentar os procedimentos e níveis de autorização.

Transferência e Descarte de Mídias

- Mídias com informações confidenciais devem ser guardadas e destruídas de forma segura e protegida.
- Haver procedimentos para identificar os itens que requerem descarte seguro.
- É mais fácil implementar a coleta e descarte seguro de todas as mídias do que separar o conteúdo que seja sensível de uma mídia.
- Muitas organizações oferecem serviços de coleta e descarte de mídia, por isso, cuidado na seleção deste fornecedor.
- O descarte de itens sensíveis deve ser registrado, sempre que possível, para manter uma trilha de auditoria.
- O acúmulo de muitas mídias pode fazer com que uma grande quantidade de informação não sensível, torna-se sensível.
- Equipamentos danificados contendo dados sensíveis podem exigir uma avaliação de riscos para determinar se é recomendado que os itens sejam destruídos fisicamente ou enviados para conserto ou descarte.

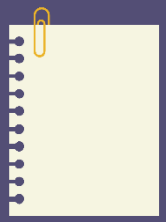
Transferência e Descarte de Mídias

- O meio de transporte ou o serviço de mensageiros devem ser confiáveis;
- Definir uma relação de portadores autorizados em concordância com o gestor;
- Estabelecer procedimento para a verificação da identificação dos transportadores;
- Transportar com embalagem protegidas contra quaisquer danos físicos e que possam reduzir a possibilidade de restauração dos dados como a exposição ao calor, umidade ou campos eletromagnéticos;
- Registrar e armazenar os logs, identificando o conteúdo da mídia, a proteção aplicada, bem como os registros dos tempos de transporte entre a organização e o destino final.

Transferência Eletrônica

- interceptação
- desvio
- cópia
- destruição
- modificação

- Criar um padrão de proteção para os anexos.



- Conscientizar os usuários do que não deve ser enviado por e-mail.

- Definir a responsabilidade dos colaboradores, dos parceiros e fornecedores.

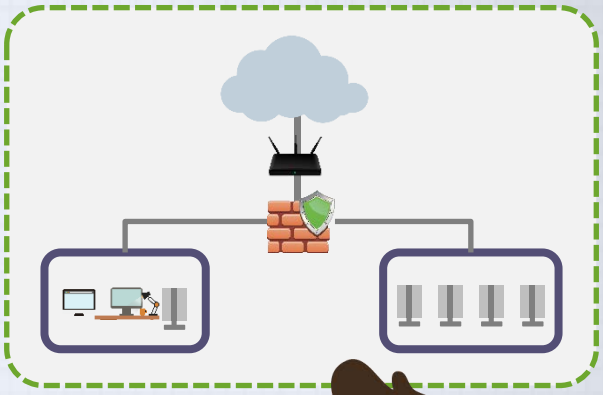
- Cuidado é o com as secretarias eletrônicas.

Transferência Eletrônica

- Ter alguma forma de rastrear;
- Seguir um padrão para a embalagem e transmissão;
- Especificar um responsável;
- Possuir algum tipo de acordo nos casos de custódia;
- Ter normas técnicas para gravação e leitura de informações e softwares;
- Ter normas para identificação de portadores;
- Deixar claro quem tem obrigações no caso de incidentes de segurança da informação, como perda de dados.

Segurança em Redes

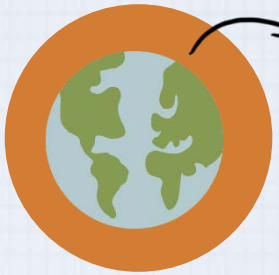
- proteção dos serviços
- confidencialidade
- acesso não autorizado
- integridade



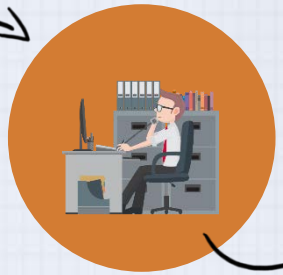
- Quais as redes e serviços de redes que são permitidos de serem acessados;
- Quais os procedimentos de autorização para determinar quem tem permissão de acesso;
- Quais os procedimentos e controles para proteger o acesso a rede;
- Meios usados para acessar a rede: Meios físicos, Wi-Fi, rede dedicada, VPN, etc.;
- Requisitos de autenticação de usuário para acessar os serviços da rede;
- Como será feito o monitoramento do uso dos serviços da rede.

Segregação de Redes

Segregar a rede é um método de controlar a segurança da informação em grandes redes, pois se divide em diferentes domínios de redes.



Domínio de acesso público

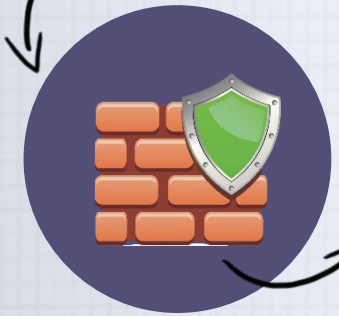


... de estação de trabalho

... de servidor

A SEGREGAÇÃO pode ser feita usando diferentes redes físicas ou diferentes redes lógicas. EX.: VPN.

O PERÍMETRO de cada DOMÍNIO deve ser bem definido.



AVALIAÇÃO DE REQUISITOS

Deve ser feita de acordo com a política de controle de acesso, os requisitos de acesso, o valor e a classificação da informação processada, e que leve em conta o impacto no desempenho e no custo do uso da tecnologia gateway.

Pronto para o próximo?

Curso Preparatório para Certificação
Em Gestão de Segurança da Informação Avançada – Baseada na ISO/IEC 27002:2013

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 9

Arquiteturas de Segurança

Definição de Arquitetura

Arquitetura

Biblioteca da ITIL® na Fase Desenho de Serviços do Ciclo de Vida de Serviço.

"A estrutura de um sistema ou de um serviço de TI, incluindo os relacionamentos dos componentes uns com os outros e com o ambiente em que se encontram. A arquitetura também inclui os padrões e as orientações que guiam o desenho e a evolução do sistema."

Compreende os princípios de desenho para: → **Os próprios objetos;** → **Suas relações;** → **Interação com seu ambiente.**

Exemplos:

- Um sistema de informação incluindo hardware, software e aplicações;
- Um sistema de gestão, incluindo múltiplos processos que são planeados e geridos em conjunto, como um Sistema de Gestão da Qualidade;
- Um sistema de gerenciamento de banco de dados ou sistema operacional que inclua muitos módulos que são projetados para executar um conjunto de funções relacionadas.

Definição de Arquitetura

Arquitetura de Segurança:

- Um conjunto de entidades relacionadas, que trabalham em conjunto para alcançar um objetivo de segurança geral.

Existem dois pontos de vista de segurança, para alcançar os objetivos:

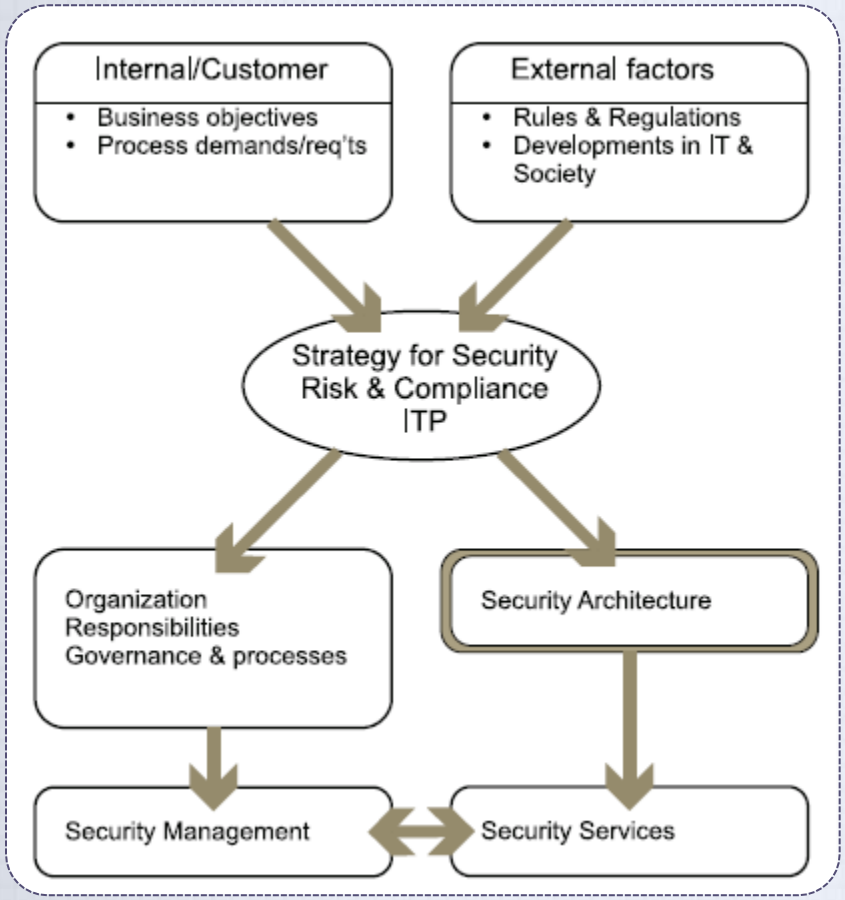
Aspecto funcional ou utilidade.

Certa funcionalidade de segurança será oferecida, o que torna a entidade adequada para o propósito, que é estabelecer um ambiente seguro.

Aspecto não funcional ou garantia.

Uma entidade que a segurança não está comprometida, mas também não pode ser ignorada, o que a torna adequada para uso em um ambiente seguro.

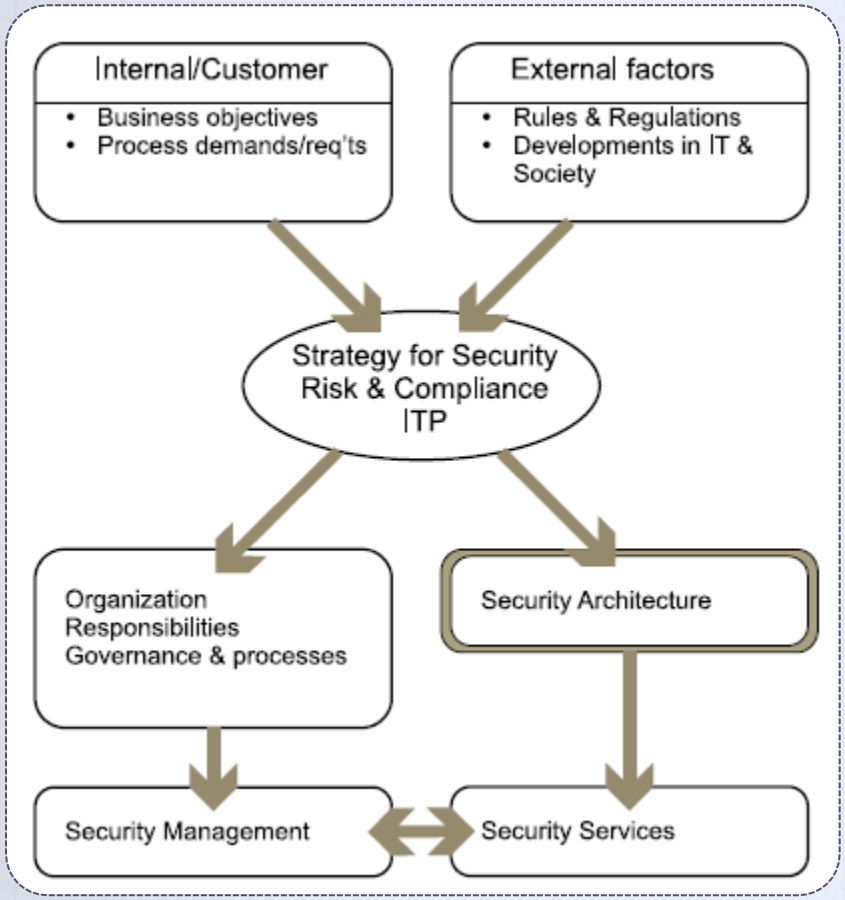
Posicionamento da Arquitetura de Segurança



A arquitetura faz um relacionamento com os clientes e colaboradores internos, interagindo com os objetivos de negócios e os processos de Demanda e Requisição de Serviços.

Faz um relacionamento também com os fatores externos, através das regras e regulamentos e da comunidade de desenvolvimento de TI.

Posicionamento da Arquitetura de Segurança



Posicionamento da Arquitetura de Segurança

A ESTRATÉGIA faz as fronteiras do que pode ser feito centralmente e o que é uma responsabilidade local.

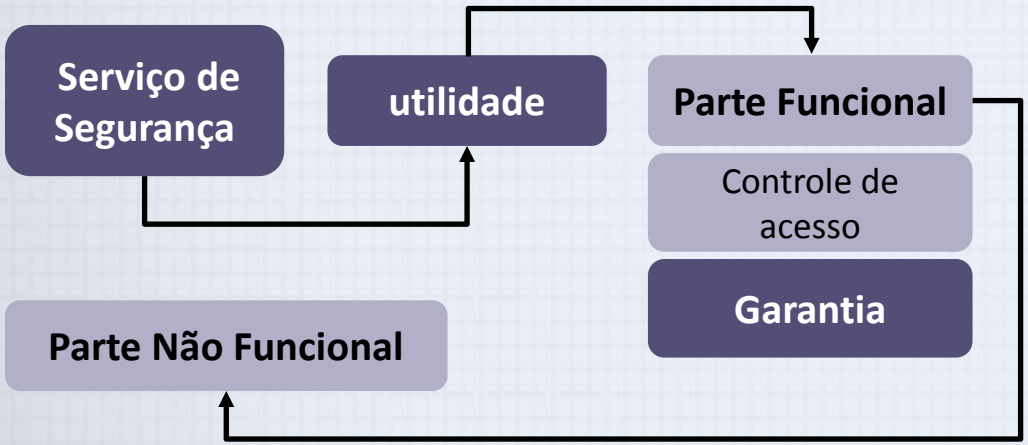
A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO traduz os objetivos de negócios, com o apoio da AVALIAÇÃO DE RISCOS, e com os OBJETIVOS DE CONTROLE, muito usado através do Framework do CobiT ®

Os OBJETIVOS DE CONTROLE são realizados através de um conjunto de controles que podem incorporar processos, fazer parte da cultura de profissionais de TI ou serem implementados no domínio da informação e TI.

Elementos de Arquitetura de Segurança

Os serviços da arquitetura de segurança são traduzidos em proteção:

- No nível da informação / dados;
- No nível de aplicação;
- Na infraestrutura geral de suporte (plataformas, redes, sistemas operacionais, aplicativos genéricos, middleware, etc.);
- Em um ambiente mais amplo, incluindo aspectos culturais e físicos.



Outros elementos da definição de um serviço de segurança incluem:

- Garantia, confiabilidade, adequação e qualidade do serviço;
- Atividades e controles de gerenciamento. EX.: métricas, funções e responsabilidades.

Elementos de Arquitetura de Segurança

A arquitetura de segurança também define os serviços de segurança e as regras para implementação.

Centralizados

Descentralizados

- **Podem ser oferecidos em sub arquiteturas de informação/dados, aplicação, infraestrutura e meio ambiente.**
- **Podem ser implementados através de uma gama de soluções técnicas.**

Princípios do Desenho de Serviços de Segurança

As principais características para definição de um serviço de segurança incluem:

- Funcionalidade: a definição do serviço;
- Modelos de confiança: suposições sobre a confiabilidade (contínua e ininterrupta) do próprio serviço e seu ambiente;
- Condição para uso efetivo: pré-requisitos, dependências e possível interação:
- **Limites:** o serviço é limitado a um determinado domínio?
- **Fontes confiáveis:** são necessárias e, em caso afirmativo, como são identificadas e autenticadas?
- **Consciência do ambiente:** o serviço pode obter qualquer informação necessária sobre ambiente?
- **Interação:** se o serviço requerer entrada ou comunicação com outros serviços, como será a interação?
- **Suposições de confiança:** que proteção é assumida em camadas subjacentes, ou seja, de outros serviços? Existe uma parte confiável da infraestrutura? O que deve ser considerado como invasivo ou amigável?
- **Sessões seguras:** é possível estabelecer uma comunicação segura e, em caso afirmativo, que protocolos são suportados e como é que a identificação, autenticação, autorização e controle de acesso?

Princípios do Desenho de Serviços de Segurança

Gerenciamento de serviço de segurança:

- Centralizado, descentralizado, com relatórios, registos, monitorização, alerta;
- Papéis e responsabilidades;
- Propriedade, responsabilidade, delegação;
- Gestão da confiança.

Resiliência:

- Endurecimento (*hardening*);
- Gerenciamento de vulnerabilidades;
- Capacidade de recuperação;

Gerenciamento de desempenho e capacidade:

- Recuperação e planeamento de contingência.

Princípios de Desenho Para Ambientes Seguros

- Isolamento
- Padrões de segurança contra falhas
- Mediação completa
- Design aberto
- Privilégios
- Limitar funcionalidade ou privilégio
- Resiliência
- Adaptabilidade
- Diversidade
- Redundância
- Ergonomia
- Zoneamento (sub-redes; DMZ)
- Deve ser gerenciável
- Relatório

Modelos de Arquitetura de Segurança

Uma arquitetura de segurança orientada a serviços...

Deve definir quais serviços de segurança são fornecidos, de forma centralizada ou descentralizada; onde os serviços são fornecidos; quais mecanismos de segurança serão obrigatórios, opcionais e suportados.

- Modelos de arquitetura de segurança ilustram implementações de segurança de informações e podem ajudar as organizações a fazerem rapidamente as melhorias através de adaptações.

- Modelos formais exemplificam como certos métodos de segurança podem ser incorporados em um sistema de informação.

Modelos mais comuns:

- Base de Computação Confiável
- ITSEC
- Critérios Comuns (CC)
- Modelo de Confidencialidade Bell-LaPadula
- Modelo de Integridade Biba
- Modelo de Integridade Clark-Wilson
- Modelo de Controle de Acesso Graham-Denning
- Modelo Harrison-Ruzzo-Ullman
- Modelo de Brewer-Nash (parede chinesa)
- A série ISO 27000

Base de Computação Confiável

Critério de Avaliação do Sistema de Computação Confiável → **TCSEC – (Trusted Computer System Evaluation Criteria)** → **"Orange Book" (Livro Laranja)** → **"Critérios Comuns"**

É um padrão **do DoD (Departamento de Defesa do Governo dos Estados Unidos)** que define os critérios para avaliar os controles de acesso em um sistema de computador.

Série Rainbow (Arco-Íris)

- **Define uma base de computação confiável *(TCB - Trusted Computing Base)* combinando todo o hardware, firmware e software responsável pela aplicação da política de segurança.**
- **Define os requisitos básicos para avaliar a eficácia dos controles de segurança de um computador e um sistema.**
- **É utilizado para avaliar, classificar e selecionar sistemas para o processamento, armazenamento e recuperação de informações confidenciais.**

Base de Computação Confiável

C B A

C1, C2, B1, B2, B3 e A1

4 divisões: D, C, B e A

- D - trata da proteção mínima;
- C - Proteção discricional:
  - ✓ C1 - Proteção de segurança discricional;
  - ✓ C2 - Proteção de Acesso Controlado.
- **B** - Proteção obrigatória:
  - ✓ B1 - Proteção marcada de segurança...
  - ✓ B2 - Proteção estruturada;
  - ✓ B3 - Domínios de segurança.
- **A - Proteção verificada:**
  - A1 - Design verificado (nível de certificação);
  - A1 - Reservado apenas para sistemas de autoproteção, top-level.

ITSEC

- **O ITSEC (*Information Technology System Evaluation Criteria* - Critérios de Avaliação do Sistema de Tecnologia da Informação) - é um conjunto internacional de critérios para avaliação de sistemas de computadores, é muito semelhante ao TCSEC.**

Metas de Avaliação (ToE - Targets of Evaluation)

- São comparadas com as especificações detalhadas das funções de segurança, resultando em uma avaliação da funcionalidade dos sistemas e testes de penetração.

- **ITSEC** - Foi, em grande parte, funcionalmente substituída pelos Critérios Comuns que detalharemos a seguir.

TCSEC e os Critérios Comuns:

E1 – EAL2

E6 – EAL7

- Classifica os produtos numa escala de E1 (nível mais baixo), até o E6 (nível mais alto).

Critérios Comuns (CC)

Common Criteria ou CC

São as normas internacionais **ISO/IEC 15408** para certificação de segurança de computadores.

Profissionais de Segurança

Organizações de Segurança

Consideram o Common Criteria o sucessor do TCSEC e do ITSEC.

Agência Nacional de Segurança (NSA)

Instituto Nacional de Padrões e Tecnologia (NIST)

Critérios Comuns (CC)

- Alvo de Avaliação (ToE - *Target Of Evaluation*);
- Perfil de Proteção (PP - *Protection Profile*);
- Destino de Segurança (ST - *Security Target*);
- Requisitos Funcionais de Segurança (SFRs - *Security Functional Requirements*);
- Avaliação dos níveis de garantia (EAL - *Evaluation Assurance Levels*);

- **EAL1**: Testado funcionalmente - confiança na operação contra ameaças não graves;
- **EAL2**: Testado estruturalmente - mais confiança necessária, mas comparável com boas práticas de negócios;
- **EAL3**: Testado e verificado metodicamente - nível moderado de garantia de segurança;
- **EAL4**: Metodicamente Projetado, Testado e Revisado – nível rigoroso de garantia de segurança, mas ainda economicamente viável sem desenvolvimento especializado;
- **EAL5**: Projetado e testado de forma semiformal – certificação que requer desenvolvimento especializado acima dos produtos comerciais padrão;
- **EAL6**: Projetado, testado e verificado de forma semiformal - especificamente projetado para a segurança do ToE;
- **EAL7**: Projetado, testado e verificado de formalmente - desenvolvido para situações de alto risco ou para sistemas de alto valor.

Modelo de Confidencialidade Bell-LaPadula

Bell-LaPadula (BLP)

- **Utiliza um modelo matemático que ajuda a garantir a confidencialidade de um sistema de informação por meio de MACs (*Mandatory Access Controls*).**

- Um modelo que segue uma abordagem conceitual, na qual o conteúdo do sistema a ser modelado está sempre numa condição segura conhecida. Modelo provavelmente seguro.
- Um sistema que serve como um monitor de referência, que compara o nível de classificação dos dados com a apuração da entidade que solicita o acesso.
- Permite o acesso apenas se o apuramento for igual ou superior à classificação.
- As regras de segurança do BLP impedem que as informações sejam movidas de um nível de segurança mais alto para um nível de menor segurança.

Modos de Acesso:

Segurança simples ou propriedade de leitura - um sujeito em um dado nível de segurança não pode ler um objeto com um nível de segurança mais alto, ou seja, não pode "ler para cima".

Propriedade estrela ou de escrita - proíbe que um sujeito em um dado nível de segurança escreva para qualquer objeto em um nível inferior de segurança (não pode escrever-para-abaixo).

Modelo de Integridade Biba

Biba

Baseia-se na premissa de que os níveis mais elevados de confiança são mais dignos de confiança do que os mais baixos.

A intenção é providenciar controles de acesso que garanta que objetos ou sujeito não podem ter menos integridade como resultado de operações de leitura/gravação.

O modelo Biba atribui níveis de integridade a objetos e sujeitos usando duas propriedades:

- **Propriedade de integridade simples (leitura);**
- **Propriedade de integridade estrela (escrita).**

O modelo Biba garante que nenhuma informação de um sujeito possa ser passada para um objeto em um nível de segurança mais elevado. Isso evita a contaminação de dados de maior integridade com dados de baixa integridade.

Modelo de Integridade Biba

Isto é para evitar que a menor integridade do nível inferior "corrompa" a santidade do nível superior.

Um padre não pode ler (ou oferecer) missas ou orações escritas pelo Biba.

Modelo de Integridade Clark-Wilson

Clark-Wilson

- **Se baseia em princípios de controle de mudanças, ao invés de níveis de integridade. Foi projetado para um ambiente de negócio.**

1. **Nenhuma mudança por ser feita por sujeitos não autorizados;**
2. **Nenhuma mudança não autorizada pode ser feita por sujeitos autorizados;**
3. **A manutenção deve ser consistente, seja a interna como a externa.**

Consistência interna - o sistema faz o que é esperado, sem exceção**.**

Consistência externa - os dados no sistema são consistentes com dados semelhantes no mundo exterior.

Estabelece um sistema de relações sujeito-programa-objeto.

Que o sujeito não tem acesso direto ao objeto.

O sujeito que precisa acessar o objeto usando uma transação deve ser feito por meio de um programa validado.

Intenção é praticar um ambiente onde a segurança possa ser praticada através do uso de atividades separadas.

Modelo de Integridade Clark-Wilson

- **Controles do modelo Clark-Wilson:**
- Autenticação e identificação de sujeitos;
- Acesso a objetos por meio de transações bem formadas;
- Execução por sujeitos em programas restritos.

Modelo de Integridade Clark-Wilson

- **Os elementos do modelo Clark-Wilson são:**
  - Item de dados restritos (CDI - *Constrained Data Item*): Item de dados com integridade protegida;
  - Item de dados não sujeitos a restrições: Dados não controlados por Clark-Wilson, ou seja, são entradas não validadas ou quaisquer saídas;
  - Procedimento de verificação da integridade (IVP - *Integrity Verification Procedure*): Procedimento que escaneia os dados e confirma sua integridade;
  - Procedimento de transformação (TP - *Transformation Procedure*): Procedimento que permite somente mudanças a um item dado restrito.

Modelo de Controle de Acesso Graham-Denning

Graham-Denning

- Um conjunto de objetos;
- Um conjunto de sujeitos;
- Um conjunto de direitos.

Processo

1. Criar objeto;
2. Criar sujeito;
3. Excluir objeto;
4. Excluir sujeito;
5. Direito de acesso de leitura;
6. Direito de acesso de concessão;
7. Direito de acesso de exclusão;
8. Direito de acesso de transferência.

Domínio

- É o conjunto de restrições que controlam como os sujeitos podem acessar objetos.
- O conjunto de direitos orienta como os sujeitos podem manipular os objetos passivos.
- Este modelo descreve oito direitos de proteção primitiva, chamado COMANDOS, que os sujeitos podem executar para ter um efeito sobre outros objetos ou sujeitos.

Modelo Harrison-Ruzzo-Ullman

Harrison-Ruzzo-Ullman (HRU)

- Define um método que permite mudanças nos direitos de acesso, na adição e remoção de objetos e sujeitos, da qual é um processo que o modelo Bell-LaPadula não faz.

Ao implementar esse conjunto de direitos e comandos e restringi-los uma simples operação, é possível determinar, se e quando, um sujeito específico pode obter um direito específico para um objeto.

É construído sobre uma matriz de controle de acesso e inclui um conjunto de direitos genéricos e um conjunto específico de comandos, que incluem:

- Criar sujeito / criar objeto;
- Direito de entrar com nova permissão;
- Direito de excluir uma permissão;
- Destruir objeto / destruir sujeito.

Modelo de Brewer-Nash (Parede Chinesa)

Brewer-Nash

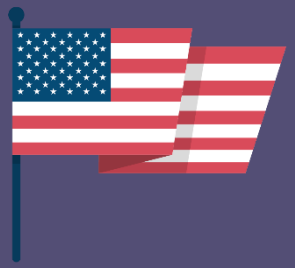
Parede Chinesa

- É projetada para evitar um conflito de interesse entre duas partes.

O modelo Brewer-Nash exige que os usuários selecionem um entre dois conjuntos conflitantes de dados, após isso, não podem acessar os dados conflitantes.

Modelos de Gerenciamento de Segurança

É evidente que existem muitos modelos de gerenciamento de segurança.



Agências Federais dos EUA.

Organizações Internacionais.

Modelos Proprietários

Centro de Recursos de Segurança de Computadores do NIST.

(http://csrc.nist.gov)

A série ISO 27000

Código de Práticas de Tecnologia da Informação para Gerenciamento de Segurança da Informação.

Originalmente publicado como o Padrão Britânico BS7799.

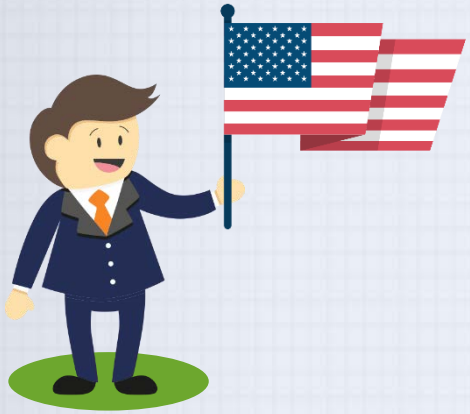
Em 2000

Foi adotado como um padrão internacional de segurança da informação pela Organização Internacional de Normalização (ISO) e pela Comissão Eletrotécnica Internacional (IEC) como ISO/IEC 17799.

- O documento foi revisado em 2005 (tornando-se ISO 17799:2005);
- Foi renomeado para ISO 27002 em 2007, para alinhá-lo com o documento ISO 27001;
- Finalmente, sofrendo a última atualização em 2013, sendo renomeado para a ISO 27002:2013.

Modelos de Segurança NIST

Centro de Recursos de Segurança Informática do NIST (http://csrc.nist.gov).



1

Estão publicamente disponíveis sem custo;

Eles estão disponíveis há algum tempo e, portanto, foram amplamente revistos por profissionais do governo e da indústria.

2

Referências na NIST:

- **SP 800-12** - Manual de Segurança do Computador;
- **SP 800-14** - Princípios e práticas de segurança geralmente aceito;
- **SP 800-18** - Guia para Desenvolvimento de Planos de Segurança;
- **SP 800-26** - Guia de autoavaliação de segurança - Sistemas de TI;
- **SP 800-30** - Gerenciamento de Risco para Sistemas de Tecnologia da Informação.

Teste M&#65533;dulo 9 - Arquiteturas de Seguran&#65533;a

Quiz - 4 questions

Last Modified: jul 21, 2017 at 08:19 PM

PROPERTIES

On passing, 'Finish' button:	Goes to Next Slide
On failing, 'Finish' button:	Goes to Next Slide
Allow user to leave quiz:	At any time
User may view slides after quiz:	At any time
Show in menu as:	Multiple items

Edit in Quizmaker

Edit Properties

Pronto para o próximo?

Curso Preparatório para Certificação
Em Gestão de Segurança da Informação Avançada – Baseada na ISO/IEC 27002:2013

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 10

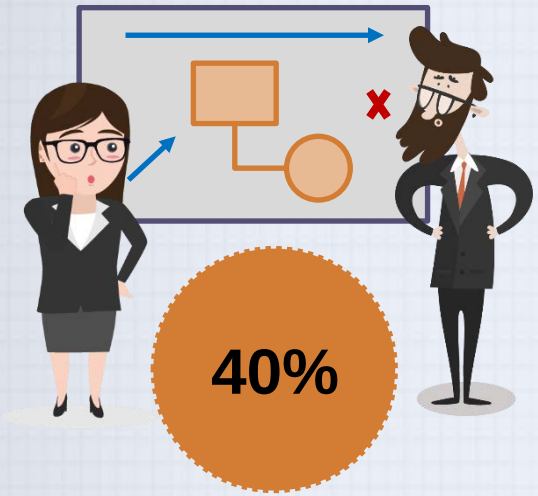
Controles Físicos e Outros Controles

Resumo

Ao longo deste módulo você vai aprender sobre os controles físicos, as relações com empregados e com a continuidade de negócios.

- **Perímetro físico de segurança;**
- **Controles de entrada física;**
- A necessidade de planejamento de contingência;
- De explorar os principais componentes do planejamento de contingência;
- Assim, como criar um conjunto simples de planos de contingência, usando análise de impacto de negócios;
- E preparar e executar um teste de planos de contingência.

Plano de Contingência



Tratar de contingência é concentrar-se no planejamento para um evento inesperado.

Para evitar estas paradas, são necessários procedimentos que permitam à organização continuar com suas funções essenciais.

É a restauração à normalidade com um custo adequado e com um mínimo de interrupção nas atividades de negócio, após um evento inesperado.

Plano de Contingência - PC

↓

Trata das ações frente aos eventos inesperados.

↓

Busca fazer com que a organização se prepare, detecte, reaja e recupere-se de eventos.

Plano de Resposta a Incidentes (*IRP - Incident Response Plan*):

- Foca na resposta imediata a um incidente.

Plano de Recuperação de Desastres (*DRP - Disaster Recovery Plan*):

- Concentra na restauração de operações após ocorrência de desastres.

Plano de continuidade de negócios (*BCP - Business Continuity Plan*):

- Facilita o estabelecimento de operações em um local alternativo, até que a organização seja capaz de retomar as operações.

Componentes do Plano de Contingência

- Identificar as funções de missão crítica de negócio.
- Identificar os recursos que suportam as funções críticas.
- Antecipar potenciais contingências ou desastres.
- Selecionar estratégias de planejamento de contingência.
- Implementar a estratégia selecionada.
- Testar e revisar planos de contingência.

A equipe do Planejamento de Contingência

A equipe de recuperação de desastres (DR)

A equipe de recuperação de incidentes (IR)

A equipe do plano de continuidade de negócios (BC)

Plano de Resposta a Incidentes

Plano de Resposta a Incidentes (IRP)

É um conjunto detalhado de processos e procedimentos que antecipam, detectam e minimizam o impacto de um evento inesperado que pode comprometer os ativos ou recursos de informações.

Evento inesperado

Incidente

Ataque Natural

Provocado pelo homem

Resposta ao incidente - RI

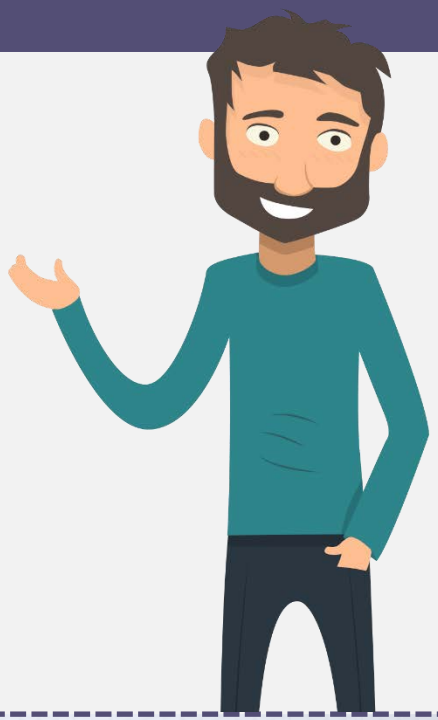
É um conjunto de procedimentos que se inicia quando um incidente é detectado.

Plano de Resposta a Incidentes

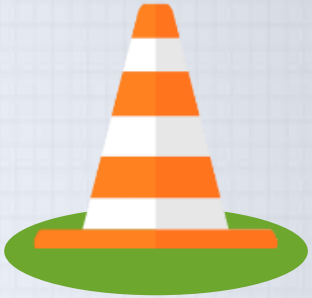
É ativado quando um incidente causa danos mínimos - de acordo com critérios previamente estabelecidos pela organização - com pouca ou nenhuma interrupção nas operações de negócio.

Quando uma ameaça se torna um ataque válido, ela é classificada então como um incidente de segurança da informação se:

- For dirigido contra os ativos de informação;
- Houver uma real chance de sucesso;
- Ameaça a confidencialidade, integridade ou disponibilidade de ativos e recursos de informação.



Etapas da Resposta a Incidentes



RI (Resposta a Incidentes)

É uma medida REATIVA, não PREVENTIVA.

- Os responsáveis desenvolvem e documentam os procedimentos que devem ser executados durante o incidente.
- Estes procedimentos são agrupados e atribuídos aos colaboradores.
- O comitê de planejamento elabora um conjunto de procedimentos específicos de função.

Após o incidente

- Uma vez que os procedimentos para a manipulação de um incidente são elaborados, os responsáveis pelo planejamento de contingência desenvolvem e documentam os procedimentos que devem ser realizados imediatamente após o incidente ter sido encerrado.

Antes do incidente

- Os planejadores elaboram um terceiro conjunto de procedimentos, as tarefas que devem ser realizadas para se prepararem para o incidente.

- Cronogramas de backup;
- Preparação de recuperação de desastres;
- Cronogramas de treinamento;
- Planos de teste;
- Cópias de contratos de serviço;
- Planos de continuidade de negócios.

Preparando-se para o Planejamento

A equipe de planejamento de RI procura desenvolver uma série de respostas pré-definidas que guiarão o time todo e a equipe de segurança da informação através das etapas necessárias para responder a um incidente.

Cada membro da equipe de RI deve conhecer seu papel específico, trabalhar em conjunto e executar os objetivos do PIR.

A equipe de RI é composta por profissionais capazes de lidar com os sistemas de informação e áreas funcionais afetadas por um incidente.

A definição prévia das respostas a incidentes permite à organização reagir de forma rápida e eficazmente ao incidente detectado, sem nenhuma confusão ou desperdício de tempo e esforço.

Deve incluir:

- Um mentor.
- Gerente de projeto.
- Membros do time.
- Gerentes de negócios.
- Gerentes de tecnologia da informação.
- Gerentes de segurança da informação.

Detecção de Incidentes

Desafio → Determinar se um evento é alerta rotineiro ou um incidente real.

Processo de classificação de incidentes

- **Examina um possível incidente ou um candidato a incidente e determina se constitui ou não um incidente real.**

Prováveis indicadores:

- Atividades em momentos inesperados.
- Presença de novas contas nos sistemas.
- Relatos de ataques.
- Notificação do IDS - Intrusion detection system.

Indicadores que sugerem a presença de um incidente:

- Presença de arquivos desconhecidos.
- Presença ou execução de programas ou processos desconhecidos.
- Consumo incomum de recursos de computação.
- Falhas inesperadas do sistema.

Detecção de Incidentes

Os indicadores definitivos:	As ocorrências reais de incidentes:
• Utilização de contas inativas.	• Perda de disponibilidade.
• Alterações nos logs.	• Perda de integridade.
• Presença de ferramentas de hackers.	• Perda de confidencialidade.
• Notificações pelos parceiros ou pares.	• Violação da política.
• Notificação por hackers.	• Violação da lei.

Resposta a Incidentes

Equipe de Recuperação de Incidentes IR | **Fase Detecção** | **Fase Reação**

Uma lista de alertas é um documento que contém informações de contato sobre os indivíduos a serem notificados no caso de um incidente real.

E existem duas maneiras de ativar esta lista de alertas:

- Sequencialmente;
- Hierarquicamente.

- Notificação do pessoal-chave;
- A atribuição de tarefas;
- Documentação do incidente.

Resposta a Incidentes

- **A mensagem de um alerta consiste na descrição do incidente e informações suficientes para que cada um saiba qual parte do RPI deve ser implementada**
- **Outro pessoal-chave que não está incluído na lista de alertas, como a gerência geral, deve ser notificada do incidente.**
- **Essa notificação deve ocorrer somente após o incidente ter sido confirmado, mas antes que a fontes externas saibam disso.**

- A documentação deve registrar o "quem", o "quê", "quando", "onde", "por que" e "como" de cada ação tomada.
- Serve como um estudo de caso para determinar se as ações corretas foram tomadas, e se eles foram eficazes.
- É uma forma também de provar que a organização fez tudo o que era possível para impedir a propagação do incidente.

Estratégias de Contenção de Incidentes/

A equipe de IR pode parar o incidente e tentar recuperar o controle por meio de várias estratégias:

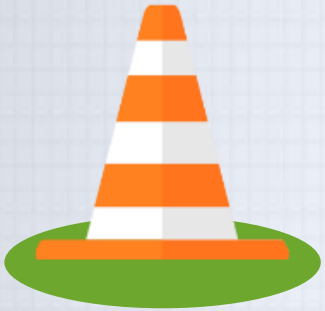
- Desconectar os circuitos de comunicação afetados;
- Aplicar dinamicamente regras de filtragem para limitar certos tipos de acesso à rede;
- Desativar contas de usuário comprometidas;
- Reconfiguração de firewalls para bloquear o tráfego problemático;
- Desativar temporariamente o processo ou serviço comprometido;
- Remover o aplicativo ou o servidor da rede;
- Parar todos os computadores e dispositivos de rede.

As estratégias de contenção de incidentes concentram-se em duas tarefas:

- Parar o incidente;
- Recuperar o controle dos sistemas;

Um dos componentes mais críticos do IR é parar o incidente ou conter seu escopo ou impacto. As estratégias de contenção de incidentes variam dependendo do incidente e da quantidade de danos causados por ele.

Escalação e Recuperação de Incidentes

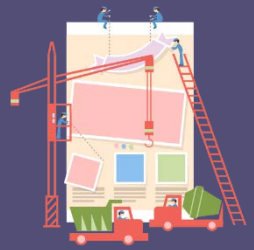


O incidente pode aumentar de escopo ou gravidade, a ponto de o RPI não conseguir lidar adequadamente com o evento.

Cada organização terá que determinar, durante a Análise de Impacto do Negócio, o ponto em que o incidente se torna um desastre.

A organização também deve documentar quando envolver uma resposta ou equipe externa.

Com o incidente contido e o controle do sistema recuperado, a recuperação de incidentes pode começar.



A equipe de RI deve avaliar toda a extensão do dano, a fim de determinar o que deve ser feito para restaurar os sistemas.

Determinar o alcance da violação da confidencialidade, integridade e disponibilidade de ativos de informação e informação.

Avaliação de Danos Incidentes.

Escalação e Recuperação de Incidentes

- Identificar as vulnerabilidades que permitiram que o incidente ocorresse e se espalhasse.
- Abordar as salvaguardas ou backups que não conseguiram parar ou limitar o incidente por não estarem ativados, instalados ou atualizados.
- Avaliar a capacidade de monitoramento, se houver.
- Restaurar os dados dos backups.
- Restaurar os serviços e processos em uso.
- Monitorar continuamente o sistema.
- Restaurar a confiança dos interessados da organização.

Revisão Após a Ação

Antes de retornar às tarefas rotineiras, a equipe de RI deve realizar uma avaliação pós-ação, a APA.

APA - Exame detalhado dos eventos que ocorreram desde a primeira detecção até a recuperação final.

Selecionando o órgão específico que aplica a lei apropriada dependendo do tipo de crime cometido, seja ele:

Federal	Estadual	Local

Vantagens

São mais preparados em processar provas, coletar declarações de testemunhas e construção de casos legais.

Desvantagens

A aplicação da lei pode resultar em perda de controle na cadeia de eventos após um incidente, incluindo a coleta de informações e provas, e na acusação de suspeitos.

Recuperação de Desastres

Planejamento de Recuperação de Desastres (DRP)

Definir como restabelecer as operações no local onde a organização está normalmente localizada.

É a preparação e recuperação de um desastre, seja natural ou feito pelo homem. Em geral, um incidente é um desastre quando:

- A organização é incapaz de conter ou controlar o impacto de um incidente, ou;
- O nível do dano ou da destruição de um incidente é tão grave que a organização é incapaz de se recuperar rapidamente.

- Catástrofes naturais.
- Catástrofes provocadas pelo homem.

- **Classificar os desastres pela velocidade do desenvolvimento, ou seja:**
- **Catástrofes de aparecimento rápido**
- **Desastres de início lento**

Planejando para o Desastre

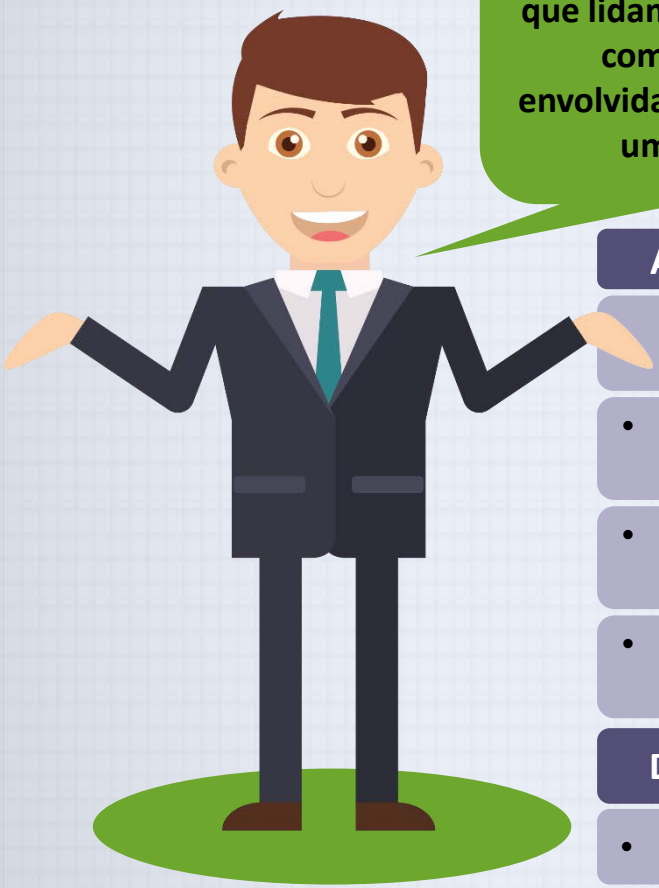
Equipe do Planejamento de Contingência - PC

- Participa do desenvolvimento de cenários;
- Da análise de impacto;
- E categoriza o nível de ameaça que cada potencial desastre representa.

Pessoas - o recurso mais importante, ao se gerar um cenário de recuperação de desastre.

- Delegação clara de papéis e responsabilidades.
- Execução da lista de alertas e notificação do pessoal chave.
- Definição clara das prioridades.
- Documentação do desastre.
- Inclusão de medidas de ação para mitigar o impacto do desastre nas operações da organização.
- Inclusão de implementações alternativas para os vários componentes do sistema, caso as versões primárias não estejam disponíveis.

Gerenciamento de Crises



Gerenciamento de crises é um conjunto de etapas que lidam principalmente com as pessoas envolvidas durante e após um desastre.

A equipe de DR trabalha em estreita colaboração com a equipe de gerenciamento de crises para assegurar uma comunicação completa e oportuna durante um desastre.

Atividades Principais:

- Durante a crise, apoiar seu pessoal (e seus entes queridos);
- Determinar o impacto do evento em operações comerciais normais e, se necessário, fazer uma declaração de desastre.
- Manter o público informado sobre o evento e as ações que estão sendo tomadas para assegurar a recuperação do pessoal e da empresa.
- Comunicação com os principais clientes, fornecedores, parceiros, agências reguladoras, outras organizações, mídia e outras partes interessadas.

Duas das principais tarefas da equipe de gerenciamento de crises são:

- Verificar o status do pessoal.
- Ativar a lista de alertas.

Respondendo ao Desastre

Quando um desastre ocorre e o DRP é ativado, eventos reais podem às vezes superar até mesmo o melhor dos planos. Então, para estar preparada, a equipe de PC deve incorporar um grau de flexibilidade no DRP.

Instalações Físicas

Intactas

- A equipe de DR deve começar a restauração de sistemas e dados para trabalhar rumo à capacidade operacional total.

Destruídas

- Ações alternativas devem ser tomadas até que novas instalações possam ser adquiridas.

Quando um desastre ameaça a viabilidade de uma organização no site principal, o processo de recuperação de desastres se torna então um famoso Processo de Continuidade de Negócios.

Lista de Contatos

Esta lista deve ajudar a definir quem chamar e reportar o mais rápido possível o ocorrido.

Pode conter nesta lista os contatos em todas as áreas de interesse.

- **Não deve conter apenas os grupos de autoridades que tenham relação com o que a empresa precisa;**
- **Cada contato nesta lista deve tratar de uma situação especifica e isso tem que estar claramente descrito;**
- **Para cada situação, um contato de uma pessoa deve estar relacionado.**

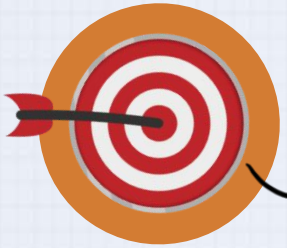
- Polícia;
- Bombeiros;
- Órgão de fiscalização;
- Responsáveis por investigar crimes eletrônicos;
- Contatos que auxiliem em um ataque vindo da internet;
- Contatos dos prestadores de serviços de infraestrutura;
- Serviços de emergências;
- Contatos de fornecedores de água, luz, telefone;
- Ambulância ou sistema de saúde;
- Responsáveis pela segurança física.

Ter esta lista de contatos é um requisito fundamental para o suporte, principalmente, no Gerenciamento de Incidentes e no processo de planejamento tanto da contingência quanto da continuidade de negócio.

Contatos com Grupos Especiais

Manter também os contatos de grupos especiais.

Grupos como associações de profissionais, fóruns e comunidades especificas, voltadas para a troca de informações sobre segurança da informação.



Ampliar o conhecimento em segurança da informação, para se manter atualizado sobre o assunto.

Conhecer com antecedência as correções, ser avisado, receber advertências de alertas, contar com o apoio relativo a ataques e pontos fracos é o ponto forte em se associar a tais grupos.

Acesso à consultoria especializada em segurança da informação ou acesso os cases de sucesso com o objetivo de ajudar com aconselhamentos especializados em melhores práticas.

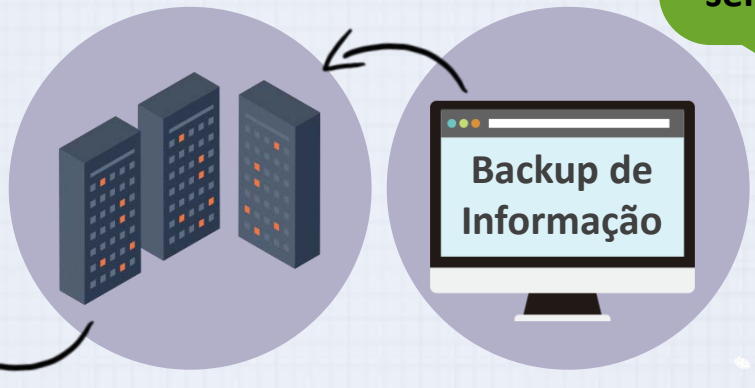
Compartilhar informações sobre novas tecnologias e formas de minimizar possíveis riscos através do recebimento de alertas antecipados, advertências e *patches* referentes a ataques e vulnerabilidades.

Controles de Continuidade

- Continuidade de segurança quando uma organização enfrenta um problema de continuidade nos negócios e;
- Disponibilidade dos sistemas de segurança, processos e serviços durante uma operação normal.

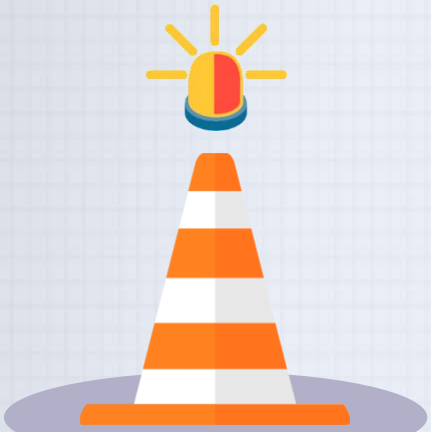
De uma perspectiva da segurança da informação, o termo CONTINUIDADE deve ser interpretado como:

- **Durante a avaliação geral de risco Gerenciamento de Continuidade de Negócio, os riscos na segurança da informação que poderiam levar a um problema na continuidade dos negócios também devem ser incluídos.**



- **Para riscos do Gerenciamento de Continuidade de Negócio que a organização decide suavizar, os aspectos de segurança da informação devem ser incluídos, por isso, os aspectos da segurança da informação relacionado a continuidade devem ser treinados periodicamente.**

Plano de Continuidade de Negócios



Incidente Grave

O tempo máximo de inatividade permitido.

Se muito longo, a organização pode não será capaz de se recuperar.

RTO - Tempo de Recuperação *(Recovery Time* Objective).

RPO - Ponto de Recuperação *(Recovery Point Objetive).*

RTO - expressado em horas, deve definir todos os esforços para a recuperação de um incidente, desde os prazos das atividades de detecção, escaladas, minimização dos incidentes, documentação até o treinamento dos interessados.

Período máximo tolerado que uma informação seja perdida em um sistema de TI devido a um incidente.

Depende muito dos riscos de negócios que uma organização enfrenta quando transações são perdidas.

Devem ser incluídos no **Business *Continuit Plan* - *BCP*** ou o ***IT Continuit Plan***.

Plano de Continuidade de Negócios

- As atividades críticas, no BCP, devem ser descritas em detalhes.
- É feito pelos especialistas que durante as operações normais são responsáveis pela TI ou pelos processos de negócios.
- Eles definem as ações, tempos e instalações necessárias para cumprir com as ações dentro do BCP.
- Qualquer BCP deve ser testado periodicamente.
- Ele deve ser conduzido de forma completa, ou seja, deve haver nestes testes a restauração dos serviços de TI conforme as exigências de RTO e RPO.
- Todo o pessoal envolvido deve ter conhecimento sobre os seus papéis e atividades neste momento.
- Qualquer mudança na organização deve, naturalmente, haver uma atualização no BCP.
- Devem ser consideradas todas as soluções de TI sobre disponibilidade, tais como os serviços de *clustering*, virtualização, e até mesmo a computação em nuvem.

Continuidade e Disponibilidade

Problemas de segurança que cause complicações e prejudiquem a operação da empresa requerem maior cuidado.

Plano de Continuidade ou um Plano de Contingência → Usados quando há um incidente ou uma mudança.

Os dois conceitos atuam juntos, um plano de contingencia é muito usado quando, por exemplo, em uma nota fiscal não pode ser emitida, ou seja, um problema de disponibilidade e neste caso uma nota fiscal de papel seria utilizada para continuar os negócios.

A continuidade exige um acordo, ou seja, um SLA, que delimita os prazos e condições.

- **A continuidade foca no gerenciamento de riscos, em como a organização pode operar mesmo depois de um problema ou da própria restauração.**

- **Estes acordos são usados para tratar os incidentes ou mudanças.**

Planejamento de Continuidade de Negócio

O Planejamento de Continuidade de Negócios garante que funções críticas de negócios possam continuar se ocorrer um desastre.

Ao contrário do DRP

BCP

Que geralmente é gerenciado pela comunidade de TI de interesse.

O Plano de Continuidade de Negócios (BCP) é mais adequadamente gerenciado pelo CEO de uma organização.

É ativado e executado junto com o DRP, quando o desastre é maior ou de longo prazo, e requer uma restauração mais completa e complexa dos ativos e recursos de informação.

Enquanto o BCP restabelece as funções críticas de negócios em um site alternativo...

A equipe do DRP se concentra no restabelecimento da infraestrutura técnica e das operações de negócios no site principal.

A identificação das funções críticas do negócio e dos recursos é fator de maior importância do BCP, uma vez que estas funções são as primeiras que devem ser restabelecidas no local alternativo.

Planejamento de Continuidade de Negócio

- Locais quentes (hot sites);
- Locais mornos (warm sites);
- Locais frios (cold sites).

- *Timeshare*;
- Escritórios terceirizados;
- Acordos mútuos.

Opções dos Sites e Uso Compartilhado

Hot Sites:

Warm Site:

Cold Sites:

Timeshares:

Serviços Terceirizados

Acordos Mútuos:

Opções dos Sites e Uso Compartilhado

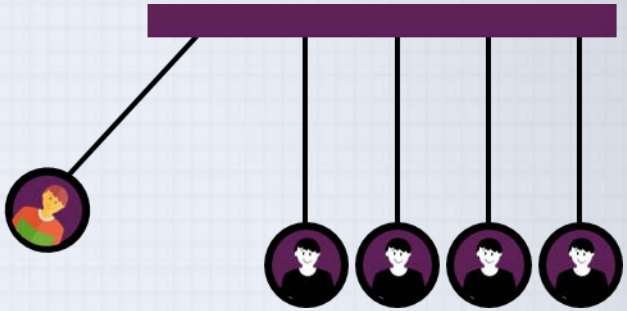
Ainda sim existem algumas alternativas especializadas:

- Site móvel;
- Recursos armazenados externamente;
- Armazenamento de Dados de Desastres Off-Site.

Opções:

- **Electronic Vaulting (salto eletrônico):** A transferência em massa de dados para uma instalação fora do local.
- **Remote Journaling (registro remoto):** A transferência de transações online para uma instalação fora do local.
- **Database shadowing (sombra do banco de dados):** O armazenamento online de dados duplicados, juntamente com a duplicação dos bancos de dados no site remoto para um servidor redundante.

Análise de Impacto do Negócio



- **A equipe do PC conduz o BIA nos seguintes estágios:**
- Identificação de ataque de ameaças;
- Análise da unidade de negócios;
- Cenários de sucesso de ataque;
- Avaliação de danos potenciais;
- Classificação do plano subordinado.

Assume que esses controles foram ignorados, falharam ou são ineficazes, e que o ataque foi bem-sucedido.

BIA

Processo de Gerenciamento de Risco

Concentra-se na identificação das ameaças, vulnerabilidades e ataques para determinar quais controles podem proteger as informações.

Análise de Impacto do Negócio (BIA)

Fornece à equipe do PC, informações sobre os sistemas e as ameaças que enfrentam. É a primeira fase do processo de PC.

É um componente crucial dos estágios iniciais de planejamento, pois fornece cenários detalhados do impacto que cada ataque potencial pode ter na organização.

Etapas do BIA

Uma organização que seguiu o Processo de Gerenciamento de Risco

1º

BIA

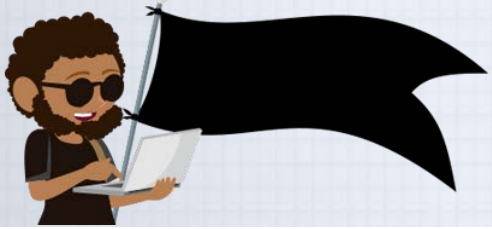
Essas organizações precisam apenas atualizar a lista de ameaças e adicionar uma informação adicional, o **PERFIL DE ATAQUE.**

Os cenários de ataque com mais detalhes são adicionados ao perfil de ataque, incluindo resultados alternativos.

Ataque Típico

- Metodologia;
- indicadores de ataque;
- Consequências.

- **2ª TAREFA -** Análise e priorização de funções de negócios dentro da organização.
- A equipe BIA deve criar uma série de cenários que descreva o impacto de uma ocorrência de cada ameaça em cada área funcional.



É uma descrição detalhada das atividades que ocorrem durante um ataque.

Combinando o DRP o BCP

Como o **DRP** e o **BCP** estão intimamente relacionados, a maioria das organizações os prepara simultaneamente e pode combiná-los em um único documento.

Para o **local alternativo** e **imediato**

Para o retorno ao **local principal**

Embora uma única equipe de planejamento possa desenvolver o DRP / BRP combinado, a execução requer equipes separadas.

Plano de Teste

Existem cinco estratégias de teste que podem ser usadas para testar planos de contingência:

- **Teste de Mesa**
- **Passo a passo estruturado**
- **Simulação**
- **Teste paralelo**
- **Interrupção total**

- **A iteração resulta em melhoria.**
- **A implementação formal desta metodologia é um processo conhecido como melhoria contínua de processos.**
- **Ela deve aprender com o processo, melhorar os planos e, em seguida, testar novamente.**

Utilidade de uma Política

A política é a base essencial de um programa eficaz de segurança da informação.

O sucesso de um programa para a proteção dos recursos e ativos de informação, depende de uma política gerada e da atitude da gerência em relação à obtenção das informações sobre os sistemas.

Ao desenvolver estas políticas...

Deve ser definido o tom e a ênfase sobre a importância do papel da segurança da informação dentro de sua organização.

A principal responsabilidade é definir a política de segurança para a organização.

Assim como os objetivos da redução dos riscos.

De estar em conformidade com leis e regulamentos.

Garantia de continuidade operacional.

Integridade da informação.

E confidencialidade.

Utilidade de uma Política

Embora as Políticas de Segurança da Informação sejam os meios de controle menos dispendiosos para serem executados, são frequentemente as mais difíceis de implementar.

As políticas adequadamente desenvolvidas e implementadas permitem que o programa de segurança da informação funcione quase perfeitamente dentro do local de trabalho.

REGRAS BÁSICAS:

- A política nunca deve entrar em conflito com a lei;
- A política deve ser capaz de ser utilizada em contestações perante aos processos judiciais, principalmente quando lidamos com a terceirização;
- A política deve ser devidamente apoiada e administrada.

Segurança Física e do Ambiente

Os perímetros e níveis de segurança precisam ser definidos com base nos riscos levantados.

Devem estar em locais com tetos e alvenaria seguros; portas e janelas que possam ser reforçadas para receber mecanismos de segurança e controle de entrada.

Alarmes

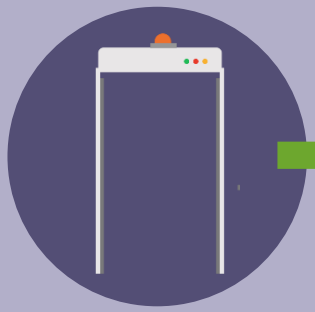
Travas e Barras de Segurança

Especialmente quando no nível térreo.

Uma recepção deve conter mecanismos e procedimentos de controle de acesso.

Segurança Física e do Ambiente

Portas e saídas de incêndio precisam estar em acordo com normas estabelecidas.



O acesso a áreas com informações confidenciais precisa ser restrito apenas a pessoas autorizadas.

O acesso e as razões para tal precisam ser mantidos em sistema ou livro de visitantes.

Todos os funcionários ou prestadores precisam possuir identificações visíveis e pessoas sem as mesmas precisam ser imediatamente identificadas.

- Os serviços externos de suporte devem possuir autorizações especiais para o acesso, com validade limitada.
- Os direitos e autorizações de entrada devem ser constantemente revistos e atualizados.

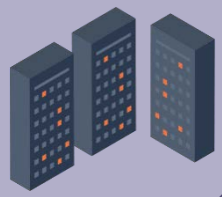
Controles Físicos

Inclui:

Os limites de um edifício..

... Ou do local que contenha as instalações de TI.

DATACENTER



Estes perímetros precisam estar seguros fisicamente, não pode ter brechas nem pontos onde poderia ocorrer facilmente uma invasão.

Manter as paredes externas do local, com construção robusta e todas as portas externas adequadamente protegidas contra acesso não autorizado, por meio de mecanismos de controle.

Barras, alarmes, fechaduras etc.

Construir barreiras físicas ou prover, nas portas corta-fogo do perímetro de segurança, com alarme, além de funcionarem de acordo com os códigos locais de prevenção de incêndios e prevenção de falhas.

Controles Físicos

EX.: Salas de computadores ou salas de comunicações, devem contar com controles físicos, como detecção de intrusos e alarmes, o tempo todo.

Deve existir proteção física ao redor das instalações. O uso de barreiras múltiplas proporciona proteção adicional, pois em caso de falha em uma delas a segurança não fique comprometida imediatamente.

Diretrizes:

- Registro da data e hora da entrada e saída de visitantes;
- O acesso às áreas das informações sensíveis deve ser restrito apenas ao pessoal autorizado;
- **EX.:** Por mecanismos de autenticação de dois fatores, como, **cartões** de controle de acesso e PIN (*personal identification number*).
- Manter uma trilha de auditoria eletrônica ou um livro de registro físico de todos os acesso.
- Exigir que funcionários, fornecedores, partes externas e visitantes tenham alguma forma visível de identificação.
- Partes externas dos serviços de suporte podem ter acesso às áreas seguras ou as instalações de processamento da informação sensíveis, porém, este acesso deve ser sempre monitorado.

Segurança Física

- **Segurança física de escritórios, salas e locais devem ser bem projetadas, para evitar:**
- Que locais-chave fiquem situados às vistas do público;
- Que a relação dos números telefônicos com a localização de áreas sensíveis fiquem expostos a todos.

Evitar que pessoas não autorizadas causem danos e interferências no processamento normal das informações da empresa. Basicamente, é manter o acesso restrito a todos que não são autorizados.

Por isso os especialistas em segurança devem ser contratados e laudos em relação à exposição a incêndios, enchentes, terremotos e outros devem ser elaborados.

Segurança Física

Os perímetros precisam ser bem definidos, implantando:

- Sistemas de detecção de intrusos;
- Portas com alarmes;
- Salas de computadores com alarmes e monitoramento 24 horas;
- Barreiras múltiplas, etc.

- **Salas importantes devem ficar fora do alcance ou acesso do público.**
- **Não colocar no mapa dos locais de livre acesso, a localização deste tipo de sala.**

Alguns dos seguintes perímetros devem ser controlados, como:

- Jardinagem;
- Grades;
- Portões;
- Postes;
- Sistema de detecção de invasão do perímetro;
- Circuito fechado de televisão;

Orientações para os Controles Físicos

Deve ser implantando procedimentos que descrevem as condições de trabalho em áreas protegidas.

Especificando que em algumas áreas ninguém deve trabalhar sozinho.

Existem ainda os controles físicos voltados as ferramentas e *utilities*.

Como os de proteção contra perda de utilitários, por exemplo: o resfriamento, energia, gás, água etc.

Ou ainda, os procedimentos e ferramentas técnicas para a eliminação de mídia (papel, discos) contendo informação confidencial.

- Verifique a legislação vigente sobre câmeras de vigilância e outros equipamentos sensíveis a privacidade.
- O gerenciamento de direitos de acesso precisa ter uma interface com o departamento de RH quando uma pessoa é admitida, demitida ou quando a muda a posição.
- Criar zonas ajuda a decidir quais partes da organização precisam de controles de entrada restritos.

Orientações para os Controles Físicos

Para otimizar esses controles para a proteção da informação:

- Um fornecimento de energia alternativo (fornecimento ininterrupto de energia para curtos períodos e sistemas nobreak – geradores – para longos períodos) é sempre exigido.
- Teste periodicamente os UPS e os sistemas nobreak.
- Sistemas de gerenciamento do prédio – controlando energia, iluminação, acesso, temperatura, etc. – aos sistemas de computadores. Eles precisam da mesma proteção que qualquer outro computador da organização.
- Uma avaliação completa de riscos no ambiente deve ditar quais tipos de controles de entrada física são necessários.
- Considerar que barreiras físicas não devem impedir que o pessoal deixe o local em caso de emergência.
- Faça testes, use um convidado misterioso (um profissional treinado que tente passar pelos controles de acesso físico).

- **Gerente de segurança**
- **Gerente de TI**
- **Gerente da instalação**

Devem trabalhar juntos nesse assunto.

Pronto para o próximo?