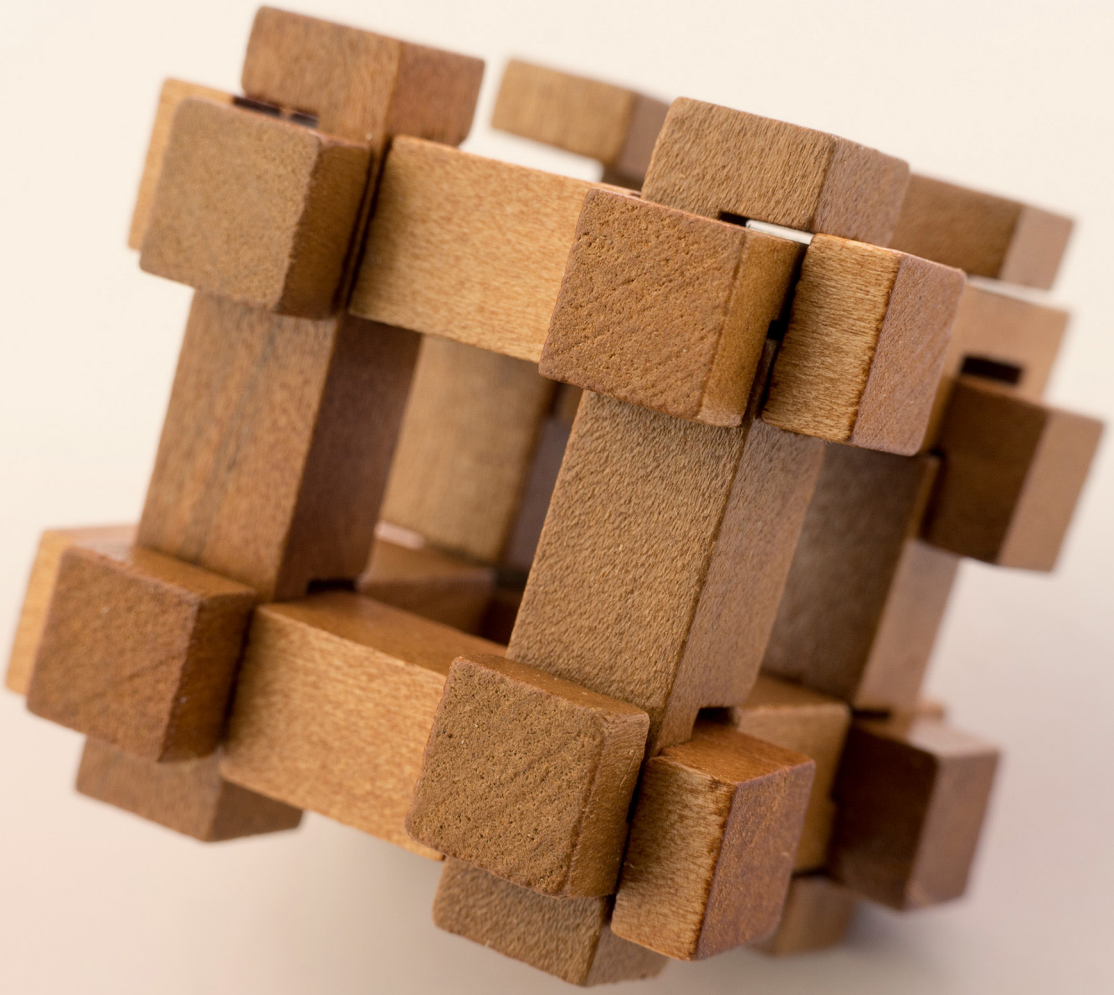
5

GESTÃO EMPRESARIAL

SISTEMAS INTEGRADOS DE GESTÃO

APLICAÇÃO DOS CONCEITOS FUNDAMENTAIS DA SEGURANÇA EM UM ERP



UNIVESP Universidade Virtual do Estado de São Paulo
CPS Centro Paula Souza
GOVERNO DO ESTADO DE SÃO PAULO

5

SISTEMAS INTEGRADOS DE GESTÃO
APLICAÇÃO DOS CONCEITOS FUNDAMENTAIS DA SEGURANÇA EM UM ERP

OBJETIVOS DA UNIDADE DE APRENDIZAGEM

Apresentar e descrever os requisitos de segurança para sistemas ERP. Descrever as medidas e ações que compõem uma política de segurança para um sistema ERP.

COMPETÊNCIAS

Identificar as vulnerabilidades no uso de sistemas ERP. Reconhecer ações e tentativas de quebra da segurança do sistema ERP. Estabelecer rotinas e processos que contribuam para a segurança dos sistemas ERP.

HABILIDADES

Entender como a exploração de vulnerabilidades pode gerar prejuízos a uma organização. Compreender como aplicar os princípios básicos da segurança da informação na utilização de sistemas ERP. Promover mudanças comportamentais em prol do uso seguro de TI.

APRESENTAÇÃO

Agora que já conhecemos bem os conceitos ligados aos Sistemas Integrados de Gestão – ERPs, vamos aprender sobre um assunto muito importante para o sucesso do uso destes sistemas.

Vamos explorar os conceitos de ameaça, vulnerabilidade e risco e suas implicações na operação de um sistema ERP. Ao final desta Unidade você vai compreender que as aplicações dos conceitos básicos de segurança da informação podem ajudar a prevenir prejuízos por falhas de segurança da informação. A segurança da informação é um processo que depende de todos os envolvidos para que dê certo.

Estude e veja como aplicar os conceitos aprendidos.

PARA COMEÇAR

A notícia abaixo não é uma novidade, porém quanto mais se avança no uso das tecnologias da informação, mais os dados das organizações ficam mais expostos a ataques.

Profissionais colocam interesse pessoal à frente de segurança da empresa[1]

SÃO PAULO – Uma pesquisa realizada pela Trend Micro nos Estados Unidos, Reino Unido, Alemanha e Japão, revelou que os funcionários colocam o interesse pessoal à frente da segurança da empresa, adotando práticas arriscadas no uso da tecnologia.

De acordo com os dados, 60% dos 1,6 mil entrevistados admitiram ter divulgado informações internas por meio de uma conta de e-mail, mensagens instantâneas ou aplicativos de mídias sociais.

E se você pensa que no Brasil é diferente, o diretor de Novos Negócios da Trend Micro, Hernan Armbruster, afirmou que não. “A pesquisa foi feita em outros países, mas a nossa experiência mostra que isso também acontece no Brasil”, revelou.

1. Disponível em: http://economia.uol.com.br/planodecarreira/ultnot/infomoney/2010/09/29/ult4229u3904.jhtm

Dentro e fora

A pesquisa mostrou que os funcionários remotos são mais abusados do que os colegas internos. Em todos os países, 60% deles admitiram ter enviado informações confidenciais da empresa por mensagens instantâneas, ante 44% dos funcionários que atuam internamente.

"A exposição ao risco aumenta com o usuário móvel. Fica muito difícil conciliar vida pessoal e profissional, porque o profissional abre o notebook em uma viagem para assistir a um filme, checa e-mails pessoais etc. A tendência é que arrisque mais pela natureza do trabalho", explicou.

O uso de redes de computadores, notebooks e da internet abriu um universo de possibilidades de melhoria da produtividade para os funcionários das empresas.

Na mesma proporção, ou talvez em maior nível, um grande contingente de pessoas tenta usar estes mesmos recursos para obter vantagens ou informações confidenciais de pessoas ou empresas.

O inimigo mais conhecido é o "hacker", elemento que navega na Internet com o objetivo de cometer atos ilícitos, desde a simples visita a sites privados ao desvio de milhões de dólares de contas bancárias.

Como nos proteger destas ameaças? Quais são seus hábitos no uso da Internet? Você costuma abrir email de desconhecidos? Você navega por sites suspeitos? Para quem usa um computador pessoal, quais são os conselhos que você daria para melhorar a segurança?

Figura 1. Ataque ao Worl Trade Center.

A imagem da página anterior apresenta o ataque às torres do *Word Trade Center* em 11 de setembro de 2001.

Os prejuízos causados por este ataque foram muito grandes. O que será que aconteceu com as empresas que operavam nas Torres Gêmeas? Será que alguma ainda existe?

No caso de empresas com matriz e filiais, como ficaram os dados que estavam no centro da tragédia? Prever uma catástrofe desta magnitude não é algo tão simples. Porém, algumas empresas se recuperaram rapidamente após este evento, enquanto outras desapareceram.

Será que a perda de dados teve alguma influência nos destinos das empresas?

Talvez não tenhamos as respostas para todas as situações que ocorreram no evento.

Podemos dizer que, em muitos casos, procedimentos simples de segurança da informação poderiam diminuir os prejuízos causados.

FUNDAMENTOS

1. SEGURANÇA DA INFORMAÇÃO

A Era da Informação alterou o foco da fonte de riqueza das organizações dos meios de produção para a produção de informação e conhecimento.

Para Fontes (2006), a informação é um recurso que move o mundo e é mais que um conjunto de dados. Transformar dados em informação é converter algo que tem baixo significado prático em um recurso fundamental para a vida pessoal ou profissional.

A informação tornou-se um bem fundamental para a continuidade e existência de uma organização.

Então, o que é segurança da informação?

> *A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida. Isto é essencialmente importante no ambiente de negócios, cada vez mais interconectado. [...]*
>
> *Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.*
>
> *A Segurança da Informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. [ABNT NBR ISO/IEC 17799:2005, p. IX]*

Turban (2010) informa que até o ano de 2002 a atribuição da proteção de informações corporativas e de sistemas de computador era considerada uma questão técnica de responsabilidade do departamento de TI. O tratamento de incidentes era realizado caso a caso e a segurança de TI tinha o status de custo, não de um recurso ou investimento para diminuir os prejuízos causados por incidentes que paralisam as operações da empresa.

Fontes (2006) complementa indicando que, quando começamos a trabalhar em uma organização, devemos ter em mente que a informação é um bem que tem valor para a empresa e deve ser protegida. Assim como protegemos os recursos financeiros e materiais, devemos criar mecanismos de proteção para a informação, um recurso crítico para a realização dos negócios. Sua utilização deve ser pautada por normas e procedimentos.

Segundo ISO/IEC 27.002 a segurança da informação tem grande importância para os negócios, sejam eles do setor público ou providos na proteção de infraestruturas críticas.

Brasil é um dos países mais vulneráveis a ataques cibernéticos, diz pesquisa da BBC Brasil[2]

Em uma comparação feita entre 14 países, um estudo colocou o Brasil como o país que menos atualiza seus programas de defesa contra piratas virtuais e o que mais sofre chamados ataques de negação de serviço (DDoS, na sigla em inglês) – aqueles em que invasores sobrecarregam um sistema para tirá-lo do ar. [...] Os pesquisadores entrevistaram 600 diretores de segurança da informação de 14 países [...] Dentre os brasileiros ouvidos, 65% disseram que as leis do país não são adequadas para combater crimes virtuais. Mais de 60% acreditam que o Brasil sofrerá nos próximos dois anos um ataque cibernético que afetará seriamente algum de seus serviços essenciais, como fornecimento de energia. [...]

2. Disponível: http://www1.folha.uol.com.br/folha/bbc/ult272u687406.shtml

A notícia acima levanta um sério problema para as organizações.

Os casos do apagão elétrico no Brasil em 2009 e dos problemas do serviço de internet rápida da Telefônica em abril de 2009 teriam sido causados pela invasão dos sistemas de computação por "piratas virtuais".

Os fatos relatados nos levam a crer que existe em um grande número de organizações no Brasil que ainda não tratam as questões da segurança da informação a sério.

Como podemos iniciar ações que nos levem a uma situação de menor risco? Vamos começar compreendendo o funcionamento da segurança da informação.

2. PRINCÍPIOS FUNDAMENTAIS

Harris (2008) e Tittel (2003) indicam que a segurança da informação apresenta três princípios fundamentais:

- **Confidencialidade:** tem como finalidade garantir que o correto nível de segredo de uma informação será reforçado pelo processamento dos dados e pela prevenção de exposição não autorizada. O grau de confidencialidade deve ser preservado para as informações que estão armazenadas nos sistemas e para a transmissão até o seu destino. Os ataques à confidencialidade podem ocorrer pelo monitoramento da rede, pelo roubo de arquivos de senhas ou engenharia social (quando alguém engana outra pessoa para obter acesso não autorizado a informações). Os usuários podem expor uma informação confidencial de forma intencional ou acidental, nos dois casos informações importantes podem ficar expostas. Os autores sugerem as seguintes ações para melhorar confidencialidade:

  - **Criptografia:** criptografar os dados armazenados e que são transmitidos por uma rede de dados;
  - **Controle de acesso:** definir quem tem direito de acesso para cada informação e quais os direitos concedidos;
  - **Classificação da informação:** definir o nível de segredo que a informação tem e assim determinar a correta proteção e níveis de acesso;
  - **Treinamento e procedimentos:** treinamento dos usuários no uso correto da informação e dos dispositivos de acesso à informação. O uso correto deve ser definido em procedimentos documentados e divulgados a todos os usuários.

  A garantia da confidencialidade é uma das tarefas de maior dificuldade de implementação, pois em suas ações são levados em conta todos os elementos que fazem parte da comunicação da informação, o valor da informação para a organização e os impactos causados pela divulgação indevida.

- **Integridade:** a integridade é mantida quando temos a garantia de precisão e confiabilidade das informações e do sistema e quando não são permitidas modificações não autorizadas. O hardware, o software e os mecanismos de comunicação devem trabalhar de forma a manter os dados corretos e movimentá-los para seus destinos sem alterações inesperadas. Os sistemas e a rede devem ser protegidos

de interferência externa e contaminação. Ambientes onde são aplicados estes atributos de segurança garantem que invasores (ou que erros cometidos pelos usuários) não comprometam a integridade dos sistemas ou dados. Quando um hacker insere um vírus, uma bomba lógica, ou uma porta dos fundos no sistema, a integridade do sistema é comprometida. Isso pode, por sua vez, afetar negativamente a integridade das informações mantidas. O controle estrito de acesso, a detecção de intrusão, entre outros métodos, podem combater essas ameaças. Portanto, a informação íntegra é aquela que não foi alterada de forma indevida ou não autorizada;

- **Disponibilidade:** os sistemas e redes de computadores apresentam uma adequada capacidade de desempenhar suas funções de maneira previsível e em um nível de desempenho aceitável. Eles devem ter a capacidade de se recuperar de rompimentos do funcionamento de modo a não afetar a produtividade da empresa. Pontos únicos de falha devem ser evitados e, quando necessário, devem ser instaladas políticas de backup e mecanismos de redundância. A disponibilidade é a garantia de que a informação estará acessível quando necessária, e relaciona-se a toda infraestrutura ligada à informação e aos serviços prestados por ela: acesso, trânsito e armazenamento.

A aplicação destes princípios tem como objetivo diminuir os riscos a que a informação está sujeita e minimizar os prejuízos no caso de incidentes.

Tabela 1.
Adaptada de Turban, (2010, p. 643).

RESULTADOS DA PESQUISA CSI/FBI: PERDAS EM 2004 E 2005

Categoria de Crime	Perda por inquirido		Porcentagem de mudança de 2004 a 2005
	2004 (n=269)	2005 (n=639)	
Acesso não autorizado a informações	$51.545	$303.234	488%
Roubo de informações proprietárias	$168.529	$355.552	111%
Perdas totais de outros os crimes	$526.010	$203.606	61%

O crescimento das perdas causadas por crimes, indicado na tabela 1, não pode ser o único argumento para o investimento em segurança, assegura Turban (2010). O custo de se eliminar um único incidente pode ser muito grande, isto sem levar em conta o que aconteceu: queda de sistemas de informações-chave, roubo de dados de clientes e produtos, desvio de dinheiro e desativação de operações de comércio eletrônico.

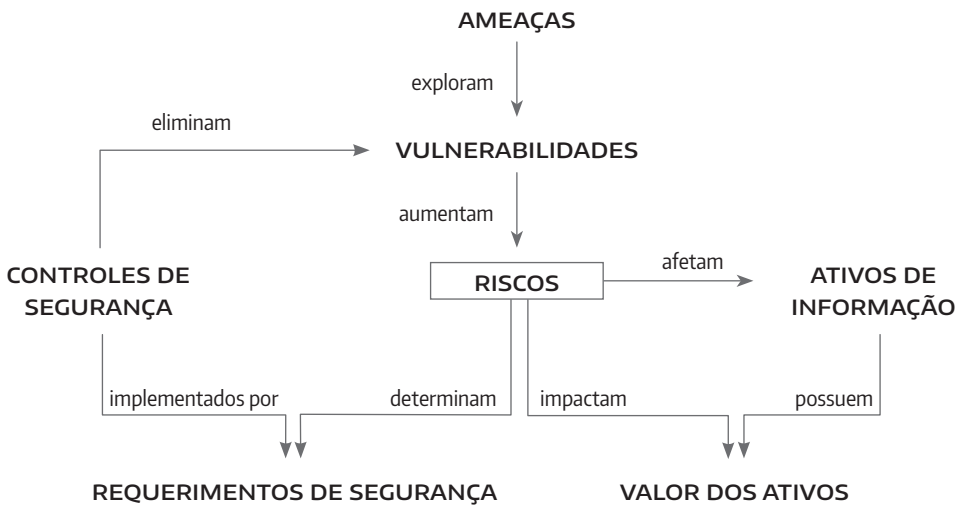
3. CONCEITOS GERAIS DA SEGURANÇA DA INFORMAÇÃO

Os princípios fundamentais da segurança da informação têm como finalidade diminuir os riscos a que estão sujeitos os ativos de uma organização. Para compreender como eles são colocados em prática é necessário apresentar alguns conceitos fundamentais da segurança da informação.

Ramos (2008) apresenta os elementos que são usados nas definições de incidentes de segurança da informação:

- **Ativos de informação:** a informação propriamente dita, toda a infraestrutura ligada à informação e as pessoas que têm acesso a informação;
- **Valor dos ativos:** é a importância para a empresa, pode ser medida pelo custo de reposição, pelo prejuízo com a perda ou ainda pelo comprometimento da imagem da organização;
- **Requerimentos de segurança:** ações necessárias para diminuir a probabilidade de um risco se efetivar;
- **Controles de segurança:** ações e procedimentos que atendem aos requerimentos de segurança; visam eliminar as vulnerabilidades dos ativos de informação;
- **Vulnerabilidade:** é uma fraqueza de procedimento, software ou hardware, que permite que um hacker invada um computador ou uma rede de computadores, obtendo acesso a recursos nestes ambientes. Uma vulnerabilidade pode ser caracterizada pela ausência ou fraqueza de uma salvaguarda que pode ser explorada;
- **Ameaça:** pode ser compreendida como a ausência ou falhas em mecanismos de proteção que não previnem algum perigo potencial para a informação ou para os sistemas. A ameaça ocorre quando há a tentativa de exploração de uma vulnerabilidade. A entidade que obtém vantagem da vulnerabilidade é conhecido como “agente”;
- **Risco:** é a probabilidade de uma ameaça se concretizar combinada com os impactos que ela trará. É a principal métrica gerencial da segurança da informação: quanto maior a probabilidade de uma ameaça se concretizar e o impacto associado a ela, maior o risco.

Figura 2. Ciclo de identificação de vulnerabilidades, ameaças e riscos.



3.1. CONFIDENCIALIDADE

A confidencialidade está ligada ao processo de classificação da informação e à concessão de direito de acesso à informação. Os direitos de acesso são disponibilizados quanto à necessidade de acesso e à classificação da informação.

Tabela 2. Exemplos de classificação da Informação.
Fonte: Adaptada de Ramos (2008, p. 111).

GOVERNO BRASILEIRO	EMPRESA PRIVADA
Ultra-secreto	Confidencial
Secreto	Restrita
Confidencial	Interna
Reservado	Pública

Em um contexto empresarial, o autor complementa que a informação pode ser classifica como:

- **Confidencial:** informação com importância vital para empresa. Sua divulgação de forma incorreta pode tornar incerta a continuidade do negócio;
- **Restrita:** informação em que o acesso é concedido para um grupo de pessoas. Sua violação afeta um ou mais processos de negócio da empresa;
- **Interna:** informação que só deve ser utilizada internamente. A divulgação pública pode causar prejuízos à imagem da empresa ou outros danos indiretos;
- **Pública:** informação que pode ser de divulgada ao público em geral.

Agora que classificamos a informação, vamos definir como concedemos acesso a ela. Harris (2008) considera três momentos no processo de controle de acesso:

- **Identificação:** nesta fase, cada usuário recebe um **nome no sistema** (*username*) que será sua identidade de acesso ao sistema. Ele será usado, se necessário, para identificar o autor de determinada ação;
- **Autenticação:** para acessar o sistema, o usuário deve identificar-se com *username* e fornecer sua senha (*password*). O conjunto correto de *username+password* dá acesso aos usuários, autenticando sua identidade;
- **Autorização:** após a autenticação, o acesso do usuário é controlado pelas permissões que foram concedidas a ele.

Todo o processo descrito acima não vai funcionar se:

- O usuário compartilhar seu *username* e senha com outros colegas de trabalho – que, normalmente, têm menos permissões de acesso);
- O usuário tiver uma senha muito difícil de ser memorizada, obrigando-o a escrevê-la em um papel e afixá-lo no monitor;
- O usuário não for alertado para não deixar seu computador com a sessão de trabalho aberta quando se ausentar.

3.2. INTEGRIDADE

A integridade dos dados está ligada ao controle de acesso, assim como a confidencialidade. No caso da integridade, podemos incluir a qualidade dos dados. Tittle (2003) apresenta as seguintes situações quanto a este aspecto:

- **Relevante:** a perda de integridade pode gerar transtornos com baixo impacto para a empresa. Neste caso, devem ser adotados controles usuais que promovam a garantia da integridade como a manutenção de uma cópia ou original de segurança, o controle e registro dos acessos etc;
- **Básica (ou normal):** é aquela cuja perda de integridade a partir de um determinado prazo não implica impactos à empresa e, portanto, não exige controles de auditoria e de acesso.

A confiabilidade dos dados está diretamente ligada aos controles de acesso e integridade. Um dado confiável é aquele que está integro e correto.

Sem dados confiáveis, toda e qualquer decisão poderá ser tomada de forma errada, causando prejuízos à organização. A base do processo de tomada de decisão está na existência de dados confiáveis.

3.3. *DISPONIBILIDADE*

O princípio da disponibilidade afirma que a informação deve estar disponível sempre que for solicitada por um usuário com direito de acesso.

Como garantir a disponibilidade dos dados?

- Garantir que a infraestrutura de comunicação esteja em condições de manter o acesso à fontes de dados com redundância para evitar a paralisação em eventuais incidentes;
- Garantir que as fontes de dados suportem o acesso concorrente de um número de usuários que seja comum na empresa;
- Garantir que os sistemas corporativos tenham interfaces de acesso aos dados compatíveis com as necessidades dos usuários;
- Definir políticas de cópias de segurança (backup) dos dados que garantam a rápida recuperação de eventuais incidentes;
- Implementar planos de recuperação de desastres que garantam o reinício das operações da empresa no menor tempo possível.

ATENÇÃO

A maior parte do trabalho para se manter a disponibilidade da informação está na manutenção da redundância dos recursos necessários para o armazenamento, transmissão e acesso.

A rápida resposta à perda de dados pode diminuir os prejuízos causados pela parada dos sistemas de informação.

4. PREMISSAS DE SEGURANÇA

A segurança da informação apresenta algumas premissas que, quando implementadas, melhoram a eficácia do processo. Tipton (2004) apresenta uma lista delas:

- **Não repúdio:** garantia de que a autoria de uma ação por um usuário não possa ser negada;
- **Auditoria:** manutenção de registros das ações executadas para todos os usuários do sistema, verificação posterior da autoria de alguma atividade e determinação de responsabilidades;

- **Saber apenas o necessário *(Need to know):*** apresentar ao usuário apenas as funções necessárias para a execução de suas tarefas rotineiras;
- **Mínimos privilégios *(Least privileges):*** o usuário deve ter acesso apenas às funções que necessita para realizar seu trabalho;
- **Rotação de funções *(Job rotation):*** a troca de funções entre usuários tem o objetivo de manter o conhecimento das tarefas compartilhado entre vários colaboradores e diminuir a possibilidade de conluio entre usuários em funções chaves;
- **Separação de funções *(Separation of duties):*** também conhecida como segregação de funções, consiste em dividir entre mais de uma pessoa as atividades de realização de uma tarefa e as atividades de verificação ou auditoria desta mesma tarefa. Esta premissa tem o objetivo de diminuir a probabilidade de fraudes;
- **Férias obrigatórias *(Mandatory vacation):*** neste caso, o usuário é colocado em férias para a verificação de suspeita de ações ilícitas. Se as ações cessarem, existe grande possibilidade de o funcionário ser o autor.

DICA

A aplicação destes conceitos pode diminuir a possibilidade de se ter problemas de segurança. Porém, o treinamento adequado e conscientização dos usuários são fundamentais para o sucesso da implantação de políticas de segurança.

A aplicação destes princípios isoladamente ou combinados pode melhorar a segurança na operação de um sistema ERP.

A segurança da informação é uma ação coletiva e deve fazer parte das premissas de funcionamento da organização.

Turban (2010) indica que regulamentos internacionais e governamentais exigem que os dados de clientes sejam protegidos contra esquemas de ataques e que os ativos de informação devem ser geridos com responsabilidade.

A governança corporativa é uma exigência do mercado. A responsabilização dos diretores das empresas pelos prejuízos causados pela má administração está prevista em leis como a Sabane/Oxley (Sox) dos Estados Unidos, que prevê a aplicação de modelos de boas práticas na gestão das empresas e a garantia da implantação de políticas de segurança da informação.

Em seu quarto estudo anual sobre segurança da informação e força de trabalho lançado em 2006, a *Computing Technology Industry Association*

(CompTIA), um grupo sem fins lucrativos, afirmou que o erro humano era responsável por quase 60% de brechas de segurança da informação das organizações em 2005 – em comparação aos 47% do ano anterior. Contudo, apesar do papel-chave do comportamento humano nas brechas de segurança da informação, somente 29% das 574 organizações governamentais, financeiras, educacionais e de TI mundialmente pesquisadas disseram que o treinamento em segurança era um requisito em suas empresas. Apenas 36% das organizações ofereciam treinamento de conscientização sobre segurança ao usuário final. (TURBAN, 2010, p. 646)

Todo investimento em tecnologia e em pessoal especializado em segurança da informação será em vão se o usuário não receber o treinamento adequado nem for objeto de um trabalho de conscientização sobre a importância de seguir as orientações e regras das políticas de segurança da informação.

ANTENA **PARABÓLICA**

A segurança da informação tem grande importância na implantação e operação de sistemas integrados de gestão. As organizações não estão mais isoladas e não contam com funcionários trabalhando diretamente na planta principal.

Os desafios de se manter a segurança da informação não são questões apenas de TI, envolvem decisões sobre a localização da empresa, do núcleo de processamento de dados dentro da organização, das políticas de controle de acesso físico e lógico aos ativos de informação.

O uso do computador pessoal deve ser pautado por ações para a segurança da informação: manter um software antivírus atualizado, não navegar por sites suspeitos, não abrir e-mails de pessoas desconhecidas, desconfiar de mensagens de pessoas conhecidas com assuntos estranhos, não acreditar que aqueles com quem se conversa on-line são quem dizem ser.

As regras apresentadas valem também para o computador da empresa em que se trabalha.

Os sistemas ERP apresentam um esquema de controle de acesso. Manter sua senha em sigilo é fundamental para a manutenção da segurança.

Todas as informações geradas na empresa são integradas no Banco de Dados do sistema ERP. A segurança destas informações depende de uma série de ações empreendidas pelo pessoal de TI. Porém, se o usuário não for devidamente treinado para o uso correto da ferramenta e conscientizado da importância dos procedimentos relativos à segurança da informação, a segurança vai falhar e dados importantes podem ser violados.

E AGORA, JOSÉ?

Nesta UA estudamos a segurança da informação e sua relação com sistemas integrados de gestão. A segurança da informação é fundamental para que o uso de

sistemas ERP tenha condições de fornecer informações para a tomada de decisão. Vimos também que o usuário de sistemas de informação tem um papel fundamental na garantia da segurança.

Na próxima UA vamos conhecer o processo de implantação de um programa ERP.

Bons estudos.

REFERÊNCIAS

ABNT NBR ISO/IEC. **Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação** – ISO/IEC 27002:2005.

HARRIS, S. **All in One CISSP® Exam Guide, Fourth Edition.** MacGraw Hill: New York, 2008.

RAMOS, A. **Guia Oficial para Formação de Gestores em Segurança da Infomação: Secutity Officer 1.** Zouk: Porto Alegre, 2008.

TIPTON, H. F. **Types of Information Security Controls. In:** _____. (Org). **Information Security Management Handbook. 5 ed.** Boca Raton, CRC Press, 2004. p 113-125

TITTEL, E. CHAPPLE, M. STEWART, J. M. **CISSP®: Certified Information Systems Security Professional - Study Guide.** Sybex: San Francisco, 2003.

TURBAN, E.; LEIDNER, D.; MCLEAN, E.; WETHERBE, J. **Tecnologia da Informação para Gestão: Transformando os negócios na economia digital.** 6 ed. Bookman: Porto Alegre, 2010.