Entendendo e implementando a Norma ABNT NBR ISO/IEC 17799:2005

Academia Latino-Americana de Segurança da Informação

Aspectos teóricos e práticos para implantação da Norma ABNT NBR ISO/IEC 17799:2005

Módulo 4

Entendendo e implementando a Norma ABNT NBR ISO/IEC 17799:2005

Apostila desenvolvida pelo Instituto Online em parceria com a Microsoft Informática

http://www.instonline.com.br/

Revisão 0.9 – Setembro de 2006

AUTORES

Luiz Gonzaga
Fernando Fonseca
Wagner Elias
Renato Opice Blum e Camilla do Vale Jimene

COORDENADORES TÉCNICOS

Fernando Fonseca
Arthur Roberto dos Santos Júnior

COMO USAR ESSE MATERIAL

Este é um material de apoio para o curso “Entendendo e implementando a ABNT NBR ISO/IEC 17799:2005” ministrado pela Academia de Segurança Microsoft. Durante o curso serão apresentados vários Webcasts com o conteúdo deste material acompanhado de slides e voz para ilustrar os conceitos e práticas. A cópia desses slides está em destaque na apostila, seguida de textos com informações que serão abordadas pelo instrutor nos respectivos Webcasts.

ÍNDICE

Capítulo
12

12 – AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO.

POR LUIZ GONZAGA.

NESTE CAPÍTULO APRESENTAREMOS CRITÉRIOS, NORMAS E PRÁTICAS – ALÉM DOS CUIDADOS COM A SEGURANÇA DA INFORMAÇÃO - NECESSÁRIOS ÀS ATIVIDADES DE AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DOS SISTEMAS DE INFORMAÇÃO.

OBJETIVOS

O objetivo deste capítulo é possibilitar que o conhecimento e a adequada compreensão dos critérios, normas e práticas necessários às atividades de aquisição, desenvolvimento e manutenção dos sistemas de informação, aliados à utilização das práticas recomendadas pela indústria e pelos organismos que promovem e divulgam estudos, pesquisas e técnicas ligadas à segurança da informação, possam servir de apoio à realização dessas atividades sem acrescentar riscos ou vulnerabilidades aos sistemas de informação e aos negócios.

Ao final deste capítulo você estará apto a:

- ❒ Avaliar os critérios, normas e práticas aplicáveis aos processos de aquisição, desenvolvimento e manutenção;
- ❒ Estabelecer parâmetros para a tomada de decisão sobre aquisição, desenvolvimento e manutenção de sistemas de informação;
- ❒ Classificar e avaliar fornecedores e produtos de software e sistemas de informação;
- ❒ Validar os objetivos e efetivar os controles da norma NBR ISO/IEC 17799:2005 nos processos de aquisição, desenvolvimento e manutenção de sistemas de informação.

De modo a garantir a segurança da informação.

UMA VISÃO DOS CRITÉRIOS, NORMAS E PRÁTICAS APLICÁVEIS.

Algumas instituições colaboradoras:

- CMM (2)
- MPS.BR (F e G)
- SA-CMM
- CMMI-AM (nível 2)
- ISO/IEC 15504 (Spice)
- CoBit (domínio Aquisição e Implementação)

Normas adicionais:

- ISO/IEC 9126 (estabelece as características de qualidade)
- ISO/IEC 14948 (processo de avaliação de produtos de software)
- ISO/IEC 12119 (requisitos de qualidade e testes de pacotes de software)

As atividades de aquisição, desenvolvimento e manutenção de sistemas estão, de forma intrínseca, ligadas à Segurança da Informação. A Norma NBR ISO/IEC 17799:2005 estabelece objetivos e controles para essas atividades, com o intuito de garantir que a Segurança da Informação seja mantida ou promovida durante todo o processo.

Diversas instituições têm colaborado na produção de normas, regulamentos e guias de melhores práticas aplicáveis a essas atividades, sendo algumas bastante divulgadas, como por exemplo:

- CMM (2)
- MPS. BR (F e G)
- SA-CMM
- CMMI-AM (nível 2)
- ISO/IEC 15504 (Spice)
- CoBit (domínio Aquisição e Implementação)

Além dessas, é bom destacar que há um conjunto adicional que auxilia no estabelecimento de critérios objetivos voltados aos cuidados necessários para a obtenção de bons resultados nesses processos. Nesse aspecto cabe citar as seguintes normas:

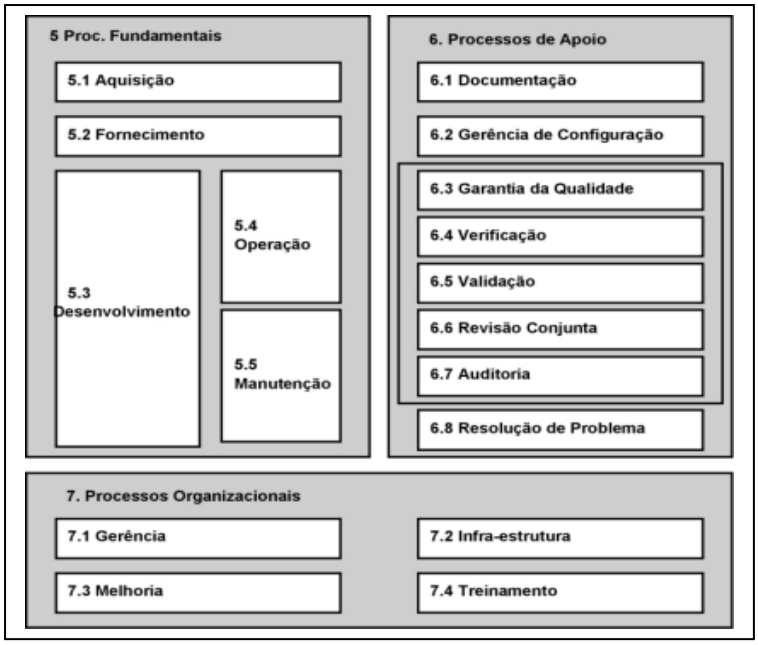
- ISO/IEC 9126 (estabelece as características de qualidade)
- ISO/IEC 14948 (processo de avaliação de produtos de software)
- ISO/IEC 12119 (requisitos de qualidade e testes de pacotes de software)

Todo o conhecimento oferecido por esse vasto material tem como objetivo dar condições para o estabelecimento de critérios objetivos e delineamento do processo de aquisição, desenvolvimento e manutenção de sistemas de informação. Esses critérios, aliados aos objetivos e controles estabelecidos pela Norma ISO/IEC 17799, compõem os mecanismos que possibilitarão o emprego correto de esforço e de recursos da organização no intuito de garantir a Segurança da Informação.

Convém salientar que normas estabelecem prioritariamente 'o quê' deve ser feito, e não 'como'. De posse desses conhecimentos cabe à cada organização, em função de suas características, regular os procedimentos de acordo com a sua política de segurança. O atendimento a legislação também deve ser uma constante preocupação dos responsáveis pela gestão da segurança da informação e pelos processos de aquisição, desenvolvimento e manutenção dos sistemas de informação. Regulamentos legais como a Lei Federal 8.078/1990 (Código de Defesa do Consumidor) e a Lei Federal 8.666/1993 (Lei das Licitações) – para organizações do setor público - são importantes marcos regulatórios e fazem parte do ferramental a ser estudado, utilizado e observado.

Fazer parte e manter constante intercâmbio de informações com órgãos empresariais de classe, tais como a Assespro e a Sucesu, manter e atualizar informações de fornecedores de produtos e serviços, solicitar demonstrações e apresentações, realizar diligências e visitas aos fornecedores e seus clientes também são medidas que fazem parte do arsenal de melhores práticas para os condutores dos processos de aquisição, desenvolvimento e manutenção dos sistemas de informação, como requisito para a garantia da segurança da informação.

A NORMA NBR ISO/IEC 12207



A norma ISO/IEC 12207 classifica o processo de aquisição de software como sendo todas as atividades e tarefas que deverão ser realizadas pela organização para concluir a aquisição. O processo inicia-se com a identificação da necessidade e a opção por adquirir um sistema, cujo desenvolvimento seja totalmente executado pelo fornecedor, pelo fato de adquirir um produto de software – ou pacote – ou contratar serviços, seja de consultoria, análise, desenvolvimento, fábrica de software, instalação, configuração, testes, suporte ou treinamento, entre outros.

A Norma NBR ISO/IEC 12207 - Processos do Ciclo de Vida do Software - tem como principal objetivo fornecer uma estrutura comum para que os agentes (comprador, fornecedor, desenvolvedor, mantenedor, operador, gerentes e técnicos) envolvidos com o desenvolvimento de software utilizem um padrão de linguagem. Este padrão é estabelecido através de processos claramente definidos.

A norma foi estruturada de maneira a ser flexível, modular e adaptável às necessidades dos usuários. Está baseada nos princípios de modularidade e responsabilidade. Essa característica modular é representada pelos processos com mínimo acoplamento e máxima coesão, e a responsabilidade representada pelo estabelecimento de um responsável único por cada processo, possibilitando a aplicação da norma mesmo em projetos nos quais há a necessidade do comprometimento de várias pessoas, inclusive com implicações legais.

Como já citado, a norma é composta por um conjunto de processos, atividades e tarefas que podem ser adaptados de acordo com os projetos de software. Estes processos são classificados em fundamentais, de apoio e organizacionais como mostrados na figura 1. Os processos de apoio e organizacionais devem existir independentemente da organização e do projeto que está sendo executado. Os processos fundamentais são instanciados de acordo com a situação.

PROCESSOS FUNDAMENTAIS

São responsáveis pela geração dos produtos de software, constituindo o ciclo de vida de software propriamente dito. São representados pelos seguintes processos:

a. ***Aquisição***: Define as atividades para a organização que busca a aquisição de um sistema ou produto de software. Este processo Inicia-se com a definição da necessidade de adquirir um sistema, um produto de software ou um serviço de software, passando pela preparação e emissão de pedido de proposta, seleção de fornecedor e gerência do processo de aquisição através da aceitação do sistema, produto de software ou serviço de software.

b. ***Fornecimento***: Define as atividades do fornecedor ou organização que oferta o produto de software. O processo inicia-se na decisão de apresentar uma proposta a um pedido de um cliente ou na assinatura de um contrato para fornecer o sistema, produto de software ou serviço de software. E segue na determinação dos procedimentos e recursos necessários para gerenciar e garantir a execução do projeto, incluindo o desenvolvimento e a execução dos planos de projeto, até a entrega do produto final, se já ele um sistema, produto de software ou serviço de software.

c. ***Desenvolvimento***: Define as atividades do desenvolvedor, ou aquele que define e desenvolve o produto de software. O processo contém as atividades para análise de requisitos, projeto, codificação, integração, testes, instalação e aceitação relacionada aos produtos de software.

d. ***Operação***: Define as atividades do operador, ou seja, aquele que provê serviço de operação de um sistema computacional no seu ambiente de funcionamento para seus usuários. O processo cobre a operação do produto de software e o suporte aos usuários.

e. ***Manutenção***: Define as atividades do responsável pelos serviços de manutenção do software, isto é, gerenciamento de modificações no software para mantê-lo atualizado e em perfeitas condições de operação. Isso ocorre quando o esse produto é submetido a modificações no código e

na documentação associada, quer seja devido a um problema ou à necessidade de melhoria ou adaptação. O objetivo é modificar o produto de existente, preservando a sua integridade.

OS PROCESSOS DE APOIO

São processos que têm como objetivo auxiliar outros processos, objetivando principalmente a qualidade e o sucesso do projeto. São representados por:

a. ***Documentação***: Trata das atividades voltadas ao registro das informações produzidas por um processo ou atividade do ciclo de vida. Contempla o conjunto de atividades que planeja, projeta, desenvolve, produz, edita, distribui e mantém os documentos necessários a todos os envolvidos com o sistema ou produto de software.

b. ***Gerência de Configuração***: Contempla as atividades para a aplicação de procedimentos administrativos e técnicos durante todo o ciclo de vida de software, com o intuito de identificar e definir os itens em um sistema e estabelecer suas linhas básicas, controlar as modificações e liberações dos itens, registrar e apresentar a situação dos itens e dos pedidos de modificação, garantir a adequação, a consistência e a correção, e controlar o armazenamento, a manipulação e a distribuição dos itens.

c. ***Garantia da Qualidade***: Define as atividades para fornecer a garantia adequada de que os processos e produtos de software, no ciclo de vida do projeto, estejam em conformidade com os requisitos especificados e sejam aderentes aos planos estabelecidos. A abrangência do processo inclui questões como garantia de qualidade do produto (NBR 13596 que corresponde à ISO/IEC 9126), do processo e do sistema de qualidade.

d. ***Verificação***: Trata das atividades para verificação dos produtos de software. É um processo para determinar se os produtos de uma atividade atendem completamente aos requisitos ou condições a eles impostas.

e. ***Processo de Validação***: Contempla as atividades para validação dos produtos produzidos pelo projeto de software. É um processo para determinar se os requisitos e o produto final (sistema ou software) atendem ao uso específico proposto.

f. ***Processo de Revisão Conjunta***: Define as atividades para avaliar a situação e produtos de uma atividade em um projeto, se apropriado. As revisões conjuntas são feitas tanto nos níveis de gerenciamento do projeto, como nos níveis técnicos e são executadas durante a vigência do contrato.

g. ***Processo de Auditoria***: Estabelece as atividades para determinar adequação aos requisitos, planos e contrato, quando apropriado.

h. ***Processo de Resolução de Problemas***: Define um processo para analisar e resolver os problemas (incluindo não-conformidades), de qualquer natureza ou fonte, que são descobertos durante a execução do desenvolvimento, operação, manutenção ou outros processos. O objetivo é prover os meios em tempo adequado e de forma responsável e documentada para garantir que todos os problemas encontrados sejam analisados e resolvidos e tendências sejam identificadas.

PROCESSOS ORGANIZACIONAIS

Têm como objetivo garantir e melhorar os processos dentro da organização. São representados pelos:

a. ***Processo de Gerência***: Define as atividades genéricas que podem ser empregadas por quaisquer das partes que têm que gerenciar seu(s) respectivo(s) processo(s). O gerente é responsável pelo gerenciamento de produto, gerenciamento de projeto e gerenciamento de tarefa do(s) processo(s) aplicável (eis), tais como: aquisição, fornecimento, desenvolvimento, operação, manutenção ou processos de apoio.

b. ***Processo de Infra-estrutura***: Define as atividades para estabelecer e manter a infra-estrutura necessária para qualquer outro processo. A infra-estrutura pode incluir hardware, software, ferramentas, técnicas, padrões e recursos para o desenvolvimento, operação ou manutenção.

c. ***Processo de Melhoria***: Define as atividades básicas que uma organização (isto é, adquirente, fornecedor, desenvolvedor, operador, mantenedor, ou o gerente de outro processo) executa para estabelecer, avaliar, medir, controlar e melhorar um processo de ciclo de vida de software.

d. ***Processo de Treinamento***: Define as atividades para prover e manter pessoal treinado. A aquisição, o fornecimento, o desenvolvimento, a operação ou a manutenção de produtos de software são extremamente dependentes de pessoal com conhecimento e qualificação. Portanto, é essencial que o treinamento seja planejado e implementado com antecedência para que o pessoal treinado esteja disponível quando o produto de software for adquirido, fornecido, desenvolvido, operado ou mantido.

A Norma também descreve o Processo de Adaptação que contém as atividades básicas para adaptar a Norma a uma organização ou projeto específico. Uma vez implantada a metodologia, o atendimento aos requisitos de segurança definidos pela política de segurança da organização poderão ser facilmente implementados nesses processos, resultando em maior efetividade.

12.1 – REQUISITOS DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

> Visa garantir que segurança é parte integrante de sistemas de informação, a partir do estabelecimento de mecanismos de controle que enfatizem essa característica no processo de aquisição, desenvolvimento e manutenção dos sistemas de informação..

Uma vez estabelecido um método para a execução, acompanhamento e controle dos processos de aquisição, desenvolvimento e manutenção dos sistemas de informação, é necessário garantir a segurança como parte integrante dos sistemas de informação, desde o primeiro momento do projeto. O objetivo desse item da norma é exatamente esse: garantir que segurança é parte integrante de sistemas de informação, a partir do estabelecimento de mecanismos de controle que enfatizem essa característica no processo de aquisição, desenvolvimento e manutenção dos sistemas de informação.

12.1.1 – ANÁLISE E ESPECIFICAÇÃO DOS REQUISITOS DE SEGURANÇA

Este elemento de controle prioriza a aderência aos requisitos de segurança estabelecidos pela política de segurança da organização, tornando-os parte do processo de análise e especificação. Desse modo, os requisitos para controles de segurança nas especificações de requisitos de negócios devem ser estabelecidos e especificados, em consonância com a política de segurança, quer seja para novos sistemas de informação a serem adquiridos, desenvolvidos, ou para a realização de manutenção ou implementação de melhorias em sistemas já existentes.

É importante que esse elemento de controle esteja plenamente integrado aos processos de desenvolvimento interno ou externo, de forma que não apresente complexidade em sua operacionalização e não comprometa os prazos, custos e objetivos dos sistemas de informação, pois, de outro modo, certamente será deixado em segundo plano em caso de necessidade.

12.2 – PROCESSAMENTO CORRETO NAS APLICAÇÕES

- Visa prevenir:
  - A ocorrência de erros,
  - Perdas de informações
  - Modificação não autorizada ou mal uso de informações em aplicações.
- Através da:
  - Validação dos dados,
  - Controle do processamento interno,
  - Proteção da integridade da mensagem,
  - Validação dos dados de saída.

Os principais objetivos dos requisitos de segurança dos processos de aquisição, desenvolvimento e manutenção dos sistemas de informação deve ser prevenir a ocorrência de erros, perdas, modificação não autorizada ou mal uso de informações em aplicações.

Convém salientar que tais ocorrências representam perdas para o negócio, e boa parte delas expressam vulnerabilidades que expõem a organização a riscos. Um sistema de informações seguro é aquele que reduz o risco, se antecipa às ameaças e, principalmente, evita desvios no objetivo de sua aplicação.

Com esse intuito, devem ser estabelecidos os mecanismos de controle que venham a garantir essa eficácia, a saber:

12.2.1 – VALIDAÇÃO DOS DADOS DE ENTRADA

Este item de controle estabelece que deva ser incorporados elementos de controle cujo objetivo é garantir que os dados de entrada de aplicações estejam corretos e sejam apropriados aos requisitos de negócio e aos requisitos de segurança. Para tanto, esses dados devem ser validados também sob a ótica da política de segurança da organização.

Esses elementos são de fundamental importância para a segurança da informação, pois é sabido que a grande maioria das tragédias tem sua origem em falhas na validação inicial dos dados que possibilitam a inserção de informações que induzem os sistemas de informação a erro, quer seja pelo descuido, pelo desconhecimento ou despreparo, ou mesmo intencionalmente. O uso de

ferramentas de automatização do processo de teste da validação dos dados de entrada e a elaboração e aperfeiçoamento constante de *check lists* é uma prática altamente recomendável.

12.2.2 – CONTROLE DO PROCESSAMENTO INTERNO

É um item de controle que implica no dever de incorporar, nas aplicações, checagens de validação com o objetivo de detectar qualquer corrupção de informações, por erros ou por ações deliberadas.

Falhas no processamento interno das aplicações geralmente implicam em perdas para a organização e, além disso, expõem elementos internos fundamentais para a segurança da informação. Consequentemente representam vulnerabilidades e risco, que devem ser mitigados através desse controle. Se uma aplicação é realmente segura, então o resultado de um processamento interno deve ser conhecido ou esperado, e, portanto, pode ser objeto de validação.

12.2.3 – INTEGRIDADE DE MENSAGENS

Mecanismos de controle precisam ser incorporados ao processo para assegurar que os requisitos de garantia de autenticidade e a proteção da integridade das mensagens das aplicações sejam devidamente implementados.

As mensagens das aplicações são os elementos principais da comunicação com os usuários, e contêm informações importantes para o sistema e para o negócio. Da comunicação eficiente entre o sistema de informações e os usuários deriva boa parte da segurança da informação das organizações. Em função disso, requisitos para garantir a autenticidade e proteger a integridade das mensagens em aplicações devem ser identificados, e os controles apropriados, identificados e implementados.

12.2.4 – VALIDAÇÃO DE DADOS DE SAÍDA

Como dito anteriormente, é característica de uma aplicação segura a previsibilidade do processamento, de tal forma que os dados de saída possam ser validados.

Esse item estabelece a necessidade de um controle, uma vez que os dados de saída das aplicações devem ser validados para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstâncias.

É importante notar que, de maneira muito freqüente, os dados de saída de uma aplicação ou processamento constituir-se-ão dados de entrada para outra aplicação ou processamento, internamente ou no ambiente externo da organização.

12.3 – CONTROLES CRIPTOGRÁFICOS

- Visa proteger a confidencialidade, autenticidade ou a integridade das informações, através de:
  - Política para uso de controles criptográficos,
  - Gerenciamento de chaves

É comum afirmar que a criptografia é um eficiente meio de proteger a confidencialidade, autenticidade ou integridade das informações. Por meios criptográficos os sistemas de informação podem evitar o acesso indevido ou a corrupção dos dados. Esse item enumera os requisitos para o correto e proveitoso uso da criptografia nos sistemas de informação da organização.

12.3.1 – POLÍTICA PARA O USO DE CONTROLES CRIPTOGRÁFICOS

Esse elemento de controle objetiva estabelecer uma política para a aplicação da criptografia nos sistemas de informação.

Deve ser desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção das informações, sua correta classificação e a definição dos meios de acesso e circulação das informações, além da definição do nível de acesso de cada usuário às informações classificadas.

12.3.2 – GERENCIAMENTO DE CHAVES

Elementos fundamentais para a segurança da informação, o gerenciamento das chaves criptográficas merece especial cuidado e atenção.

Esse mecanismo de controle tem por objetivo a definição e implementação de um processo de gerenciamento de chaves para apoiar o uso de técnicas criptográficas pela organização.

Especial atenção deve ser dada à armazenagem, custódia e manuseio das chaves, com a responsabilização formal e plenamente consciente de todos os que participarem desses processos.

12.4 – SEGURANÇA DOS ARQUIVOS DO SISTEMA

- Visa controlar os acessos aos arquivos e aos programas de código-fonte através de:
  - Controle de software operacional,
  - Proteção dos dados de teste de sistema,
  - Controle de acesso ao código-fonte de programa.

Os arquivos do sistema sejam bibliotecas, rotinas ou arquivos de configuração, são alvos prediletos dos ataques intencionais. Além disso, são também cruciais para garantir a disponibilidade das informações e o correto funcionamento dos sistemas de informação. Um item elementar para a segurança das informações é a garantia da segurança de arquivos de sistema, através dos controles enumerados a seguir:

12.4.1 – CONTROLE DE SOFTWARE OPERACIONAL

Um item de controle de fundamental importância é a definição de procedimentos para controlar a instalação de software em sistemas operacionais.

O alto grau de dependência entre os sistemas de informação e os sistemas operacionais, aliado ao fato de estes terem seu funcionamento e funcionalidades amplamente divulgados e estudados, representam um elevado grau de risco.

Vulnerabilidades recém descobertas de sistemas operacionais, e falhas extremamente simples de configuração de sistemas de informação em ambientes de sistemas operacionais conhecidos são os alvos preferidos de ataques maliciosos, e representam um expressivo contingente de problemas de segurança da informação.

Políticas de segurança que contemplem procedimentos relativamente simples de serem implementados e seguidos, porém compactos e consistentes - no que tange à instalação de sistemas e controle do ambiente operacional - são um

diferencial para o sucesso da garantia da segurança da informação em sistemas de informação.

12.4.2 – PROTEÇÃO DOS DADOS PARA TESTE DE SISTEMA

Importante mecanismo de controle é o que deve ser implementado visando à segurança e a confiabilidade dos dados a serem utilizados para testes dos sistemas de informação e sistemas operacionais.

Uma vez que tais dados devem refletir ao máximo possível o ambiente real de operação dos sistemas – e, na maioria das vezes são obtidos desse ambiente - esses dados de teste devem ser selecionados com cuidado, protegidos durante seu manuseio, obedecendo aos mesmos requisitos de segurança dos dados do ambiente de produção, e o acesso a eles controlado.

Fundamental importância deve ser dada também ao descarte dos resultados dos testes, principalmente no caso de geração de mídias ou documentos impressos.

12.4.3 – CONTROLE DE ACESSO AO CÓDIGO-FONTE DE PROGRAMA

Um controle crucial e polêmico é o que deve ser estabelecido quanto ao acesso ao código-fonte dos sistemas de informação.

Por definição, o acesso ao código-fonte deve ser restrito. O acesso, manuseio e o armazenamento desses devem estar submetidos a um rígido controle, e devem ser objeto de destaque na elaboração dos requisitos de segurança. Preferencialmente, deve ser evitado ou limitado o acesso ao conjunto dos códigos-fonte, o qual deverá ocorrer apenas no momento de geração das versões executáveis para teste e entrega, em ambiente especificamente preparado para isso e, evidentemente, seguro. O uso de produtos de controle de acesso e de versão é altamente recomendável, chegando mesmo a ser essencial.

Cópias de segurança requerem tratamento especial, que deve ser claramente definido nos requisitos de segurança e na política de segurança da organização. Deve ser evitada a utilização de mídias removíveis, e o transporte, se realmente necessário, deve fazer uso da criptografia. Uma boa e salutar prática também é o apagamento seguro dos arquivos dos códigos-fonte, quando houver a necessidade da utilização destes em ambientes distintos.

12.5 – SEGURANÇA EM PROCESSOS DE DESENVOLVIMENTO E DE SUPORTE

- Visa manter a segurança de sistemas aplicativos e da informação, através:
  - Procedimentos para controle de mudanças,
  - Análise crítica técnica das aplicações após mudanças no sistema operacional,
  - Restrições sobre mudanças em pacotes de software,
  - Ações preventivas contra vazamento de informações,
  - Supervisão e monitoramento de desenvolvimento terceirizado de software.

Os processos de desenvolvimento e suporte a sistemas de informação trazem em si grande quantidade de riscos em potencial.

Seja por falhas ou por ações intencionais, grande parte das vulnerabilidades é decorrência dessas etapas ou atividades. O objetivo dos controles preconizados nesse item é manter a segurança de sistemas aplicativos e da informação durante o processo de desenvolvimento e as atividades de suporte à operação dos sistemas de informação.

12.5.1 – PROCEDIMENTOS PARA CONTROLE DE MUDANÇAS

Esse mecanismo de controle estabelece que a implementação de mudanças deva ser monitorado utilizando procedimentos formais de controle de mudanças.

Uma boa referência para a implementação desses mecanismos é o que estabelece o PMBOK do PMI, no item 4.6 – Controle Integrado de Mudanças. Especial atenção deve ser dada aos impactos das mudanças propostas em todos os aspectos do negócio e da segurança da informação. Ações preventivas e corretivas devem ser estabelecidas, e o tratamento da comunicação das mudanças requer planejamento e apoio, o que implica em comprometimento.

12.5.2 – ANÁLISE CRÍTICA TÉCNICA DAS APLICAÇÕES APÓS MUDANÇAS NO SISTEMA OPERACIONAL

O objetivo desse mecanismo de controle é possibilitar que aplicações críticas de negócios sejam analisadas e testadas quando houver alterações nos sistemas

operacionais, para garantir que não haverá nenhum impacto adverso nas operações da organização ou na segurança das informações causada por falhas nos sistemas de informação.

Um tópico pertinente a esse controle que deve ser objeto constante de monitoramento e aprimoramento é a aplicação de *patches* de correção, cujo procedimento deve ser cuidadosamente planejado e exaustivamente testado, preferencialmente com o apoio dos fornecedores.

12.5.3 – RESTRIÇÕES SOBRE MUDANÇAS EM PACOTES DE SOFTWARE

O controle proposto por esse item estabelece a expressa limitação de modificações em pacotes de software. Mudanças não devem ser incentivadas e devem ser limitadas àquelas estritamente necessárias.

Todas as mudanças devem ser estritamente controladas por procedimentos formais definidos pelo controle de mudanças mencionado no item 12.5.1, e o impacto dessas mudanças deve ser calculado, planejado e deve servir de base para a preparação de ações preventivas e corretivas, de forma que não coloquem em risco a segurança da informação durante a sua operacionalização.

12.5.4 – VAZAMENTO DE INFORMAÇÕES

A identificação de oportunidades para o vazamento de informações é o objetivo desse controle. Sua implementação destina-se também à prevenção do vazamento de informações e também deve planejar e estabelecer medidas de contenção e ações preventivas e corretivas no caso de ocorrências dessa natureza.

O acesso a informações classificadas deve ser planejado de forma a, primeiramente, inibir o vazamento ou acesso indevido a essas informações. E, caso esse vazamento venha a ocorrer, deve prover mecanismos de identificação e responsabilização, também como forma de inibição. A utilização de termos de sigilo e confidencialidade é uma opção bastante eficaz a ser considerada, aliada aos já tradicionais dispositivos de tecnologia baseados em software e hardware.

12.5.5 – DESENVOLVIMENTO TERCEIRIZADO DE SOFTWARE

Este item de controle estabelece que a organização deva supervisionar e monitorar o desenvolvimento terceirizado de software.

Item essencial à segurança da informação, o desenvolvimento terceirizado deve ser tratado com especial atenção. Parceiros comerciais comprometidos no desenvolvimento de sistemas de informações seguro devem submeter-se às mesmas políticas de segurança da informação. Termos de sigilo e confidencialidade devem ter itens comuns de co-responsabilização, e a atuação dos terceiros avalizadas por órgãos da classe empresarial também é fundamental.

Os já mencionados aspectos de seleção dos fornecedores e parceiros, as normas e recomendações aplicáveis, a previsão de inspeções periódicas e a divulgação das políticas de segurança aliada à exigência do estrito cumprimento são fatores de sucesso no relacionamento com terceiros e na garantia do desenvolvimento de software seguro.

Dada à complexidade da gestão do desenvolvimento terceirizado de software, apresentamos alguns itens de atenção e recomendações resumidas das melhores práticas a serem adotadas e exigidas dos colaboradores e parceiros:

Cuidados no desenvolvimento:

- Criar e usar funções intrinsecamente seguras;
- Sempre testar o retorno das funções chamadas;
- Documentar corretamente as funções (entrada, processamento e saída);
- Verificar o tratamento de caracteres especiais;
- Manter uma política de versão consistente;
- Só usar componentes e bibliotecas confiáveis;
- Evitar manter informações sensíveis em arquivos temporários;
- Não colocar senhas e chaves de criptografia no código;
- Tratar todas as entradas como não confiáveis;
- Exercer rígido controle de versão e acesso a código-fonte;
- Geração de código executável em ambiente específico e controlado;
- Controle da distribuição e instalação de código executável;
- Ter em mente que a redução dos erros nos sistemas de informação significa a redução de riscos e de vulnerabilidades.

Cuidados com as equipes:

- Educação, informação e formação contínua são essenciais no processo de desenvolvimento;
- Lembrar que o desconhecido sempre representa risco;
- Duvidar sempre, por princípio, não somente por hábito;
- Outros podem conhecer as falhas do software;
- Novos profissionais chegam ao mercado sem o treinamento e a experiência em escrever - e testar - código seguro;

- Profissionais experientes podem estar desinformados dos ataques e ameaças mais recentes, uma vez que geralmente estão mais envolvidos com as demandas diárias;
- Excesso de confiança representa um maior risco;
- Funcionários, fornecedores e terceiros:
    - Se você contratar, confie. Se não pode confiar, não contrate!
    - Contratos e termos de sigilo e confidencialidade realmente funcionam como inibidores;
    - Consciência das ameaças e preocupações ajudam na prevenção e contenção dos riscos e redução das vulnerabilidades;
- Conhecimento e apoio à política de segurança;
- Substituir a abordagem "policial" por uma abordagem colaborativa, através do conhecimento e apoio à política de segurança, do respeito mútuo e do comprometimento de todos os membros das equipes e da organização.

Cuidados com o treinamento:

- Estabelecer e cumprir um treinamento obrigatório de segurança para toda a equipe do projeto;
- Atualização constante (pelo menos uma reciclagem anual);
- Treinamento básico comum, e avançado específico por função:
    - Para a Gerência do Projeto;
    - Para a equipe de desenvolvimento;
    - Para a equipe de testes;
    - Para a equipe de suporte;
- Treinamento interno ou externo baseado no tamanho da organização;
- Definir métricas de treinamento:
    - Quantidade e % da equipe treinada por período;
    - Conscientização e educação contínua;

Cuidados com a propriedade intelectual e com o direito autoral:

- Conhecer e divulgar a legislação pertinente: Leis Federais № 9.609/1998 e 9.610/1998;
- Providenciar o registro no órgão competente (INPI);
- O contrato deve ser expressamente claro nesses aspectos.

12.6 – GESTÃO DE VULNERABILIDADES TÉCNICAS

- Visa reduzir os riscos decorrentes da exploração de vulnerabilidades técnicas conhecidas. Para isso:
  - Obtenha informações sobre vulnerabilidades técnicas dos sistemas de informação,
  - Avalie a exposição da organização a estas vulnerabilidades,
  - Tome medidas apropriadas para lidar com os riscos associados.

Grande parte dos atos de violação da segurança da informação advém da exploração de vulnerabilidades conhecidas. Em função disso, o objetivo da gestão de vulnerabilidades é exatamente reduzir os riscos resultantes da exploração dessas vulnerabilidades técnicas.

12.6.1 – CONTROLE DE VULNERABILIDADES TÉCNICAS

Esse mecanismo de controle deve ser estabelecido com o intuito de se obter informação suficiente e em tempo hábil sobre vulnerabilidades técnicas dos sistemas de informação em uso, para que seja avaliada a exposição da organização a estas vulnerabilidades, e tomadas às medidas apropriadas para lidar com os riscos associados.

Com a velocidade da circulação da informação na atualidade, esse controle deve ser planejado para utilizar todos os meios disponíveis, incluindo a comunicação pessoal móvel, de modo a permitir que ações preventivas e corretivas sejam adotadas antes que as vulnerabilidades técnicas possam ser exploradas ou, em não sendo possível, que se possa fazer uma análise aprofundada dos riscos aos quais a organização estará sujeita.

CONCLUSÃO.

Os processos de aquisição, desenvolvimento e manutenção dos sistemas de informação são fundamentais para a preservação da segurança da informação nas organizações.

Devido à sua complexidade inerente, e do envolvimento de grande parte das organizações em todo o processo, é necessário um contínuo aprimoramento dos métodos para adequá-los às necessidades de cada organização e torná-los cada vez mais eficaz.

Nesse tópico abordamos o capítulo específico da norma ISO/IEC 17799 destinada à de aquisição, desenvolvimento e manutenção dos sistemas de informação, agregando informações de outras fontes aliadas às melhores práticas, no intuito de fornecer as bases para a implementação dessas recomendações como forma de garantia da segurança da informação.

Capitulo
13

13 – GESTÃO DE INCIDENTES DE SEGURANÇA DA **INFORMAÇÃO.**

POR: FERNANDO FONSECA

TRATAREMOS NESTE CAPÍTULO SOBRE AS AÇÕES QUE DEVEM SER TOMADAS EM CASO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO.

OBJETIVOS

O objetivo deste capítulo é alertar para as medidas que devem ser tomadas em caso de incidentes de segurança da informação, bem como na detecção de possíveis fragilidades do sistema.

Ao final deste capítulo você estará apto a:

- ❒ Saber quais os procedimentos adequados a serem criados, para que ações rápidas possam ser desencadeadas em caso de incidentes de segurança;
- ❒ Saber da importância da notificação de eventos de segurança;
- ❒ Entender a necessidade da coleta e manutenção de evidências de eventos de segurança da informação.

13.1 - GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

- Visa a que fragilidades e eventos de segurança da informação sejam comunicados permitindo tomadas de decisões. Obtido através de:
  - Processos de notificação de eventos de segurança da informação;
  - Notificação de fragilidades de segurança da informação.

Para que um sistema de gestão seja bem sucedido, é importante que se institucionalizem alguns aspectos básicos do comportamento organizacional e também que nos certifiquemos que o mesmo possua uma série de decisões rápidas previamente definidas, evitando um dispendioso atraso na tomada de decisões.

Algumas das comunicações mais importantes dizem respeito à notificação de incidentes de segurança da informação. Deve existir um caminho fácil e bem documentado a ser seguido por todos os funcionários, fornecedores e terceiros que possam vir a identificar um evento como este.

13.1.1 NOTIFICAÇÃO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO

Quando uma violação da política de segurança ocorre, este é sem dúvida o momento em que a empresa mais necessita de uma seqüência de ações precisa e inequívoca. Para que isso aconteça, todos devem conhecer um ponto de contato sempre disponível para as notificações destes eventos. Um processo formal de notificação assegura que uma resposta rápida ao incidente seja iniciada e que o procedimento adequando de escalonamento seja utilizado.

Para que se obtenha uma ação eficiente dos colaboradores da organização, é necessário que todos saibam identificar um incidente de segurança da informação e que conheçam sua responsabilidade de notificá-los. Para o sucesso deste processo, são recomendados alguns passos importantes:

a) A criação de um formulário interno (eletrônico ou não) no qual o colaborador possa relatar o incidente sem se esquecer de nenhum detalhe importante;
b) A documentação e treinamento dos colaboradores quanto ao comportamento correto a ser tomado no momento do incidente. Esta documentação inclui itens como:
    - Anotar minuciosamente todos os detalhes, por mais que não pareçam importantes;
    - Informar o fato imediatamente ao posto de contato sem tomar nenhuma atitude própria;
    - Não tomar nenhuma atitude que modifique o status do computador (desligar, fechar o programa, etc.);
c) Criar um processo disciplinar que fortaleça a política de segurança, estabelecendo penalidades para os colaboradores que cometerem violações à política de segurança. Para que a política de segurança não caia em descrédito, é necessário que a alta administração se comprometa a apoiar as ações disciplinares, sem concessões ou exceções.

Quando se fala em incidente de segurança, logo se pensa em uma invasão. Mas temos que manter em mente que um incidente de segurança é qualquer coisa que viole a política de segurança da empresa, o que geralmente significa algo que prejudique a integridade, disponibilidade e a confidencialidade dos dados. Alguns exemplos de eventos e segurança da informação são:

- Mau funcionamento de um sistema;
- Erros humanos;
- Violação da segurança física do ambiente;
- Mau funcionamento de um hardware (servidor, roteador, switch, etc.);
- Presença de vírus em um computador.

Um simples mau funcionamento de um sistema pode ser conseqüência de uma invasão do equipamento, de um ataque de vírus ou de uma falha iminente de hardware. Por este motivo é recomendado que se notifiquem todas as anomalias detectadas no ambiente para que elas possam ser avaliadas por um profissional e identificadas.

13.1.2 – NOTIFICANDO FRAGILIDADES DE SEGURANÇA DA INFORMAÇÃO

Melhor do que notificar um vento de segurança da informação é notificar uma fragilidade que possa gerar este evento. Muitas vezes as pessoas envolvidas nos processos têm uma visão de uma fragilidade que não é de conhecimento da área responsável. Deve-se procurar estimular os colaboradores para que auxiliem com a melhoria do processo e da segurança final do ambiente.

13.2 – GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E MELHORIAS

- Defina responsabilidades da gestão de eventos de segurança da informação;
- Crie procedimentos de monitoramento de sistemas e alertas;
- Cuide da manutenção das evidências do evento de segurança da informação;
- Quantifique e monitore os custos e quantidades dos incidentes de segurança da informação;
- Colete, armazene e apresente evidências.

Uma vez detectado um incidente de segurança da informação, é necessário que se estabeleça um processo de reavaliação das contramedidas aplicadas e dos processos de identificação de eventos de segurança.

Outro ponto importante do processo é a apropriada manutenção das evidências do evento. Neste ponto recorremos a uma técnica de perícia forense denominada "Cadeia de custódia". O termo perícia forense diz respeito à análise das evidências para serem utilizadas em um processo judicial. Já a cadeia de custódia consiste na seqüência de ações que visa proteger as evidências da mesma forma que foram encontradas, utilizando métodos formais desde a coleta de evidências até a apresentação na corte.

13.2.1 – RESPONSABILIDADE E PROCEDIMENTOS

Para que se tenha uma resposta rápida a eventos, faz-se necessário que se identifique o responsável por cada ação a ser tomada durante um incidente, assim como os procedimentos adequados.

Em um primeiro momento é necessário que se tenham procedimentos de detecção e reação a eventos como:

- Perda de disponibilidade de serviços de informação;
- Uso impróprio de sistemas;
- Negação de serviço;
- Infecção por códigos maliciosos;

- Invasão em sistemas de informação;
- Falha de disponibilidade de dados.

Além da reação ao evento em si e a garantia da continuidade da operação, faz-se necessário que estes procedimentos contenham ações que garantam o correto diagnóstico da causa do evento e a geração de informações importantes para eventuais melhorias nos sistemas de informação existentes. Algumas dessas ações devem visar:

- Identificação da causa do incidente;
- Comunicação com os colaboradores afetados pelo evento;
- Notificação do ocorrido à autoridade apropriada quando necessário;
- Geração de dados para planejamento de ação corretiva na vulnerabilidade responsável pelo acontecimento do evento.

Outra ação importantíssima para o processo de detecção de fragilidades e adoção de contramedidas é a apropriada configuração do sistema para que sejam criadas trilhas de auditoria, que possam ser coletadas, copiadas, protegidas e analisadas para a melhor compreensão dos eventos. Estes registros e eventos serão de extrema utilidade para análise de problemas internos, uso forense e negociações de ressarcimento e compensação por perdas.

Neste ponto, torna-se evidente a importância de um procedimento bem estabelecido de controle de “logs” dentro de qualquer organização. Para se obter as informações necessárias sobre um evento, deve-se considerar desde a correta configuração de coleta de dados até a forma de backup dos registros para consultas futuras.

Uma vez que o incidente está ocorrendo, é necessário que se tomem determinados cuidados para que as ações de recuperação do sistema sejam cuidadosamente controladas, evitando que um dano maior ocorra, ou que as evidências dos eventos sejam destruídas no processo de restabelecimento do ambiente. Uma ação importante para o sucesso deste processo é cuidar para que todas as ações de recuperação sejam documentadas detalhadamente. Isso permitirá que se possa avaliar o impacto das mesmas no estado das evidências, a fim de que se identifique um possível problema criado pelo próprio procedimento de recuperação e finalmente para que a análise do evento contribua para o aperfeiçoamento do processo como um todo.

13.2.2 – APRENDENDO COM OS INCIDENTES DE SEGURANÇA

Uma das máximas do gerenciamento é a que “só se controla o que se mede”. Desta forma, com os incidentes de segurança não poderia ser diferente. O registro adequando dos incidentes é valiosa fonte de informação para que se possa avaliar recursividade de determinados eventos e a necessidade de se implantar controles adicionais para determinados sistemas.

Um histórico bem documentado pode servir para verificar falhas no processo, nas ferramentas e até mesmo justificar um investimento maior em um controle específico devido a um alto número de incidentes de mesma natureza.

13.2.3 – COLETA DE EVIDÊNCIAS

Para que se possa demonstrar que determinado fato realmente ocorreu em um ambiente informatizado, é necessário que se respeite a devida seqüência de proteção destas provas, garantindo que as mesmas cheguem ao seu destino sem a contaminação por parte de pessoas envolvidas no processo. Na hipótese em que o caso pode ir à corte, é necessário que se estabeleça uma cadeia de custódia que garanta que a evidencia seja aceitável, de acordo com a legislação local em vigor.

Para garantir que determinada vidência seja aceita em juízo, as empresas devem se certificar que seus sistemas estão de acordo com a norma ou código de prática vigente para coleta de evidência admissível.

Existem vários aspectos relevantes à manutenção da cadeia de custódia que devem ser analisados antes de agir em um ambiente atacado, ou melhor, dizendo “na cena do crime”. Alguns destes procedimentos são:

- Assegurar-se que a empresa está coletando as provas de maneira legal;
- Estabelecer um processo de coleta de evidências em memória volátil;
- Nunca se trabalhar diretamente na evidência, uma cópia fiel da evidência deve ser tirada para que possa ser utilizada para localização de dados relevantes;
- Proteger a integridade da evidência com transporte e armazenamento adequado;
- Proteger a credibilidade da evidência lacrando-a e sempre sendo acessada por dois ou mais elementos simultaneamente.

Como última consideração, vemos que as evidências nem sempre estão restritas a nossa empresa ou país. Nestes casos torna-se mais complexa a obtenção de evidências, tomando-se o cuidado necessário para que não se tome nenhuma atitude que as tornem inaceitáveis perante a corte.

Capítulo

14

14 – GESTÃO DE CONTINUIDADE DE NEGÓCIOS

.

POR: WAGNER ELIAS

TRATAREMOS NESSE CAPÍTULO A GESTÃO DE CONTINUIDADE DE NEGÓCIOS. O QUE É UM PLANO DE CONTINUIDADE DE NEGÓCIOS? QUAIS AS EQUIPES ENVOLVIDAS? E SUA RELAÇÃO COM A NBR ISO/IEC 17799.

OBJETIVOS

Este capítulo aborda a gestão de continuidade de negócios. Ao final deste capítulo você estará apto a:

- Elaborar um plano de continuidade de negócios;
- Realizar manutenção em um plano de continuidade de negócios;
- Testar um plano de continuidade de negócios.

14.1 – ASPECTOS DA GESTÃO DA CONTINUIDADE DE NEGÓCIOS, RELATIVOS À SEGURANÇA DA INFORMAÇÃO

- Motivador:

  "Não permitir interrupções das atividades do negócio e proteger os processos críticos contra falhas ou desatres, assegurando a retomada em tempo hábil".

Um plano de continuidade de negócios compreende uma série de atividades desenvolvidas para suportar o negócio em uma situação adversa, situação em que, os ativos que suportam os processos de negócio não estejam disponíveis ou aptos a sustentar o negócio.

Devemos considerar ativos de todos os tipos:

- TECNOLOGIA DA INFORMAÇÃO
  - Servidores;
  - Sistema operacional;
  - Software básico;
  - Software aplicativo;
  - Controladoras de discos;
  - Impressoras corporativas;
  - Rede Lan e Wan.

- NÃO TI
  - Catracas, controles de acesso;
  - Equipamentos de escritório;
  - Máquinas industriais;
  - Antenas e estações de transmissão;
  - Central telefônica, etc.

- INFRA-ESTRUTURA
  - No-break;
  - Geradores;

- Ar condicionado;
- Transportes;
- Abastecimentos (óleo, gás, etc.).

- PROVEDORES E PARCEIROS
  - Provedores de telefonia;
  - Suporte às redes e infra-estrutura;
  - Serviços de comunicação;
  - Serviços de entrega, guarda e manuseio;
  - Suporte técnico e manutenção geral.

- RECURSOS HUMANOS
  - Funcionários;
  - Consultores;
  - Sub-contratados.

Equipes definidas no Plano de Continuidade de Negócios

Para facilitar a execução dos planos é definido um Comitê de Continuidade de Negócios que entre outras atribuições terá que definir as equipes que estarão envolvidas na execução do Plano de Continuidade de Negócio.

Segue um modelo de equipes e suas responsabilidades:

Equipe Executiva: garantir que a restauração do processamento ocorra dentro do prazo estipulado no Plano de Contingência conforme criticidade de cada sistema;

Hardware e Software: identificar o hardware mínimo necessário para processamento dos sistemas muito críticos e críticos. Garantir a disponibilidade do software básico e de apoio necessários à operacionalidade;

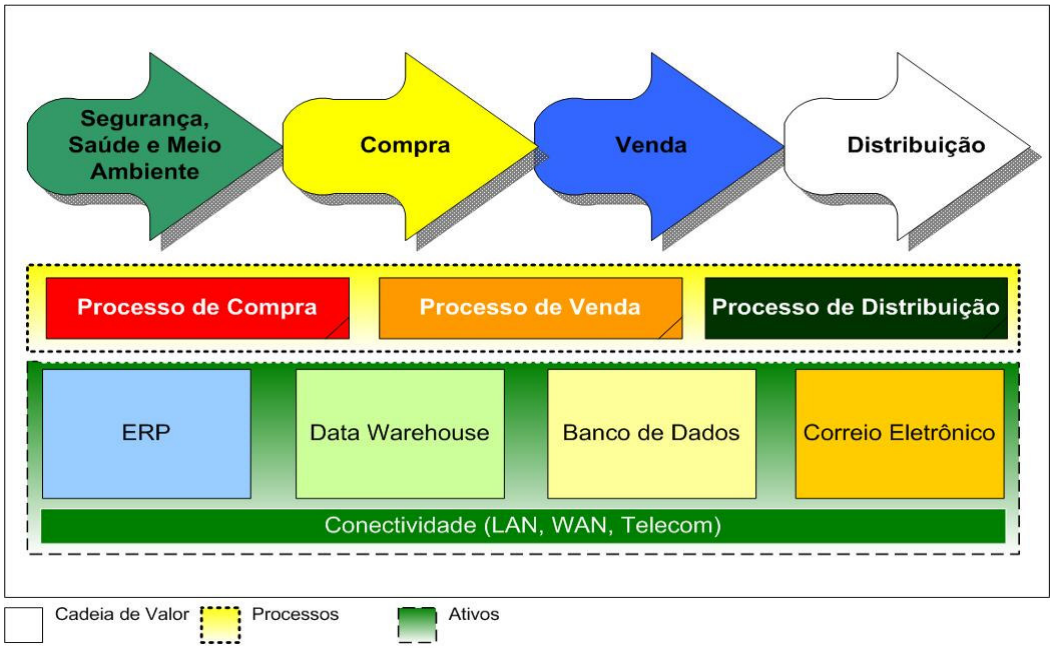
Salvamento e Rescaldo: combater o sinistro, prestar os primeiros socorros, salvar o que puder ser salvo, avaliar a extensão dos danos às instalações, equipamentos e recursos humanos. Prover a EQUIPE EXECUTIVA de informações;

Logística: assegurar a disponibilidade de recursos necessários, de serviços administrativos e de comunicações para as demais equipes, imediatamente após a ocorrência do desastre e da decisão de ativar o Plano;

Comunicação: garantir que as vias de comunicação entre as equipes estão disponíveis.

Plano de Continuidade de Negócios e a Cadeia de Valor

Para desenvolver um Plano de Continuidade de Negócio efetivo, é necessário mapear a cadeia de valor do negócio. O mapeamento da cadeia de valores é feito entendo os processos que suportam o negócio, as interdependências entre eles e conseqüentemente os ativos que suportam os processos.



14.1.1 – INCLUINDO SEGURANÇA DA INFORMAÇÃO NO PROCESSO DE GESTÃO DA CONTINUIDADE DE NEGÓCIO.

O processo de Gestão da Continuidade de Negócios deve ser referenciado na parte que trata de disponibilidade das informações na política de segurança da empresa.

Na política de segurança da informação será endereçado a Norma de Continuidade de Negócios, norma que dentre outras informações, irá descrever principalmente: quais as responsabilidades da equipe de continuidade de negócios, riscos aceitáveis pela empresa e definir o que será considerado um incidente para o comitê de continuidade de negócios.

O comitê de continuidade de negócios deverá ser instituído no início das atividades de elaboração da avaliação de riscos e da elaboração dos planos. Ele será constituído por profissionais com habilidades distintas e complementares,

alguns dos profissionais são:

- Especialistas jurídicos;
- Especialistas em marketing e comunicação;
- Especialistas em Tecnologia;
- Especialistas em Segurança da Informação e Patrimonial; e
- Principais Stakeholders.

14.1.2 – CONTINUIDADE DE NEGÓCIOS E ANÁLISE/AVALIAÇÃO DE RISCOS.

A primeira etapa de elaboração de um Plano de Continuidade dos Negócios após a fase inicial que se resume a planejamento e gestão de projetos, é a fase de avaliação de riscos e Análise de Impactos no Negócio (*BIA – Business Impact Analysis*).

Essa fase do projeto tem como objetivo levantar as ameaças a que o negócio está exposto; uma inspeção física é realizada nos *sites* onde há processamento de dados ou operação de processos considerados críticos para o negócio, essa inspeção física busca controles de segurança física nas instalações.

De posse dessa análise, e através de entrevistas com pessoas envolvidas com a manutenção e operação das instalações é possível fazer uma análise de risco que será base para implementação de controles que mitigam esses riscos e análise de uma possível estratégia de contingência.

Já a Análise de Impactos nos Negócios é feita buscando identificar os processos críticos que suportam a cadeia de valor, e qual impacto para o negócio caso as ameaças mapeadas venham a se concretizar.

O Comitê de Continuidade de Negócios junto com os especialistas envolvidos irá definir qual o impacto que determinado risco irá causar ao negócio caso seja concretizado. Por se tratar de uma análise quantitativa os pesos devem ser lançados usando classificações que identifiquem o nível de impacto.

Exemplo de classificação de impactos:

1. Muito Baixo;
2. Baixo;
3. Médio;
4. Alto;
5. Muito Alto.

Exemplo de impactos ao negócio:

- Abalo na Imagem da Empresa;
- Alteração na Quantidade de pessoal necessário a operação do processo;
- Aumento nos custos operacionais;
- Comprometimento em Negócios Futuros;
- Dano à integridade física de funcionários / clientes / outras pessoas;
- Exposição negativa na mídia;
- Aumento no Fluxo de Trabalho;
- Financeiro (perdas derivadas de natureza diversa);
- Multas e/ou sanções de qualquer natureza;
- Não atendimento de normativas e determinações Legais (ANEEL, ANATEL, ANP, BACEN);
- Parada no Negócio da Empresa;
- Perda da capacidade de gestão e controle;
- Perda de Ativos (recriando registros e Transações);
- Perda de Confiança dos Clientes Patrocinadores;
- Perda de mercado;
- Perda ou diminuição de Receita;
- Perda de vantagem competitiva;
- Processos legais decorrentes da paralisação;
- Quebra de cláusulas contratuais;
- Redução do lucro;
- Saúde, Segurança e Meio Ambiente;
- Sindicais;
- Suspensão do serviço para o cliente (interno);
- Suspensão do serviço para o cliente (externo).

14.1.3 – DESENVOLVIMENTO E IMPLEMENTAÇÃO DE PLANOS DE CONTINUIDADE RELATIVOS À SEGURANÇA DA INFORMAÇÃO.

TIPOS DE PLANOS QUE COMPÕEM UM PLANO DE CONTINUIDADE DOS NEGÓCIOS

- *Business Continuity Plan:* fornece procedimentos para suprir as necessidades operacionais dos processos críticos priorizados pela Análise de Impactos no Negócio;
- *Business Recovery (or Resumption) Plan (BRP):* fornece procedimentos para recuperação dos ativos não TI;
- *Continuity of Operations Plan (COOP):* fornece estratégias para gestão de crise e restabelecimento do negócio;
- *Continuity of Support Plan/IT Contingency Plan:* fornece procedimentos para sustentar os sistemas críticos em contingência;

- *Crisis Communications Plan:* fornece procedimentos para acionamento e comunicação em situação de crise;
- *Disaster Recovery Plan (DRP):* fornece procedimentos para recuperação dos ativos não TI;
- *Occupant Emergency Plan (OEP):* fornecer procedimentos coordenados minimizando a perda de vida ou de ferimento de pessoas.

Os planos que compõem o plano de continuidade são elaborados através de metodologia que se baseia em entrevistas e coleta de informações na empresa.

Através de entrevistas de tecnologia é possível identificar cenários de falhas e estudar os procedimentos para restabelecer ativos de tecnologia ou executar procedimentos de contingência. Entrevistas específicas levantam informações para elaborar procedimentos para operação em situação de crise em ativos não TI.

14.1.4 – ESTRUTURA DO PLANO DE CONTINUIDADE DE NEGÓCIO.

Atualmente existe uma série de entidades e grupos apoiando o estudo sobre Continuidade de Negócios. Entre esses grupos os principais são: DRII – (Disaster Recovery Institute International) e BCI – (Business Continuity Institute).

O DRII situado nos Estados Unidos divide as atividades de desenvolvimento de um Plano de Continuidade em 10 fases, que o mesmo intitula de “Dez práticas profissionais”:

1. Project Initiation and Management;
2. Risk Evaluation and Control;
3. Business Impact Analysis;
4. Developing Business Continuity Strategies;
5. Emergency Response and Operations;
6. Developing and Implementing Business Continuity Plans;
7. Awareness and Training Programs;
8. Maintaining and Exercising Business Continuity Plans;
9. Crisis Communications;Coordination With External Agencies.

O BCI com forte atuação na Europa divide as atividades em cinco fases intituladas como:

1. Understanding Your Business;
2. Business Continuity Management Strategies;
3. Develop and Implement a Business Continuity Management Response;
4. Building and Embedding a Business Continuity Management Culture;
5. Exercising, Maintenance and Audit.

14.1.5 – TESTES, MANUTENÇÃO E REAVALIAÇÃO DOS PLANOS DE CONTINUIDADE DE NEGÓCIO.

Uma das atividades mais importantes da gestão de continuidade de negócios são os testes, através de testes é possível mensurar e identificar a real eficácia do plano de continuidade de negócios.

Os testes e simulações também possibilitam uma manutenção e atualização adequada dos planos.

Os planos de continuidade de negócios devem estar alinhados com o negócio e prover suporte para continuidade da empresa em situações adversas. Para isso os planos devem estar atualizados e eficientes, os planos se manterão atualizados quando existir um procedimento que associe o plano aos processos de gestão de incidente, configuração e mudanças e através de testes constantes.

Os testes devem ter uma periodicidade mínima de seis meses, buscando desvios ou procedimentos ineficientes no plano. Durante esse período podem acontecer mudanças significativas que deverão ser analisadas nos processos de gestão de incidentes, configuração e mudanças. Caso seja identificada alguma mudança que torne o plano ineficiente a mesma deve ser submetida a uma avaliação e atualização.

Para um teste efetivo é necessário estabelecer um cenário de teste e definir qual tipo de teste será possível realizar e qual irá fornecer as evidências necessárias para uma auditoria.

Dentre os tipos de testes destacam os seguintes:

- *Structured Walkthrough*: o tipo o mais básico de teste, ocorre em uma

reunião onde a finalidade principal é assegurar que o pessoal crítico de todas as áreas está familiarizado com o BCP.

- *Tabletop*: é definido um cenário específico e executados os planos. Os objetivos principais são praticar a interação da equipe, as tomadas de decisão e habilidades para resolver o problema:
    - *Functional Testing*: é realizado para testar funções específicas, geralmente voltados a teste de gerenciamento de crises e execução de procedimentos que envolvam pessoas.
    - *Full Scale*: o tipo mais detalhado de teste. Com este teste, todo o ou a maioria dos planos são postos em ação. Os objetivos principais aqui são simular uma situação real de recuperação. Os exercícios neste caso são geralmente mais longos.

REFERÊNCIAS

[1] DRII's Professional Practices document
http://www.drii.org/displaycommon.cfm?an=2

[2] The BCI Guide
http://www.thebci.org/gpg.htm

Capitulo

15

15 – CONFORMIDADE

.

POR: RENATO OPICE BLUM E CAMILLA DO VALE JIMENE

TRATAREMOS NESTE CAPÍTULO DE CONCEITOS

OBJETIVOS

O objetivo deste capítulo é

Ao final deste capítulo você estará apto a:

- ❒ Avaliar os riscos de segurança relacionados à nõ conformidade
- ❒ Avaliar possíveis infrações de direitos de propriedade intelectual

- ❒ Criar recomendações de manutenção de registros
- ❒ Lidar com questões relativas à privacidade dentro da empresa
- ❒ Analisar os recursos de criptografia sobre a ótica de conformidade
- ❒ Dimensionar controles de auditoria

15 - CONFORMIDADES

> ✓ *Objetivo: "Evitar a violação de qualquer lei criminal ou civil, estatutos, regulamentações contratuais e de quaisquer requisitos de segurança da informação".*

Nos dias atuais, pode-se afirmar que o que há de mais importante no mundo corporativo é a informação. Os detentores obtêm larga vantagem na disputa pelo exigente mercado, porém só isso não basta, é imprescindível ainda garantir a disponibilidade e o acesso à mesma.

Outrossim, os meios eletrônicos por onde trafegam a informação são expostos constantemente a todo tipo de ameaça, tais como: espionagem, concorrência desleal, fraudes eletrônicas, sabotagem, e até mesmo seqüestro de informações essenciais para a organização.

Desse modo, as questões relacionadas à Segurança da Informação conquistaram lugar de destaque nas estratégias corporativas em âmbito mundial. Proteger a informação das inúmeras ameaças tornou-se essencial para garantir a continuidade do negócio, minimizando riscos e maximizando o retorno sobre os investimentos.

Diversas normas regem os procedimentos relativos à Segurança da Informação, dentre elas a ABNT NBR ISO/IEC 17799:2005, que constantemente é revisada e atualizada para acompanhar o dinamismo da área de tecnologia da informação.

No entanto, não podemos esquecer que o universo corporativo está alocado em um Estado de Direito, onde o exercício aos direitos sociais e individuais é assegurado, como valores supremos da sociedade, através de vasta legislação.

Mas em que ponto a Segurança da Informação e o Estado de Direito convergem?

Ora, a adoção e a implementação do código de práticas para a gestão da segurança da informação devem estar obrigatoriamente alinhadas às leis, estatutos, regulamentações ou obrigações contratuais inerentes, sob pena de sofrer sanções legalmente previstas. Em que pese referidas práticas, mormente estarem restritas ao universo corporativo, em hipótese alguma deve deixar-se de considerar os aspectos legais envolvidos.

Nesse passo, estudaremos uma das seções de maior relevância da norma, cujo teor essencialmente trata das questões legais e jurídicas inerentes à gestão da segurança da informação.

Como é notório, as questões jurídicas são consideradas de difícil compreensão para os profissionais não especializados na área, entretanto a norma apresenta estrutura extremamente clara, facilitando consideravelmente a utilização do documento.

Certamente, a análise de referidas questões não dispensa o apoio de consultoria jurídica especializada, pois se trata de apertada síntese de objetivos, controles, conceitos e diretrizes para implementação, porém, não deixam de ser de grande valia para os administradores que pretendem adotar as técnicas de segurança previstas na ABNT ISO/IEC NBR 17799:2005.

15.1 - CONFORMIDADE COM REQUISITOS LEGAIS

Neste item da norma há especificação direta sobre o assunto abordado, tendo por escopo evitar a violação de qualquer legislação, seja civil ou criminal, bem como de estatutos, regulamentações ou obrigações contratuais inerentes aos requisitos de segurança da informação.

A categoria em comento frisa ainda que o projeto, a operação, o uso e a gestão dos sistemas de informação podem eventualmente estar em seara submetida a requisitos contratuais, regulamentares ou estatutários.

Nesse sentido, válido se faz trazer à baila algumas definições conceituais jurídicas, as quais serão certamente elucidadoras. Vejamos:

- **Legislação**: conjunto de leis decretadas ou promulgadas em um país, disciplinando matéria em caráter geral ou específico. Ex.: Constituição Federal, Código Civil, Código Penal, Consolidação das Leis do Trabalho, Lei do Software, Lei da Propriedade Industrial;

- **Estatutos**: complexo de regras estabelecidas e observadas por uma instituição jurídica a serem adotadas como lei orgânica, que fixam os princípios institucionais de uma corporação pública ou privada. Ex.: Estatuto Social, Estatuto dos Funcionários Públicos;

- **Regulamentos**: conjunto de normas ou regras, em que se fixam o modo de direção ou condução de uma instituição ou associação. Ex.: Regulamento de Segurança da Informação;

Obrigações Contratuais: obrigações oriundas de acordo de duas ou mais pessoas físicas ou jurídicas para entre si, constituir, regular ou extinguir uma

relação jurídica. Ex.: Contrato de Compra e Venda, Contrato de Trabalho, Contrato com Empresas Terceirizadas.

Após as definições acima citadas, restam evidentes quais são os instrumentos jurídicos que devem ser observados para a implementação de gestão de segurança da informação nos moldes da ABNT NBR ISO/IEC 17799:2005, a fim de evitar a violação dos mesmos.
Inoportuno seria deixar de salientar que em nosso ordenamento jurídico ninguém pode alegar desconhecimento da lei para se eximir de seus efeitos, com apoio no art. 3º, do Decreto-Lei n.º 4.657/42 (Lei de Introdução ao Código Civil Brasileiro). E mais: a própria norma alerta para o fato de que os requisitos legislativos podem variar de país para país, o que torna a análise jurídica imperiosa nesse sentido, evitando demandas judiciais em face das corporações.

Tal procedimento resguarda não só a organização, como também os administradores, os empregados e terceiros envolvidos em todas as esferas do Direito.

Nesse sentido, o Código Civil Brasileiro, em seu art. 186, prevê a responsabilidade civil para aquele que viola direito ou causa dano a outrem, ainda que exclusivamente moral, por ação ou omissão voluntária, negligência ou imprudência, configurando-se ato ilícito, ficando obrigado a repará-lo independentemente de culpa, quando a atividade normalmente desenvolvida pelo autor do dano implicar por natureza em risco para outrem (art. 927,Código Civil).
Ainda na mesma trilha de entendimento, referido diploma legal preconiza, através do art. 1.016, a responsabilidade solidária dos administradores perante a sociedade e terceiros prejudicados no desempenho de suas funções.

Desse modo, resta evidente a enorme importância da efetiva aplicação do item 15.1 da ABNT NBR ISO/IEC 17799:2005 no desenvolvimento da estrutura para

blindar juridicamente a corporação na gestão da segurança da informação, considerando-se que o objetivo maior das corporações na adoção da norma é a minimização dos riscos inerentes e não a geração de mais riscos.

15.1.1 – IDENTIFICAÇÃO DA LEGISLAÇÃO VIGENTE

No mesmo sentido, o sub-item 15.1.1 relata a necessidade da identificação da legislação vigente e, conforme anteriormente exposto, é imperiosa a identificação minuciosa de toda a legislação vigente no país. Entretanto, há previsão de controle específico para gerir esse procedimento. Vejamos:

O tipo de controle sugerido para a identificação da legislação vigente é fundamentado na verificação através de documentação. A norma preconiza que todos os requisitos estatutários, regulamentares e contratuais relevantes, bem como o enfoque da organização para atender tais requisitos, sejam explicitamente definidos, documentados e mantidos atualizados para cada sistema de informação.

No tocante às diretrizes para implementação, estas também indicam a documentação como a melhor maneira de implementar os controles específicos e as responsabilidades individuais para atender aos requisitos de maneira similar ao controle sugerido.

Assim, podemos afirmar que todo o processo de análise jurídica da legislação vigente, suas atualizações, bem como a relação de todas as normas inerentes a serem observadas e, por fim, a atribuição de responsabilidades para atendimento de tais requisitos, devem ser documentados pela organização de maneira formal e segura.

15.1.2 – DIREITOS DE PROPRIEDADE INTELECTUAL

Tratando de assunto mais específico e não menos importante, o sub- item 15.1.2 relaciona os procedimentos a serem adotados quanto aos direitos de propriedade intelectual. A observância de tal previsão da norma é de extrema importância considerando o prejuízo iminente caso a corporação descumpra a legislação vigente.

Primeiramente, o controle sugerido defende a aplicação de procedimentos apropriados para garantir a conformidade com os aspectos legais no uso de material, os quais podem estar sob proteção de direitos de propriedade intelectual e uso de software. Mais adiante, nas diretrizes para implementação, são feitas considerações muito relevantes para proteção de material que possa ser considerado propriedade intelectual.

Dentre tais considerações, a norma elenca as principais posturas a serem adotadas, quais sejam:

- divulgação de política de conformidades com direitos de propriedade intelectual, que contenha definição expressa sobre o uso legal de software. Seria adequado que a política mencionasse a legislação vigente sobre o tema;
- aquisição de software somente por meio de fontes idôneas para assegurar que o direito autoral não seja violado;
- conscientizar os empregados através de políticas e adotar ações disciplinares em face dos que violarem tais políticas. Seria adequado que as ações disciplinares culminassem até em demissão por justa causa;
- manter o registro de ativos e identificar todos os ativos possivelmente relacionados aos direitos de propriedade intelectual. Assim, deve-se

verificar e registrar tudo dentro da organização que esteja submetido à legislação pertinente;

- manter provas da propriedade de licenças, tais como contrato de licença, recibos, manuais, discos mestres;
- implementação de controles para que o número de usuários permitidos seja compatível com o número de licenças adquiridas, tal recomendação é de extrema importância, haja vista o disposto na Lei n.º 9609/98 (lei do software);
- proceder a constantes verificações para que somente sejam instalados produtos de software autorizados e licenciados na corporação;
- criar normas para manutenção das condições adequadas de licenças;
- adotar contratos para transferência de software para terceiros;
- utilizar ferramentas adequadas de auditoria ;
- identificar e respeitar termos e condições para software obtidos a partir de redes públicas;
- não duplicar, alterar para outro formato ou ainda extrair registros de filme ou áudio além do que permitido pela lei de direito autoral, qual seja, Lei n.º 9610/98;
- não copiar livros, artigos ou outros documentos, fora dos padrões admitidos pela lei de direitos autorais n.º 9610/98.

Finalizando tal sub-item, as informações adicionais esclarecem que os direitos de propriedade intelectual incluem os direitos sobre software. Isto porque a lei de propriedade intelectual brasileira equipara os programas de computadores às obras que contenham criação de espírito.

15.1.3 – PROTEÇÃO DE REGISTROS ORGANIZACIONAIS

Partindo para o sub-item 15.1.3, verificamos que esse relaciona controles e diretrizes para a proteção de registros organizacionais. No tocante ao controle, sugere que os registros importantes para a organização sejam protegidos contra perda, destruição e falsificação, nos moldes dos requisitos regulamentares, contratuais, estatutários ou do negócio.

Outrossim, a premissa de maior relevância inserta em referido tópico é a retenção de alguns registros de forma segura que podem ser exigidos eventualmente para subsidiar defesas adequadas em processos cíveis e criminais. Nesse passo, é adequada ainda a ideal proteção de tais registros, não só para defesas judiciais, como também propositura de demandas a fim de resguardar os direitos da corporação, incluindo-se os registros relativos à seara do Direito Tributário e Trabalhista.

A 17799 apenas faz breve menção sobre a proteção dos registros organizacionais, frisando que a ISO 15489-1 trata mais especificamente do gerenciamento de registros organizacionais.

15.1.4 – PROTEÇÃO DE DADOS E PRIVACIDADE DE INFORMAÇÕES PESSOAIS

Ainda na trilha de proteções, o item subseqüente 15.1.4 sugere como controle essencial o cumprimento das legislações aplicáveis à privacidade e a proteção de dados, sendo esta a única opção segura às corporações para evitar ofensas às leis pertinentes.

A adoção de contratos para regulamentar o tema em comento, e a comunicação a todas as pessoas envolvidas no processamento de informações pessoais são as diretrizes para implementação indicadas pela norma. Ademais, a norma preconiza também a indicação de pessoa responsável pelo controle apropriado e

gestão da privacidade de informações pessoais e proteção de dados, formalizando-se através de um "gestor de proteção de dados", o que minimiza consideravelmente a violação de legislação nesse sentido, pois o gestor será responsável pelas orientações gerais a serem fornecidas a todos os gerentes, usuários e provedores de serviços sobre as responsabilidades de cada um e os procedimentos específicos recomendados.

A título de precaução, a norma salienta, ainda, que alguns países têm promulgado leis que regulamentam a coleta, processamento e transmissão de dados pessoais, impondo responsabilidades sobre aqueles que coletam, processam e disseminam informações pessoais.

15.1.5 – PREVENÇÃO DE MAU USO DE RECURSOS DE PROCESSAMENTO DA INFORMAÇÃO

Prosseguindo em nossos estudos, passamos para o próximo sub-item, que trata da prevenção ao mau uso de recursos de processamento da informação, qual seja, o 15.1.5, indicando como controle o convencimento dos usuários a não utilizar os recursos de processamento da informação para propósitos não autorizados.

Posto isso, é adequado que a direção indique claramente quais são os propósitos não relacionados ao negócio ou os não autorizados através de instrumento específico, considerando o uso impróprio tudo o que fugir dos parâmetros estabelecidos, implantando-se dispositivos que verifiquem a conformidade com a política de uso dos recursos de processamento da informação.

A norma considera a monitoração como dispositivo válido para viabilizar supra citada verificação, frisando a imprescindibilidade de assessoria legal antes da implementação de tal dispositivo.

Inoportuno seria deixar de salientar que o Tribunal Superior do Trabalho, bem como os Tribunais Regionais do Trabalho Brasileiros, vêm cristalizando a jurisprudência pátria no sentido de permitir o monitoramento dos meios eletrônicos da corporação para verificação do mau uso dos recursos de processamento da informação, o que possibilita inclusive a dispensa motivada por justa causa, inexistindo expectativa de privacidade por parte dos empregados da organização.

Acertadamente, e a fim de evitar maiores discussões, a norma sugere que todos os usuários estejam conscientes do escopo de suas permissões de acesso e da monitoração realizada, o que pode ser viabilizado através de registro de autorizações por escrito devidamente assinadas por funcionários, fornecedores e terceiros envolvidos na organização, o que mormente é denominado de termo de uso dos sistemas de informação.

A norma ainda sugestiona uma ótima opção para as corporações, que consiste em apresentar mensagem no momento da conexão inicial advertindo ao usuário que o recurso de processamento da informação utilizado é de propriedade da organização e que não são permitidos acessos não autorizados, necessitando de confirmação do usuário para o prosseguimento do processo de conexão.

15.1.6 – REGULAMENTAÇÃO DE CONTROLES DE CRIPTOGRAFIA

Finalizando a categoria das conformidades legais, o sub-item 15.1.6 vem regulamentar os controles de criptografia, instituindo como itens a ser

considerados para conformidade com leis, acordos e regulamentações pertinentes:

- verificação das restrições à importação e exportação de hardware e software para execução de funções criptográficas, bem como de programas que foram projetados com funções criptográficas embutidas;
- restrições específicas ao uso de criptografia;
- questões relacionadas ao acesso das autoridades dos países à informação cifrada por hardware ou software para fornecer confidencialidade ao conteúdo.

Novamente a norma atenta para a necessidade de apoio jurídico especializado para verificar qual a legislação vigente sobre criptografia, garantindo a conformidade legal, bem como a ajuda de consultoria para enviar informações cifradas ou controles de criptografia para outros países.

15.2 - CONFORMIDADES COM NORMAS E POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E CONFORMIDADE TÉCNICA

- Garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação, através de:
  - Conformidade com as políticas e normas de segurança da informação;
  - Verificação da conformidade técnica com as normas de segurança da informação.

Primeiramente, insta salientar que houve alteração na nomenclatura do tópico principal e de todas as categorias relacionadas na nova versão da ISO/IEC 17799 editada em 2005, excetuando-se o sub- item 15.2.2, que continua com a mesma denominação de "verificação de conformidade técnica".

A seção 15.2 tem por escopo garantir a conformidade e compatibilidade dos sistemas com as políticas de segurança da informação, analisando-se a segurança dos sistemas em intervalos regulares e programados, guiando-se através das políticas instituídas e auditando-se as plataformas técnicas.

15.2.1 – CONFORMIDADE COM AS POLÍTICAS E NORMAS DE SEGURANÇA DA INFORMAÇÃO

Na ordem subseqüente, o sub-item 15.2.1 estabelece como controle a atribuição de responsabilidade aos gestores, que verificariam se todos os procedimentos de segurança dentro da sua área estão sendo executados adequadamente nos moldes previstos no regulamento de segurança da informação adotada pela corporação.

Análises críticas a intervalos regulares da conformidade do processamento da informação com a política de segurança devem ser realizadas pelos gestores, e caso alguma não-conformidade seja detectada, o gestor deve adotar o seguinte procedimento: determinar a causa da não conformidade; avaliar a real necessidade de ação para que a não-conformidade não se repita novamente; aplicar ação corretiva, e, por fim, registrar e manter todo o ocorrido, relatando os resultados para as pessoas competentes, o que vem a ser medida de cautela que resguarda os direitos do gestor, haja vista a grande responsabilidade atribuída ao mesmo.

15.2.2 – VERIFICAÇÃO DA CONFORMIDADE TÉCNICA

Finalizando tal categoria, a norma traz o tema verificação da conformidade técnica (15.2.2), sugestionando como controle a verificação periódica dos sistemas de informação em conformidade com as normas de segurança implementadas na organização, sendo referida verificação técnica realizada manualmente por engenheiro de sistemas, gerando relatório técnico para interpretação por técnico especialista.

15.3 - CONSIDERAÇÕES QUANTO À AUDITORIA DE SISTEMAS DE INFORMAÇÃO

- Objetivo: elevar ao máximo a eficácia e diminuir a interferência no processo de auditoria dos sistemas de informação, protegendo-se a integridade das ferramentas de auditoria.

Por fim, encerrando a ABNT ISO/IEC 17799:2005, a categoria 15.3 relata considerações quanto à auditoria de sistemas de informação, objetivando elevar ao máximo a eficácia e diminuir a interferência no processo de auditoria dos sistemas de informação, protegendo-se a integridade das ferramentas de auditoria.

15.3.1 – CONTROLES DE AUDITORIA DE SISTEMAS DE INFORMAÇÃO

Como em toda a extensão da norma há controle previsto para auditoria de sistemas de informação (15.3.1), aconselhando que a auditoria e suas atividades inerentes, quando envolvida na verificação dos sistemas operacionais, sejam minuciosamente planejadas e acordadas internamente a fim de evitar quaisquer riscos de interrupção nos procedimentos e processos do negócio.

As diretrizes para implementação no assunto em testilha têm caráter bastante sintético, porém não de menor importância, senão vejamos os aspectos mais relevantes. Os acordos relativos aos requisitos de auditoria devem ser acordados com o nível apropriado de administração (observância de hierarquia); objetivo da verificação da auditoria deve ser acordado e controlado, limitando-se a verificação apenas a acesso para leitura de software e dados. Caso haja necessidade de acessos que ultrapassem os limites da leitura, devem ser permitidos apenas e tão somente através de cópias dos arquivos do sistema, apagando-se os mesmos ao final da auditoria, e caso, eventualmente, exista a necessidade de guardar

referidos arquivos como documentos de auditoria, que seja realizado com a proteção apropriada; monitoração de todo acesso; documentação de todo o procedimento, bem como que os auditores não tenham nenhum vínculo com as áreas auditadas.

Tais diretrizes certamente têm por finalidade a preservação da idoneidade do procedimento de auditoria, gerando confiabilidade inequívoca nas conclusões apresentadas.

15.3.2 – PROTEÇÃO DE FERRAMENTAS DE AUDITORIA DE SISTEMAS DE INFORMAÇÃO

Encerrando definitivamente a 17799, o sub-item 15.3.2 trata da proteção das ferramentas de auditoria dos sistemas de informação, adotando como controle a restrição e proteção ao acesso a referidas ferramentas, prevenindo assim o uso inadequado ou o comprometimento das ferramentas.

No tocante às diretrizes para implementação, a norma estabelece que o acesso às ferramentas, tais como software ou arquivo de dados, seja devidamente separado de sistemas em operação ou desenvolvimento, vedando-se o arquivamento em áreas de livre acesso aos usuários do sistema, a menos que seja criado um nível de proteção apropriado.

Quanto aos terceiros envolvidos na auditoria (empresas terceirizadas especializadas em auditagem, por exemplo), a norma salienta o risco de mau uso de ferramentas e da informação acessada por tais profissionais. Dessa forma, para evitar maiores riscos, é recomendado controle para avaliação de riscos e restrição de acesso físico, previstos na própria 17799:2005.

ENCERRAMENTO

Diante de todo o exposto, resta evidente a extrema importância da seção 15 da ABNT ISO/IEC 17799:2005, que alerta e direciona a conduta a ser adotada pelas corporações no tocante aos aspectos legais inerentes à Segurança da Informação, frisando-se sempre a necessidade de apoio de consultoria jurídica especializada no assunto, haja vista as peculiaridades da legislação, propiciando a adoção de postura adequada e segura, sempre resguardando os direitos das corporações.

Autores:

Renato Opice Blum - Advogado e economista; Professor da FGV, PUC, IBMEC/IBTA, UFRJ, FIAP, ITA/CTA (convidado) e outras; Árbitro da FGV, da Câmara de Mediação e Arbitragem de São Paulo (FIESP), do Tribunal Arbitral do Comércio e outras; Presidente do Conselho de Comércio Eletrônico da Federação do Comércio/SP; Autor/ Colaborador das Obras: "Direito Eletrônico - a internet e os tribunais", “Novo Código Civil – questões controvertidas”, “O direito na Sociedade da Informação”, “Internet Legal”, “Conflitos sobre Nomes de Domínios”, "Comércio Eletrônico", "Direito & Internet - aspectos jurídicos relevantes”, “Direito da Informática – temas polêmicos”, "Responsabilidade Civil do Fabricante e Intermediários por Defeitos de Equipamentos e Programas de Informática", "O Bug do Ano 2000 - aspectos jurídicos e econômicos” e outras.

Camilla do Vale Jimene - Advogada atuante nas esferas cível e trabalhista, com ênfase em Direito Eletrônico e da Informática. Pós-graduanda em Processo Civil pela PUC-SP. Cursou Aperfeiçoamento em Processo Trabalhista, junto ao Prima-Ielf. Desenvolveu estudos sobre a NBR ISO/IEC 17799:2005 (Tecnologia da Informação). Palestrante convidada no Seminário “Riscos do Outsourcing e Internet” realizado na Bovespa, o qual originou matéria publicada em edição da revista Banco Hoje; atuou como Presidente de Mesa e Palestrante no curso “Controle de E-mails, Segurança da Informação e os Tribunais” na Academia de Desenvolvimento Profissional e Organizacional (ADPO); congressista no Congresso de Auditoria de Sistemas e Segurança da Informação (CNASI), participante do seminário “Práticas, Políticas e Instrumentos sobre o Uso da Internet nas Empresas” no Canal Executivo. Autora de diversos artigos relacionados ao Direito da Informática e Internet.