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 8

Legislação e regulamentações

Este módulo cobre:

- Observação das regulamentações
- Adequação, medidas de conformidade
- Direitos autorais
- Documentos do negócio a serem protegidos
- Proteção e confidencialidade de dados pessoais
- Prevenção de abuso das instalações de TI
- Observação da política de segurança e das normas de segurança
- Monitoramento
- Auditoria

Slide 2

Legislação e regulamentações

Observância de regulamentos legais

A meta primária de toda empresa é alcançar seus próprios objetivos de negócio. Isto significa produzir certo tipo de produto ou fornecer certos serviços. Cada empresa, entretanto, precisa observar legislação, regulamentos e obrigações contratuais locais e internacionais. Os requisitos de segurança a que uma empresa precisa atender estão relacionados a estes. A polícia e órgãos de investigação vão assegurar que certa legislação e regulamentos estão sendo observados.

Legislação local e regulamentos podem ser projetados/desenhados para facilitar às empresas que operam internacionalmente – cuja política é um pouco mais genérica e cujos documentos de política relacionados devem ser adaptados à legislação em vigor no país em que elas se baseiam – para fazer negócios localmente.

Exigências legislativas podem diferir um pouco, particularmente na área de privacidade. Portanto, a maneira na qual se lida com a informação privada também pode diferir.

A fim de assegurar que os requisitos regulatórios e legislativos são observados, é sempre importante procurar uma consultoria jurídica.

Slide 3

Conformidade

Conformidade está relacionada a algo que uma organização deve atender. Uma organização precisa observar tanto regulamentos internos como leis, requisitos de legislação e regulamentos locais.

Algumas vezes isso pode causar conflitos. Organizações multinacionais em particular devem cumprir, por um lado, sua política interna para assegurar que a empresa opera de forma consistente. Por outro lado, devem atender à legislação e regulamentos locais e internacionais.

Legislação e regulamentos relacionados à privacidade são os mesmos dentro da União Européia, mas são um pouco diferentes nos EUA.

Conformidade não envolve apenas observar a legislação e regulamentos prescritos por governos, mas regras internas também devem ser consideradas. Nos últimos anos, padrões internacionais para segurança da informação têm sido desenvolvidos em forma de guias ou requisitos para Segurança da Informação. Derivado do Padrão Britânico BS 7799, um padrão ISO foi desenvolvido e é agora conhecido como ISO 27002.

Vários organismos de padronização na União Européia e outros internacionais têm adotado este padrão ISO. Deste modo, um padrão com medidas de segurança tem sido criado por governo e empresas.

Slide 4

Medidas de conformidade

Como resultado do que foi mencionado anteriormente, tem se tornado claro que elaborar a política interna dentro de uma organização é uma forma de estar em conformidade (em inglês, compliant).

A organização precisa produzir uma política na qual ela declara que é preciso cumprir a legislação e regulamentos nacionais e locais. Procedimentos e subsídios precisam ser desenvolvidos para ajudar funcionários a aplicar estes regulamentos na prática. Uma análise de riscos precisa ser conduzida para assegurar que níveis de segurança sejam estabelecidos, e medidas apropriadas para estes níveis de segurança sejam determinados e implantados.

Slide 5

Direitos de Propriedade Intelectual – DPI

As seguintes diretrizes precisam ser consideradas a fim de proteger o material que pode ser considerado propriedade intelectual, como software, por exemplo:

- Publicar uma política relacionada a conformidade com direitos de propriedade intelectual, na qual uso legal dos programas de computador de produtos de informação são definidos.
- Manter conscientização da política para proteção de direitos de propriedade intelectual. Incluir na política de DPI as medidas disciplinares que a organização irá tomar contra qualquer funcionário que a viole.
- Direitos de propriedade intelectual incluem direitos de cópia (copyright) para programas de computador, documentos, direitos de projetos, marcas, patentes e licenças de código-fonte.
- Apenas comprar programas de computador de fornecedores conhecidos e de boa reputação, para assegurar que nenhum direito de cópia é infringido.
- Se for de fonte aberta (open source), a licença associada precisa ser respeitada e observada.
- Manter um registro de ativos e identificar todos os ativos com requisitos relacionados à proteção de direitos de propriedade intelectual.
- Programas de computador que são assunto de direitos de propriedade são geralmente fornecidos com base em um acordo de licença no qual se declaram as condições de uso.

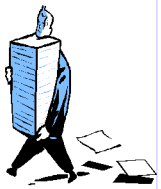
Slide 6

Protegendo documentos do negócio

Documentos importantes do negócio precisam ser protegidos contra perda, destruição e falsificação de acordo com os requisitos legais e regulatórios. O mesmo se aplica, claro, a obrigações contratuais. Convém que registros sejam categorizados em tipos, como contábeis, de base de dados, de transações, de auditoria e procedimentos operacionais, cada qual com detalhes do período de retenção e do tipo de mídia de armazenamento, como por exemplo papel, microficha, meio magnético ou ótico.

Quaisquer chaves de criptografia relacionadas com arquivos cifrados ou assinaturas digitais devem também ser armazenadas, para permitir a decifração de registros pelo período de tempo em que eles são mantidos. Cuidados devem ser tomados a respeito da possibilidade de deterioração das mídias usadas no armazenamento dos registros. Convém que os procedimentos de armazenamento e manuseio sejam implementados de acordo com as recomendações dos fabricantes. Convém que para armazenamento de longo tempo o uso de papel e microficha seja considerado.

Alguns registros podem precisar ser retidos de forma segura para atender a requisitos estatutários, contratuais ou regulamentares, assim como para apoiar as atividades essenciais do negócio. Exemplo disso são os registros que podem ser exigidos como evidência de que uma organização opera de acordo com as regras estatutárias e regulamentares, para assegurar a defesa adequada contra potenciais processos civis ou criminais ou confirmar a situação financeira de uma organização perante os acionistas, partes externas e auditores.



Slide 7

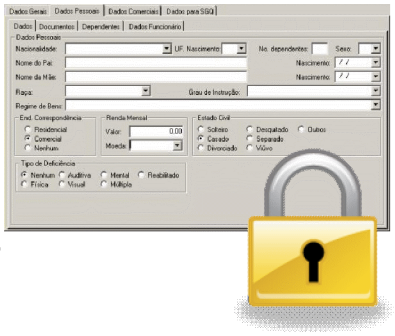
Proteção de dados e confidencialidade de dados pessoais

A proteção de dados e a privacidade dos dados pessoais são definidas pela legislação. Adicionalmente, acordos contratuais com clientes podem ser gerenciados à parte.

Cada organização deve ter políticas para proteção de dados pessoais, a qual deve ser conhecida de todos que processam estes dados.

A observação desta política, de leis relevantes e de regulamentações para proteção de dados pode ser melhor realizada se houver uma pessoa responsável que dê apoio aos gerentes, usuários e provedores de serviço que atuam nesta área.

Claro que medidas de proteção técnicas e organizacionais também devem ser implementadas.



Slide 8

Prevenção de uso abusivo das instalações de TI

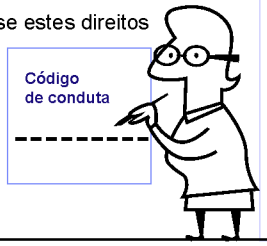
Um dos aspectos que a gestão deve incluir na política de segurança da informação é a forma que as instalações de TI podem ser usadas dentro da organização. O uso destas instalações para propósitos pessoais ou não autorizados deve ser considerado uso inapropriado das instalações.

Se uma atividade não autorizada é observada por monitoramento ou outro meio, esta atividade necessita ser levada ao conhecimento da gestão, a qual deve considerar se alguma medida disciplinar deve ser aplicada.

Existem dois lados nesta questão: de um, a organização necessita atender às regulamentações mencionadas anteriormente, levando em conta o correto uso das licenças, somente uso legal de software e correta observação dos direitos autorais, e de outro, é esperado dos funcionários que não abusem das instalações disponíveis para eles. Em muitas organizações há um código de conduta que estipula os direitos e funções dos funcionários e do empregador neste tema.

Em muitas organizações existe monitoramento para verificar se estes direitos estão sendo corretamente usados.

Existe também legislação para prevenção de crimes conduzido através do uso de computadores, como por exemplo "negação de serviço": um site é atacado (inundado de solicitações) até que falhe e não consiga mais dar atendimento.



Slide 9

Atendendo à política e às normas de segurança

Segurança da informação envolve responsabilidade em diversos níveis. A direção da organização deve sempre assumir a responsabilidade final. Gerentes necessitam regulamente ser orientados e assessorados a respeito dos dados processados dentro de suas áreas de responsabilidade, para saber se eles estão atendendo à política de segurança, às normas ou a outros requisitos de segurança.

Nos próximos slides veremos alguns acordos e legislações relevantes no Brasil em termos de segurança da informação, abrangendo análise de risco, confidencialidade de dados e plano de continuidade do negócio.

Este assunto é abordado apenas para que você tenha uma visão geral – pois ele não cai no exame.

Slide 10

Acordo de Basileia II

- O Acordo de Basileia II afeta as instituições de crédito (bancos) e instituições de investimentos.
- Sob o enfoque da administração de risco mais rígida, o Acordo de Basileia de 1988 firma exigências mínimas de capital que devem ser respeitadas por bancos comerciais como precaução contra risco de crédito.
- Estabelece regras para que os bancos centrais executem auditorias nas instituições financeiras, verificando se estas têm gerenciamento de riscos operacionais e de crédito adequados.
- Do ponto de vista da governança corporativa e de TI, o Acordo de Basileia se aplica à exigência da criação de políticas de gerenciamento de riscos para garantir total segurança e confidencialidade dos dados de clientes. Isso exige que as empresas do setor alterem processos e sistemas para cumprir as regras do novo acordo[1].

Fontes:
[1] Mateo, Jose Gomiz em http://www.timaster.com.br/revista/artigos/main_artigo.asp?codigo=931

Slide 11

Resolução 3380 do Banco Central

- Em junho de 2006 foi publicada a Resolução 3380 do Banco Central do Brasil, que determina que as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil implantem a sua própria estrutura de gerenciamento do risco operacional.
- Para os efeitos desta resolução, define-se como risco operacional a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e **sistemas**, ou de eventos externos.
- As implicações desta resolução para a TI de uma instituição financeira são [1]:
  - → Identificar, avaliar, monitorar, controlar e mitigar os riscos operacionais de TI que afetam a instituição
  - → Desenvolver e implementar um Plano de Continuidade de TI em apoio às atividades da instituição
  - → Gerenciar os riscos que os prestadores de serviços representam para a continuidade do negócio

Fontes:
[1] FERNANDES, Aguinaldo Aragon. Implantando a Governança de TI

Slide 12

Outros regulamentos no Brasil

- **SUSEP** (Superintendência de Seguros Privados)
  - → Exige que as operadoras de seguros tenham uma política de segurança da informação e um plano de continuidade das operações.
- **ANS** (Agência Nacional de Saúde)
  - → As operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde devem constituir proteções administrativas, técnicas e físicas para impedir o acesso eletrônico ou manual impróprio à informação de saúde. Recomenda o uso da norma NBR ISO/IEC 27002 para cumprir os objetivos de segurança da informação.
- **CVM** (Comissão de Valores Mobiliários)
  - → Compete às corretoras eletrônicas garantir a segurança e o sigilo de toda a informação sobre seus clientes, suas ordens de compra ou venda de valores mobiliários e sua carteira de valores mobiliários, bem como sua comunicação com os clientes, devendo utilizar elevados padrões tecnológicos de segurança de rede.
- **Governo** – decreto 3.505/2000
  - → Institui a política de segurança da informação nos órgãos e entidades da administração pública federal.
- **TCU** (Tribunal de Contas da União)
  - → Criou a SEFTI – Secretaria de Fiscalização de Tecnologia da Informação – que fiscaliza e avalia programas de governo na área de TI. Está auditando com base no COBIT.

Monitoramento e auditorias

Medidas de monitoramento

Finalmente, o auditor interno ou externo irá verificar se a organização está atendendo às regulamentações. O auditor verifica se as medidas definidas estão sendo aplicadas, isto é, se o que foi definido esta sendo usado na prática e se as medidas funcionam como deveriam. Por exemplo: uma medida é o uso de password com 8 caracteres que tenha no mínimo uma letra e um número.

O auditor olha o que está estabelecido e amostra algumas passwords para verificar se os requisitos definidos foram efetivamente implantados.

Auditorias do sistema da informação

Realizar auditorias sempre envolve riscos para o processo de produção de uma organização. Auditores sempre pegam informação de um sistema enquanto ele está processando. Isto sempre afeta a capacidade de processamento do computador, porque ele tem que realizar tarefas extras. Portanto, é importante garantir que não hajam falhas ou paradas devido ao processo de auditoria.

Devido a isso não é aconselhável ter uma terceira parte ou um cliente examinando a mesma atividade. O auditor pode notificar a terceira parte quando encerrar suas atividades. Essa declaração é feita pelo auditor indicando em qual extensão as medidas necessárias estão funcionando, em termos de set-up, implementação e operação.

Proteção adicional usada para auditoria de sistemas da informação

A ajuda usada para auditorias de sistema, como por exemplo programas de computador ou bancos de dados, deve ser conservada separada dos sistemas de desenvolvimento e produção, e não deve ser armazenada em fitas de biblioteca ou salas de usuários sem a devida medida de proteção conforme for adequado.

Se terceiras partes estão envolvidas em uma auditoria, existe o risco de que o auxílio da auditoria e a informação que a terceira parte está acessando possam se misturar.

Medidas como limitação de acesso para somente aqueles sistemas que o auditor necessita para sua investigação, um acordo de confidencialidade e limitação do acesso físico podem ser consideradas um auxílio para a limitação deste risco. Uma vez que a auditoria esteja completa, a organização deve imediatamente alterar qualquer password que tenha sido fornecida ao auditor.

Finalmente, após tudo ter sido discutido, apenas uma regra imutável deve ser aplicada: não importa como a organização tenha planejado sua segurança, segurança sempre será sua força e sua fraqueza.