TI.exames Com êxito

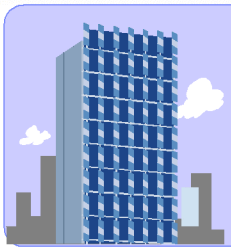
EDUCAÇÃO E TREINAMENTO
PARA ALAVANCAR A SUA CARREIRA

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

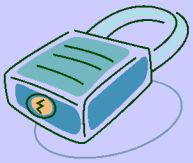
Curso e-learning completo

Preparatório para o exame EXIN ISO 27002 Foundation

Módulo 7



Medidas Organizacionais



Este módulo cobre:

- Política de segurança
- Pessoal
- Gestão de continuidade do negócio
- Processos operacionais e gestão de comunicação

Slide 2

Medidas de organizacionais

Medidas organizacionais estão intimamente relacionadas com medidas técnicas. Quando necessário vamos relembrar as medidas técnicas para que se consiga implantar adequadamente as medidas organizacionais.

Neste módulo vamos olhar mais de perto a política de segurança, vamos falar sobre o ciclo PDCA e os requisitos das normas ISO 27001 e 27002. Também vamos discutir como se pode difundir segurança da informação dentro da organização.

Vamos ver como lidar com desastres e como nos preparar para estas situações.

Além disso, vamos examinar processos operacionais, comunicação, procedimentos para teste e gestão de ambiente de TI em um provedor externo.

Política de segurança

Política de segurança da informação

A gestão da organização provê direcionamento estabelecendo a política de segurança da informação, que deve ser escrita de acordo com os requisitos do negócio e com as regulamentações e legislação aplicáveis, deve ser aprovada pela direção e comunicada para todos os funcionários e partes externas relevantes, como fornecedores e clientes.

Hierarquia

É comum um documento como este ter uma estrutura hierárquica pois várias outras políticas serão desenvolvidas tendo a política da organização como base (como por exemplo uma política para uso de criptografia). Também podem ser escritos tendo a política da organização como base:

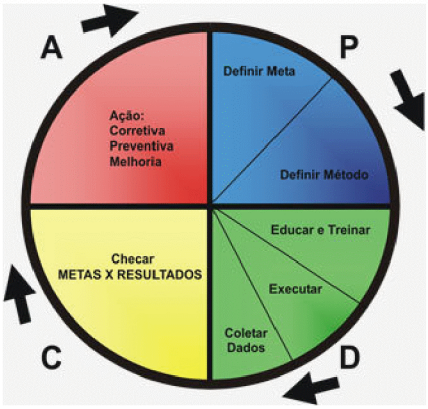
- → Regulamentos, detalhamento de uma política
- → Procedimentos, por exemplo política de mesa limpa
- → Guias, uma orientação. Por exemplo: para atender à política de classificação os funcionários tem liberdade de escolher a forma da classificação
- → Normas, como por exemplo ISO/IEC 27001 e 27002

Política de segurança – Avaliação

Elaborar a política de segurança da informação é uma coisa, implementar e verificar se ela está sendo cumprida é outra.

A política de segurança da informação é o documento maior, que inclui documentos, procedimentos e guias do que se deseja seguir e que provêem detalhes.

Muitas organizações trabalham com o ciclo PDCA.



Modelo do ciclo PDCA

P = Planejar
D = Desenvolver
C = Checar
A = Agir

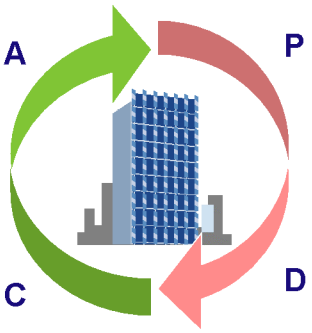
Slide 5

Política de segurança – Estabelecendo um SGI

A organização desenvolve uma estrutura para controlar seu SGSI. Esta estrutura fornece uma classificação lógica para todas as questões relacionadas à segurança da informação e as organiza em domínios.

Um domínio é um grupo de temas que são conectados logicamente um com o outro. Domínios são a base da estrutura do SGSI. Muitos destes grupos produzem seus próprios documentos, procedimentos e instruções de trabalho.

O SGSI compreende 11 domínios identificados pelas normas ISO/IEC 27001 e 27002. Estes domínios estão alinhados com a Gestão de Serviços de TI descrita na ISO/IEC 20000-1.



Slide 6

Política de segurança – Os 11 domínios da 27002

Os números listados abaixo são capítulos da ISO/IEC 27002. Os 4 capítulos iniciais fazem uma introdução aos 11 domínios. Cada domínio tem diversos sub-domínios. Um domínio é descrito por um objetivo de controle e depois detalhado.

A.5	Política de Segurança
A.6	Organização da Segurança da Informação
A.7	Gestão de Ativos
A.8	Segurança em Recursos Humanos
A.9	Segurança Física e do Ambiente
A.10	Gerenciamento das Operações e Comunicações
A.11	Controle de Acesso
A.12	Aquisição, Desenvolvimento e Manutenção de Sistemas
A.13	Gestão de Incidentes de Segurança da Informação
A.14	Gestão da Continuidade do Negócio
A.15	Conformidade

Slide 7

Política de segurança

Monitorando a política de segurança da informação

A política de segurança da informação deve ser regularmente revisada, e se necessário modificada. As mudanças devem ser aprovadas pela alta direção.

A organização da segurança da informação

Sem uma efetiva segurança da informação não é possível a uma organização sobreviver. Todos na organização devem aceitar isso, e a direção e os gerentes devem servir de exemplo. Somente quando eles apóiam sua própria política é que os funcionários vão levar com seriedade a segurança da informação e cumprir com as medidas definidas.

Segurança da informação é um processo no qual muitas pessoas estão envolvidas. O processo necessita ser efetivamente controlado. Se não houver responsabilidade ou gestão, então a segurança da informação não será efetiva. É importante que a segurança da informação seja gerenciada dependendo do tamanho e da natureza da organização. Em organizações pequenas a segurança da informação pode ser somente uma das responsabilidades de diversas pessoas, já em uma grande organização pode haver pessoas especificamente responsáveis por ela.

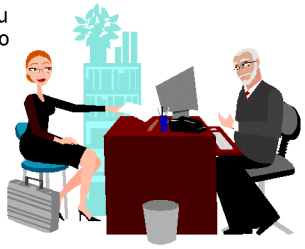
Slide 8

Pessoal

Pessoas também podem ser ativos do negócio. Pessoas e seu conhecimento e habilidades têm valor como ativos, e medidas são necessárias para proteger este valor.

Todas as pessoas são responsáveis pela segurança da informação. Esta responsabilidade deve ser clara no contrato de trabalho. O manual dos funcionários pode conter um código de conduta e as sansões que serão impostas caso este não seja cumprido e um incidente ocorra como resultado. Os gerentes devem relacionar as responsabilidades relativas à segurança da informação nas descrições de cargo. Exemplo de código de conduta: e-mails particulares são proibidos.

Quando uma pessoa se candidata para um cargo que envolve informações sensíveis, devem ser verificados seus diplomas, referências e identidade. Se a pessoa cometeu um crime isso pode ser descoberto solicitando o atestado de antecedentes criminais do profissional.



A organização deve ter um procedimento rigoroso para quando as pessoas saem ou entram na companhia ou quando trocam de cargo dentro da organização. Não se pode esquecer de remover direitos, acessos, passes e coletar equipamentos. Direitos de acesso devem ser controlados regularmente.

Slide 9

Pessoal

Fiscalização e acordo de confidencialidade

Para uma posição envolvendo confidencialidade, esta deve ser observada sempre que o contrato de trabalho é encerrado. O gerente é responsável pela documentação de regras especiais para posições específicas. De qualquer forma, todas as pessoas em posição que envolve confidencialidade devem assinar um acordo de confidencialidade. É também usual que nestes casos essas pessoas tenham que submeter o atestado de antecedentes.

Acordo de confidencialidade

Também se pode fazer uma investigação de segurança. Quão profunda esta investigação vai ser depende do grau de confidencialidade requerido pela posição em questão. Tome, por exemplo, guardas de segurança, gerentes e funcionários da área financeira. Verificação é um processo que tem um custo elevado, é mais barato para a organização utilizar a estrutura governamental pedindo um atestado de antecedentes criminais e/ou consulta ao Serviço de Proteção ao Crédito estruturado pelas associações comerciais.

Slide 10

Pessoal

Empresas terceirizadas

Os requisitos de segurança que são aplicados aos funcionários também devem ser aplicados a qualquer pessoal que venha a trabalhar temporariamente na organização. Acordos documentados devem ser realizados com os fornecedores e agências de recrutamento, e devem incluir sanções caso o acordo seja violado.

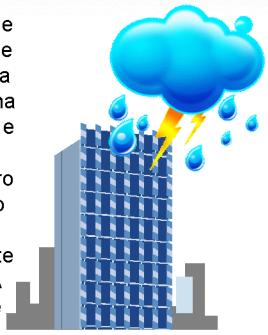
Acesso

Para grandes organizações onde nem todos se conhecem um bom sistema de controle de acesso é importante. Um exemplo é tanto funcionários quanto visitantes terem de usar o crachá à mostra.

Todos os visitantes devem ser registrados na entrada indicando para qual departamento se dirigem. Todo horário de acesso de entrada e de saída deve ser registrado da recepção. Todo funcionário que está esperando uma visita deve receber esta visita na recepção e conduzi-la até a recepção no momento da partida.

Gestão de continuidade do negócio

Não estamos preparados para tudo. Inundações como as que ocorreram na primavera de 2007 na Inglaterra e no outono de 2007 em Bangladesh causaram grandes perdas na economia desses países. Houve um imenso dano com o furacão Katrina em Nova Orleans. Terroristas atacaram Nova York, Londres e Madri. Tanto quanto a perda de energia pode haver consequências consideráveis para pessoas e sistemas dentro da companhia. Todos os anos, empresas ao redor do mundo são atingidas por desastres que têm um impacto imenso na disponibilidade de seus sistemas. Apenas uma pequena parte destas empresas está preparada para tais eventualidades. A maioria das empresas atingidas por desastres não sobrevive a eles.



Uma organização é dependente de seus ativos, pessoal e atividades que são realizadas diariamente de forma a manter a organização operando e rentável. A maioria das organizações tem uma rede complexa de relacionamentos entre fornecedores e ativos, dependentes uns dos outros para a realização das atividades. Existem canais de comunicação como telefone e e-mail e há edifícios nos quais o trabalho é realizado.

Se uma conexão na cadeia de dependências se rompe isso pode gerar uma série de problemas. Se mais conexões se rompem então haverá realmente um grande problema, e mais tempo se levará para o restabelecimento normal das operações.

Gestão de continuidade do negócio

Pensar antecipadamente na continuidade dos processos de trabalho é essencial para uma organização. Não importa se é um processo simples ou complexo de produção. Para os funcionários e para os clientes o que importa é a continuidade dos processos de trabalho apesar das dificuldades a serem enfrentadas.

O propósito de um Plano de Continuidade do Negócio – PCN (em inglês BCM – Business Continuity Management) é prevenir que as atividades sejam interrompidas e proteger processos críticos contra consequências como interrupções ou perda de velocidade.

Na gestão do plano de continuidade do negócio os processos de negócio mais críticos devem ser identificados. Medidas para garantir a continuidade contra perda de informação como consequência de desastres naturais, ataque, fogo e falha de energia devem ser implantadas. As consequências de desastres, incidentes de segurança e falhas de serviço são avaliadas na Análise de Impactos no Negócio – AIN (em inglês Business Impact Analysis – BIA). O plano de continuidade descreve como requisitos para os processos críticos do negócio podem rapidamente tornarem-se disponíveis. Temos então:

- **Planejamento da Continuidade do Negócio**, no qual a continuidade dos processos do negócio é garantida.
- **Planejamento para Recuperação de Desastres**, onde a recuperação após o desastre é organizada.

  A norma BS 25999 trata da Gestão da Continuidade do Negócio, e a 27002 inclui algumas medidas.

Gestão de continuidade do negócio

Continuidade

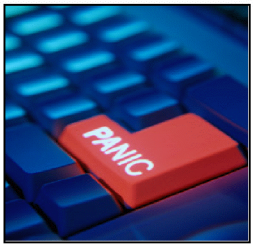
Continuidade tem haver com disponibilidade de sistemas da informação no momento que estes sistemas são necessários. Os requisitos de disponibilidade podem ser diferentes em função de cada situação específica: é diferente se você tem 50 pessoas trabalhando 24x7 ou se você tem apenas uma pessoa atendendo ao telefone e recebendo poucas ligações por hora.

Para uma prefeitura a disponibilidade do banco de dados municipal é de grande importância. Se o banco de dados ficar indisponível por um longo período a maioria dos funcionários não vai conseguir realizar seu trabalho – mas se a indisponibilidade for à noite pode ser que isso não cause problemas.

Pode-se ver que dependendo da organização e do tipo de trabalho os requisitos de disponibilidade diferem dramaticamente.

Gestão de continuidade do negócio

O que são desastres



Desastre soa como uma grande ameaça, mas nada do que se imagina chega perto da verdade. Neste contexto a falha de um simples sistema pode ser considerada um desastre. Um desastre não precisa ser uma enchente ou um ataque terrorista. A falha de um sistema do qual uma organização efetivamente dependa, por um único dia de trabalho, pode ser um grande desastre.

Como sua empresa responde a desastres

As consequências de um desastre para o negócio vão depender da natureza do desastre. Pode ser que apenas uma tarefa tenha sido interrompida, um sistema ter falhado ou uma rede inteira ter caído. No primeiro caso pode bastar uma ligação para o help desk e o incidente será corrigido. Nas duas outras situações pode ser que não.

Se a saúde de um empregado está sendo ameaçada então uma ligação para a emergência de um pronto socorro, a fim de se obter uma ambulância, pode ser a correta ação a ser tomada.

De qualquer forma a saúde de uma pessoa é mais importante que qualquer software ou equipamento.

É importante que existam procedimentos claros que orientem as ações.

Gestão de continuidade do negócio

Plano para Recuperação de Desastres

Qual a diferença entre Plano de Continuidade do Negócio – PCN (Business Continuity Plan – BCP) e Plano para Recuperação de Desastres – PRD (Disaster Recovery Planning – DRP)?

O propósito do Plano para Recuperação de Desastres é minimizar as consequências de um desastre e tomar as medidas necessárias para garantir que os funcionários, os ativos do negócio e os processos do negócio estarão disponíveis dentro de um tempo aceitável.

Isso é diferente do Plano de Continuidade do Negócio, cujos métodos e processos são também organizar-se para falhas que duram um longo período de tempo.

O Plano para Recuperação de Desastres deve ser disparado imediatamente após o desastre. Ele vai ser colocado em ação quando o desastre ainda estiver ocorrendo. O trabalho é focado em determinar o dano e em colocar os sistemas novamente em operação.

O Plano de Continuidade do Negócio tem uma abrangência maior. O PCN arranja uma localidade alternativa onde o trabalho pode ser realizado enquanto a localidade original é reconstruída. No PCN tudo é focado em manter a empresa operando, mesmo que parcialmente, desde o momento em que o desastre ocorre até quando a empresa esteja completamente recuperada. Então:

PRD – Quando há um desastre ele mostra o que fazer para retomar a produção.

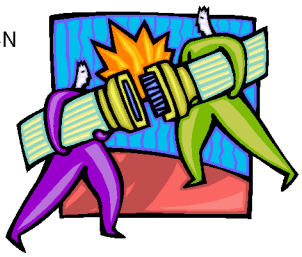
PCN – Houve um desastre e ele mostra como voltar à situação anterior ao desastre.

Gestão de continuidade do negócio

Plano para Recuperação de Desastres

Quando se desenvolve um PRD e/ou um PCN existe uma grande variedade de alternativas que podem ser utilizadas:

- Locais de trabalho alternativos
- Localidade redundante
- Localidade móvel



Existem várias soluções, mas tanto o PRD quanto o PCN devem considerar diversas eventualidades, serem aprovados pela direção e testados regularmente. Isso significa que todos os funcionários devem saber o que fazer (serem treinados). Além disso, sempre que mudanças ocorrerem na organização os planos devem ser revisados.

Se os profissionais que realizam as tarefas mais importantes também estão envolvidos no desastre, é importante considerar nos planos como estas pessoas serão substituídas.

Gestão de processos de comunicação e operação

Procedimentos operacionais e responsabilidades

A fim de manter uma gestão eficaz e controle de TI de uma organização, é importante documentar os procedimentos para funcionamento dos equipamentos e atribuir responsabilidades às pessoas apropriadas para as atividades requeridas. Detalhes podem ser fornecidos através de instruções de trabalho, tais como: computadores são ligados e desligados, fazer backups, manutenção, processamento de correio, etc. Um PC rodando Windows pode ter problemas se desligado incorretamente, enquanto um PC Unix tende a responder de forma diferente. É por isso que os procedimentos iniciais após uma falha do sistema são tão importantes.

Um procedimento operacional inclui:

- Como lidar com a informação
- Como, quando e quais backups são feitos
- Como e quem contatar no evento de um incidente
- Como gerenciar trilhas de auditoria e arquivos de log
- Etc.

O principal propósito de um procedimento operacional é certificar que não existam mal-entendimentos em relação à maneira na qual o equipamento tem que ser operado.

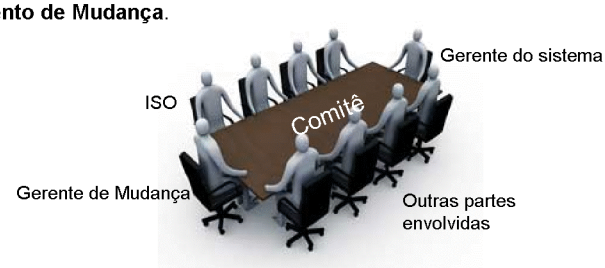
Gestão de processos de comunicação e operação

Gerenciamento de Mudança

A implantação de uma mudança pode ser uma faca de dois gumes. Implantar ou não implantar uma mudança envolve riscos. Não instalar um patch de segurança em um aplicativo é um risco, pois o sistema pode ficar vulnerável a uma falha e provocar interrupção no serviço. Por outro lado, instalar o patch também é um risco, pois podem acontecer circunstâncias imprevistas que podem levar à interrupção do serviço.

O risco potencial de não se instalar um patch relacionado à segurança é determinado pelo Information Security Officer (ISO), enquanto os riscos associados com a mudança precisam ser avaliados pelo gerente do sistema.

Se mudanças tiverem que ser feitas nos serviços de TI e sistemas de informação, então estas têm que ser cuidadosamente consideradas com antecedência e realizadas de maneira controlada. No Gerenciamento de Serviço de TI, este processo é chamado de **Gerenciamento de Mudança**.



Gestão de processos de comunicação e operação

Gerenciamento de Mudança – continuação

O Gerenciamento de Mudança gerencia mudanças nos sistemas de TI. Na ITIL você vai encontrar mais detalhes sobre como desenhar este processo.

Sistemas em produção devem apenas ser alterados se houver razões substantivas para a alteração, tal como um aumento de risco para o sistema. Atualizar sistemas com a última versão de um sistema operacional ou aplicativo não é sempre de interesse para uma empresa, pois isto pode algumas vezes resultar em maior vulnerabilidade e instabilidade.

Esta situação mostra por que a segregação de funções é importante. Se todo mundo estiver habilitado a realizar suas próprias mudanças, uma situação incontrolável surgiria na qual várias pessoas não estariam conscientes das mudanças implantadas por outras. Ainda mais importante, seria impossível identificar rapidamente qual mudança foi responsável pelos problemas que estariam ocorrendo e não seria conhecida a mudança que precisaria ser revertida.

Gestão de processos de comunicação e operação

Segregação de funções

Tarefas e responsabilidades precisam ser segregadas para evitar a chance de mudanças não autorizadas ou intencionais ou uso incorreto dos ativos da organização (também se refere aos termos de integridade e confidencialidade).

Na segregação de funções, uma revisão é conduzida para saber se a pessoa realiza tarefas de tomada de decisão, controle ou execução.

É determinado se a pessoa precisa de acesso à informação. Acesso não necessário aumenta o risco da informação ser usada intencionalmente, ser alterada ou destruída. Este é o princípio chamado “precisa saber?”. Um funcionário que trabalha em uma empresa que tem ações na bolsa de valores, por exemplo, não precisa ter acesso a informações da empresa relacionadas ao desempenho na bolsa de valores, tal como o lucro esperado e prejuízos.

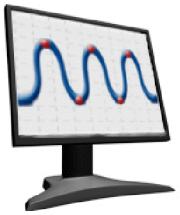
Tarefas podem ser divididas para reduzir os riscos para a organização. Um exemplo é a transferência de valores altos. Um membro prepara a transação e outro autoriza o lançamento. E ainda pode haber outro membro que verifica se a transação foi realizada correta e legitimamente.

Slide 21

Gestão de processos de comunicação e operação

Desenvolvimento, teste, aceite e produção

Para assegurar que mudanças não possam ser implantadas de maneira descontrolada, é ainda aconselhável criar vários ambientes físicos para desenvolvimento, teste, aceite e produção de sistemas da informação.



Para o ambiente de desenvolvimento podem existir requisitos de segurança específicos. O ambiente de testes destina-se a determinar se o desenvolvimento atende aos requisitos e, mais especificamente, aos requisitos de segurança.

O ambiente de aceite é o ambiente no qual os usuários finais verificam se o produto atende a suas especificações. Após o aceite, o sistema pode ser colocado em produção seguindo um conjunto de procedimentos.

Durante a transição do software existente para o novo software, deve existir um plano de remediação. Desta forma, caso ocorra algum problema grave, será possível reverter para a versão antiga.

Slide 22

Gestão de processos de comunicação e operação

Gerenciamento de serviços de terceiros

Nem todas as atividades importantes para uma organização são realizadas pela própria organização. Alguma coisa pode ser realizada por um terceiro, e é importante documentar os requisitos a que o terceiro deve atender.

Quando uma empresa decide terceirizar alguns ou todos os seus serviços de TI, um bom contrato deve ser assinado com a parte que vai fornecer o serviço. Todos os aspectos de segurança devem ser observados com atenção neste tipo de contrato.

É uma prática comum estabelecer um SLA (Service Level Agreement – Acordo de Nível de Serviço) no qual ambas as partes descrevem quais serviços elas esperam que sejam realizados e sob quais circunstâncias. Auditorias são regularmente realizadas para ver se estes acordos estão sendo observados.

Slide 23

Gestão de processos de comunicação e operação

Proteção contra malware, phishing e spam

Malware é uma combinação de das palavras “malicious” e “software” e refere-se a softwares indesejados tais como vírus, worms, trojans e spywares. Uma medida padrão contra malware é usar um examinador (scanner) antivírus e um firewall. Está, entretanto, se tornando claro que um examinador antivírus sozinho não é suficiente para parar o malware. Uma das razões para a explosão de vírus é as ações humanas. Uma infecção de vírus pode ocorrer frequentemente quando um usuário abre um anexo em um e-mail que além de conter o jogo, documento ou imagem prometida, tem também um vírus. Por isso não é recomendável abrir qualquer e-mail suspeito ou e-mail de remetentes desconhecidos.

Phishing é uma forma de fraude na internet. Usualmente a vítima recebe um e-mail pedindo para verificar ou confirmar a conta com um banco ou provedor de serviço, por exemplo. Algumas vezes mensagens instantâneas são usadas. Ainda contato telefônico pode ser tentado. É difícil pegar os autores do phishing. Usuários da internet precisam manter a vigilância e nunca devem responder a uma requisição por e-mail para transferir dinheiro ou enviar informações pessoais, tais como números da conta bancária, códigos PIN ou detalhes do cartão de crédito.

Slide 24

Gestão de processos de comunicação e operação

Proteção contra malware, phishing e spam

Spam é um nome coletivo para mensagens indesejadas. O termo é normalmente usado para e-mail indesejado, mas mensagens de publicidade indesejadas nos websites também são consideradas spam. Para ajudar a combater o spam, usuários devem, sempre que forem re-encaminhar mensagens para um grupo de pessoas, usar o campo Cópia Oculta (Cco). Outra dica é nunca responder a mensagem de spam, pois isto confirma para o spammer que o destinatário usa o e-mail e ele vai aproveitar isso para enviar mais spam.

Malware, phishing e spam são assuntos importantes no código de conduta e na campanha de conscientização para os funcionários.

Gestão de processos de comunicação e operação

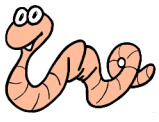
Algumas definições

Vírus: é um pequeno programa de computador que se replica propositalmente, algumas vezes em forma alterada. As versões replicadas do vírus original também são vírus.

Exemplos: Brain, Chernobyl.

Worm: é um pequeno programa de computador que se replica propositalmente. O resultado da replicação são cópias do original que se espalham por outros sistemas fazendo uso dos recursos da rede.

Exemplos: Melissa, I love you, Happy99, Storm Worm.



Trojan: é um programa que propositalmente conduz atividades secundárias, não observadas pelo usuário do computador e que podem causar dano à integridade do sistema infectado.

Exemplos: Backorifice, Netbus.

Hoax: é uma mensagem que tenta convencer o leitor da sua veracidade e então persuadí-lo a realizar uma ação particular. A propagação do hoax depende do leitor deliberadamente mandar a mensagens para outras vítimas potenciais que podem também fazer o mesmo.

Exemplos: Good times, Pen pal.

Gestão de processos de comunicação e operação

Logic Bomb: é um pedaço de código que foi criado dentro de um sistema de software. Este código irá, então, realizar uma função quando condições específicas forem encontradas. Ele nem sempre é usado para propósitos maliciosos. Um programador, por exemplo, pode criar um código que destrói arquivos quando ele for demitido da empresa. Vírus e worms normalmente contêm logic bombs.

Spyware: é um programa de computador que coleta informação do usuário do computador e a envia para outra parte. O propósito é ganhar dinheiro. Spyware não tenta danificar o PC propositalmente e/ou o software instalado, mas irá violar a privacidade do usuário.

Botnets: esta palavra é geralmente usada para referir-se a uma coleção de computadores infectados (chamados de computadores zumbis) executando o software, geralmente instalados através worms, cavalos de Tróia ou backdoors, sob o comando de controle das infra-estruturas.

Rootkit: é um conjunto de ferramentas que são usadas por um terceiro (usualmente um hacker) após ter ganho acesso a um sistema. O rootkit se esconde dentro de um sistema operacional, possivelmente deixando-o instável.

Slide 27

Gestão de processos de comunicação e operação

Back up e restauração

O propósito de se fazer backups ou guardar cópias é manter a integridade e disponibilidade da informação.

As consequências da perda de informação dependem da idade da informação que pode ser recuperada do backup. Por isso é importante considerar o intervalo no qual os backups são feitos.

É importante que os backups sejam testados regularmente.

Além de fazer e testar os backups, é necessário considerar como eles serão guardados.

Slide 28

Gestão de processos de comunicação e operação

Gerenciando a segurança da rede

Um desafio significativo para a segurança da informação é que a rede compartilhada pode se estender além dos limites da organização. Tipos de redes e medidas aconselháveis:

Rede	Descrição	Medidas
Intranet	Rede privada dentro da organização	Firewall para evitar que acessos externos penetrem na rede privada
Extranet	Quando a organização torna parte da sua intranet acessível para clientes, parceiros, fornecedores e outras partes fora da organização, esta é chamada de extranet	- Firewall - Certificados digitais para autenticação - Criptografar dados que são transmitidos - Uso de VPN (Virtual Private Network) para se comunicar na internet

Gestão de processos de comunicação e operação

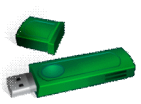
Tratando mídias

O termo “mídia” refere-se a qualquer coisa na qual dados possam ser gravados. Isto inclui papel, CD, DVD, pen drive, HD, fita de backup, blackberry, celular, MP3 player, etc.

O propósito de se ter diretrizes para tratar estas mídias é evitar que informação de valor caia em mãos erradas e prevenir as seguintes consequências: publicação não autorizada, mudança, exclusão ou destruição de ativos ou interrupção das atividades de negócio.

A maneira pela qual a mídia precisa ser tratada está frequentemente vinculada à classificação e é documentada nos procedimentos. Após o término do tempo de armazenamento, documentos com informação sensível são colocados no triturador de papel ou destruídos pela empresa. Pen drives devem ser esvaziados, preferencialmente usando uma ferramenta de limpeza que destrua seguramente os dados. Além disso, PCs prontos para serem eliminados não podem ser simplesmente jogados no lixo.






Gestão de processos de comunicação e operação

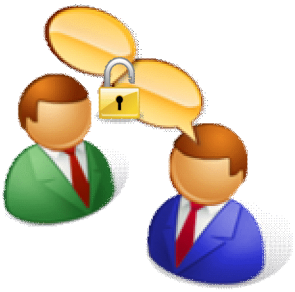
Equipamento móvel

O uso de equipamento móvel está crescendo exponencialmente e tem ainda ganhado mais recursos. É, portanto, aconselhável ter regras para tais equipamentos. Pense sobre as implicações da perda de tais dispositivos. Eles são mais do que hardware: eles também contêm software e dados. Muitos incidentes ocorrem envolvendo equipamentos móveis. Laptops são roubados todos os dias. É muito simples notar uma mala de notebook entre outras bagagens em qualquer aeroporto, tornando as coisas fáceis para os ladrões. É difícil obter seguro contra este tipo de perda. Deixe seu equipamento móvel no trabalho, se possível, ou forneça um meio adequado para armazená-lo quando viajar, combinado com seguro.

Procedimentos devem ser desenvolvidos para armazenar e tratar informação a fim de protegê-la contra publicação não autorizada ou uso indevido. O melhor método para isso é a classificação e a categorização. Este conceito deve ser estendido para os dispositivos móveis. Dispositivos autorizados para usar dados mais sensíveis vão precisar de medidas mais fortes para proteger a informação contra acesso não autorizado ou medidas mais fortes para todos os dispositivos móveis precisarão ser aplicadas.

Gestão de processos de comunicação e operação

Trocando informação



A fim de evitar que informações acabem sendo usadas de forma não pretendida, é importante fazer acordos internos e externos em relação à troca de informações. O propósito da troca de informações, no qual as partes tenham acordado, deve ser documentado. Pode ser acordado com que frequência as informações devem ser compartilhadas e de que forma.

É importante evitar que informações sejam trocadas entre pessoas em diferentes empresas. Sem expectativas claramente documentadas, um funcionário ou contratante pode compartilhar informações confidenciais com uma parte errada, sem perceber o efeito prejudicial que isso pode ter sobre a posição competitiva da sua própria empresa.

Aumentar a conscientização nesta área é uma medida de segurança importante.

Gestão de processos de comunicação e operação

Trocando informação

Mensagens eletrônicas

Mensagens eletrônicas têm mais riscos que a comunicação feita em papel. É por isso que informações trocadas digitalmente devem ser protegidas de forma adequada.

É particularmente importante estar ciente de que quando a informação é enviada por e-mail ela pode ser lida por qualquer um que deseje fazê-lo.

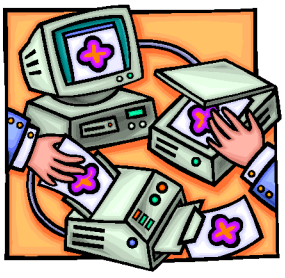
Além do mais, as cópias dos e-mails poderão ser armazenadas em servidores espalhados por todo o mundo.

A internet não escolhe o caminho mais curto, mas o percurso mais rápido. O percurso mais rápido de Londres a Paris em um determinado dia pode ser através de Moscou, Nova Iorque ou Berlim. Se a informação é altamente confidencial, é melhor não enviá-la por e-mail. Se não houver outra forma, assegure-se primeiro de que você protegeu a mensagem com criptografia.

Gestão de processos de comunicação e operação

Trocando informação

Sistemas de informação empresarial



Quando os sistemas dentro de uma empresa estão ligados uns aos outros, os procedimentos devem ser desenvolvidos e implementados com antecedência, a fim de proteger as informações de segurança contra riscos inesperados.

Embora os aplicativos possam ser protegidos eficazmente de forma individual, vulnerabilidades podem surgir quando eles estão ligados, como por exemplo em sistemas de gestão e contabilidade, onde informações são compartilhadas entre as diferentes partes da organização. As vulnerabilidades também podem surgir nas conexões dos sistemas de comunicação da empresa, tais como chamadas telefônicas ou conferências por telefone, conversas telefônicas confidenciais ou armazenamento digital de faxes.

Quando informação (altamente) confidencial está envolvida, é importante lembrar que as impressoras de escritório mais modernas, que muitas vezes são combinadas com scanner, fax copiadora estão equipadas com um disco rígido. Este disco armazena todas as informações processadas. Através de aplicativos especiais, muitas vezes é possível obter acesso a esse disco rígido e copiar todos os dados gravados nele. Além do mais, um "engenheiro de manutenção" poderia levar esse disco rígido para fora do prédio, muitas vezes despercebido.

Gestão de processos de comunicação e operação

Serviços para comércio eletrônico

Quando uma empresa decide estabelecer uma loja pela internet, ela vai encontrar novos riscos além daqueles com os quais se depara quando usa a internet apenas para pesquisa de informações. Serviços de comércio eletrônico e sua utilização devem ser devidamente protegidos. Considere por exemplo: realização de pagamentos seguros (Visa, MasterCard, Dinners, etc.), proteção de informações contra fraudes, condições contratuais claras, não repúdio da aquisição, preços indiscutíveis, etc.

A confidencialidade e a integridade de transações e informações de pagamento, incluindo detalhes de cartões de crédito, endereços, etc., devem ser garantidas aos clientes. Eles precisam estar seguros de que nenhum estranho irá acessar estes dados.

Informações em transações online precisam ser protegidas para garantir que não ocorram transferências incompletas, encaminhamento incorreto, mudanças não autorizadas, publicações não autorizadas, exibição de mensagens não autorizadas, etc.

Slide 35

Gestão de processos de comunicação e operação

Informação publicamente disponível

Informações da empresa que são apresentadas mundialmente ou pela internet são públicas, mas que ainda necessitam ser corretas e não passíveis de manipulação. Informações erradas causam dano à imagem e à reputação da organização. Seria extremamente irritante se você consultasse o website de uma empresa para obter seus dados bancários a fim de realizar um pagamento e depois viesse a descobrir que os dados estavam incorretos e que você realizou o depósito na conta errada.

Pode ser que informações disponíveis em um sistema público (por exemplo, informações de um site) atendam à legislação e regulamentações da localidade onde este se encontra, e, se a transação ocorrer, será onde o site está registrado.

Slide 36