VERSÃO 1

GSIC345

AUDITORIA E CONFORMIDADE DE SEGURANÇA DA INFORMAÇÃO

Roberto Wagner da Silva Rodrigues
Jorge Henrique Cabral Fernandes

Dilma Rousseff
Presidente da República

José Elito Carvalho Siqueira
Ministro do Gabinete de Segurança Institucional

Antonio Sergio Geromel
Secretário Executivo

Raphael Mandarino Junior
Diretor do Departamento de Segurança da Informação e Comunicações

Reinaldo Silva Simião
Coordenador Geral de Gestão da Segurança da Informação e Comunicações

Fernando Haddad
Ministro da Educação

UNIVERSIDADE DE BRASÍLIA

José Geraldo de Sousa Junior
Reitor

João Batista de Sousa
Vice-Reitor

Pedro Murrieta Santos Neto
Decanato de Administração

Rachel Nunes da Cunha
Decanato de Assuntos Comunitários

Márcia Abrahão Moura
Decanato de Ensino de Graduação

Oviromar Flores
Decanato de Extensão

Denise Bomtempo Birche de Carvalho
Decanato de Pesquisa e Pós-graduação

Noraí Romeu Rocco
Instituto de Ciências Exatas

Priscila Barreto
Departamento de Ciência da Computação

CEGSIC

Coordenação
Jorge Henrique Cabral Fernandes

Secretaria Pedagógica
Andréia Lacê
Eduardo Loureiro Jr.
Lívia Souza
Odacyr Luiz Timm
Ricardo Sampaio

Assessoria Técnica
Gabriel Velasco

Secretaria Administrativa
Indiara Luna Ferreira Furtado
Jucilene Gomes
Martha Araújo

Equipe de Produção Multimídia
Alex Harlen
Lizane Leite
Rodrigo Moraes

Equipe de Tecnologia da Informação
Douglas Ferlini
Osvaldo Corrêa

Texto e ilustrações: Roberto W. S. Rodrigues; Jorge H. C. F.ernandes | Capa, projeto gráfico e diagramação: Alex Harlen

Desenvolvido em atendimento ao plano de trabalho do Programa de Formação de Especialistas para a Elaboração da Metodologia Brasileira de Gestão de Segurança da Informação e Comunicações – CEGSIC 2009-2011.

Sumário

CURRÍCULO RESUMIDO DO AUTOR

Roberto Wagner da Silva Rodrigues

É PhD em Computação pelo Imperial College of Science Technology and Medicine (2001)-Inglaterra; Mestre em Ciência da Computação pela Universidade Federal de Pernambuco (1996); Especialista em Informática pela Universidade de Fortaleza (1992); e obteve as seguintes graduações: Licenciatura Plena - Eletrônica & Desenho Industrial pelo Centro Federação de Educação Tecnológica de Minas Gerais (1991) e Bacharelado em Ciência da Computação pela Universidade Estadual do Ceará (1988); Cursou Bacharelado em Matemática (incompleto) pela Universidade Federal do Ceará (1988-89); e Bacharelado em Administração de Empresas (incompleto) pela UECE (1988-1990); Técnico em Telecomunicações pela ETFCE (1984). EXPERIÊNCIA PROFISSIONAL: atualmente é professor do Instituto Federal de Brasília. Foi professor adjunto da Universidade de Brasília até 2009 - Departamento de Ciência da Computação. Foi Professor do Centro Federal de Educação Tecnológica do Ceará; foi Secretário Interino e Diretor de Gestão da Informação da Secretaria de Avaliação e Gestão da Informação, no Ministério do Desenvolvimento Social e Combate à Fome - MDS. Foi Diretor de Tecnologia da Informação do CEFET-CE, professor do Mestrado da Universidade Estadual do Ceará e professor substituto da Universidade Federal do Ceará no Departamento de Engenharia Elétrica. Tem experiência profissional em organizações públicas nas seguintes áreas: gestão pública, monitoramento e avaliação de politicas e programas sociais, sistemas de informação e bases de dados sociais. Na iniciativa privada trabalhou em Teleprocessamento, Computação (analista de sistemas programador) e Telecomunicações. Foi Pesquisador associado da British Telecomm. São temas de interesse: avaliação, meta-avaliação e monitoramento de políticas públicas (tecnologia e informação), gestão da informação e do conhecimento, auditoria de segurança da informação, arquitetura de sistemas, sistemas distribuídos, workflow e gestão de processos de negócio (BPM).

CURRÍCULO RESUMIDO DO AUTOR

Jorge Henrique Cabral Fernandes

É doutor (2000) e mestre (1992) em Ciência da Computação pela Universidade Federal de Pernambuco. Especialista em Engenharia de Sistemas (1988) e graduado em Ciências Biológicas (1986) pela Universidade Federal do Rio Grande do Norte. É Professor Adjunto do Departamento de Ciência da Computação (CIC), professor e representante da coordenação na Pós-Graduação em Ciência da Informação da Faculdade de Ciência da Informação e Documentação (PPGCINF/FCI), na Universidade de Brasília. É sócio da Sociedade Brasileira de Computação (SBC) e da Associação Nacional de Pesquisa e Pós-Graduação em Ciência da Informação (ANCIB). Tem experiência nas áreas de Ciência da Computação e Ciência da Informação, com ênfase em engenharia de software, segurança cibernética, segurança da informação, linguagens de programação, bancos de dados e tecnologias educacionais.

1. Introdução

A sempre crescente demanda por prestação de mais e melhores serviços públicos tornou necessário disponibilizar meios de processamento de dados e de comunicação para troca de informações, bem como para permitir interação entre as organizações públicas e os cidadãos. Essa interação tem sido mediada cada vez mais pela *Internet* e por meio de serviços de e-gov apoiados em sistemas de informação computadorizados. Consequentemente, a segurança (especialmente a disponibilidade, a integridade, a confidencialidade ou sigilo e a autenticidade) dessas informações passou a ser uma preocupação do poder público e um tema crítico da gestão moderna, seja ela pública ou privada. Uma forma de gerenciar essa criticidade é criar normas, formular políticas, padronizar procedimentos e práticas, estabelecer medições e métricas, além de automatizar controles, de modo a não só aumentar previsibilidade dos resultados dessa prestação de serviço, mas principalmente melhorar a capacidade de lidar com riscos decorrentes das vulnerabilidades dos sistemas – sejam eles manuais ou automatizados - e das ameaças existentes (sobretudo as originadas da Internet).

Essas normas, políticas, procedimentos, práticas, métricas e mecanismos automatizados são controles, e podem ser analisadas através de sua vinculação com os objeto de controle que são decompostos em pontos de controle. A auditoria de segurança de informação é uma atividade devidamente estruturada para examinar criteriosamente a situação desses controles que se aplicam à segurança da informação, especialmente por meio da análise de objetos e seus pontos de controle, *vis-a-vis* a probabilidade de ameaças às informações críticas sobre as quais atuam esses controles. Isto é necessário porque os controles ou a ausência deles podem se constituir em vulnerabilidades exploráveis ou portas de entrada para produzir incidentes de segurança da informação. A auditoria cria condições técnicas para investigar e emitir um juízo sobre as evidências encontradas, de modo a se antecipar ante a possíveis riscos de violação de um patrimônio precioso: os ativos de informação. Esses ativos correspondem àquelas informações e todos os recursos associados que têm alto valor para o negócio público ou privado. Consideram-se como ativos de informação os processos organizacionais e processuais (procedimentos, roteiros, atividades), itens físicos (instalações, equipamentos, cabeamento) e lógicos (programas, sistemas, estruturas de dados), que devem ser auditados continuamente.

De outra forma, auditoria é a expressão de opinião feita por um profissional devidamente qualificado, acerca de uma determinada situação, e documentada na forma de um relatório ou parecer. Para tal, o auditor emprega práticas geralmente aceitas, baseadas em um método racional, em evidências, em respeito aos princípios éticos, com responsabilidade perante o cliente, com devido cuidado e habilidade profissional, sujeito à revisão por pares, mas com independência no que se refere à roteirização, à investigação e análise e à produção do relato.

Em linhas gerais, a auditoria de segurança da informação pretende assegurar que os ativos de informação, considerados os objetos de auditoria em segurança da informação, estejam absolutamente sob controle da organização. Para tal, é preciso verificar que os controles estejam de acordo com as normas e políticas de segurança estabelecidas para esses ativos, bem como se o que está em operação alcança os objetivos de segurança definidos. A auditoria de segurança de informação envolve também o provimento de uma avaliação independente dos controles da organização (normas, políticas, padrões, procedimentos, práticas, métricas e mecanismos) empregados para salvaguardar a informação, em formato eletrônico ou não, contra perdas, danos, divulgação não intencional e indisponibilidades. Por fim, a auditoria é uma atividade realizada na forma de ações projetizadas, que tem um início, meio e fim, e que visam produzir resultados dentro de custos, prazos e qualidades esperadas. Para alcançar tais objetos, as auditorias, projetos individuais, agrupam-se em programas, que compreendem a realização de várias auditorias ao longo de um período de tempo de meses ou anos, e que visam melhorar sistematicamente o desempenho, a eficiência e a segurança organizacionais.

1.1 Princípios Gerais

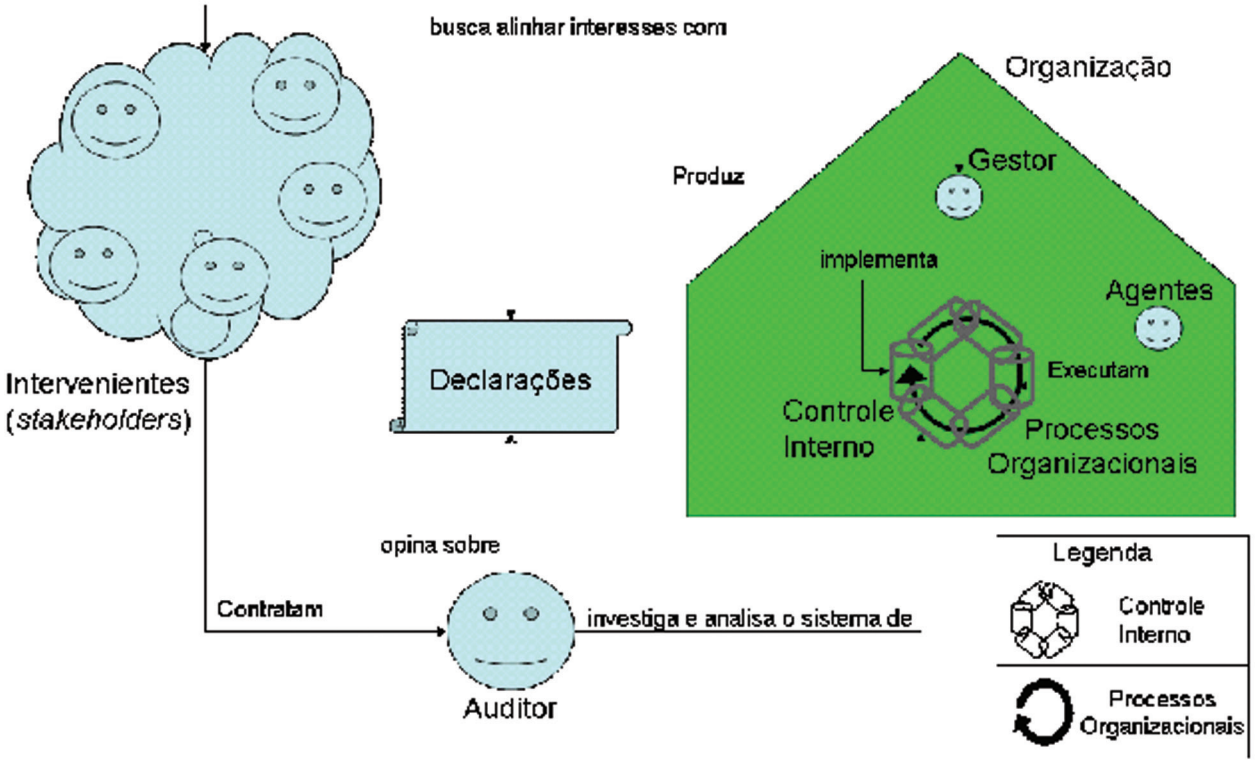

Figura 1. O Papel do Auditor numa Auditoria.
Fonte: Adaptado de Fernandes (2009).

Embora a atenção e o motivo de se realizar auditorias de segurança da informação seja a existência de ativos de informação, é preciso que o auditor domine não só o conhecimento especializado necessário, mas também todo o processo e os princípios de auditoria geral, pois os mesmos se aplicam à auditoria de segurança da informação. A título de ilustração dos princípios gerais de auditoria, a Figura 1 mostra as principais relações entre um gestor, um auditor, os intervenientes ou interessados numa organização (também chamados de stakeholders) e os agentes que executam os processos organizacionais sob direção do gestor. Primariamente, interesses dos intervenientes e da gestão devem estar alinhados, ou seja, as ações devem caminhar no mesmo sentido, conforme os objetivos de negócio da organização. Como o gestor é o principal responsável pela organização, este alinhamento de interesses deve ocorrer entre os intervenientes e o gestor.

No Curso de Especialização em Gestão da Segurança da Informação, edição 2007/2008, foram desenvolvidas algumas monografias que abordaram o tema auditoria, que estão sumarizadas em Fernandes (2010d).

1.2 Controle Interno

A Figura 1 ilustra que, na organização, existe um elemento responsável pelo controle dos processos da organização, chamado de controle interno. O controle interno compreende todo o conjunto de controles, implementado sob responsabilidade da gestão da organização. Tem por objetivo assegurar que as miríades de processos executados pelos agentes humanos e computacionais da organização - em última instância sob sua responsabilidade - não sofrerão desvio de finalidade. Dado que o gestor declara fatos sobre o desempenho das atividades da organização, periodicamente e para o interesse dos intervenientes, faz-se necessário recorrer

a um profissional especializado, o auditor, para opinar sobre a veracidade de tais declarações. Uma vez que é inviável ao auditor examinar minuciosamente a ocorrência de todos os processos e atividades realizados pela organização, mesmo ao longo de um curto período de tempo, o trabalho do auditor basicamente consiste em verificar que as declarações do gestor estão satisfatoriamente coerentes com as condições observadas no controle interno, emitindo uma opinião fundamentada acerca de tais declarações. O auditor tem como clientes os intervenientes, inclusive o próprio gestor, no caso de uma auditoria interna.

Note que o controle interno, representado graficamente por um hexágono de tubos que conduzem fluxos de processos, consiste num complexo sistema de informações, acoplado aos processos organizacionais. Os princípios do controle interno estão descritos em modelos como o COSO (), adotado em modelos como o COBIT. Os componentes de um sistema de controle interno, segundo o COSO (2007), são:

- Ambiente de Controle

O ambiente de controle é um ambiente organizacional favorável ao controle. Consiste num conjunto de ações que provê disciplina e estrutura à organização. É baseado nos princípios da integridade, em valores éticos e em competência, definindo um padrão de conduta, especialmente por parte da gestão.

- Avaliação do risco

A avaliação de risco consiste na identificação, análise e priorização de riscos relevantes, relacionados ao alcance dos objetivos da organização. Os riscos devem ser analisados apenas quando forem relevantes para o alcance dos objetivos da organização. Estes objetivos devem ser claramente definidos.

- Atividades de Controle

Segundo o COSO (2007), atividades de controle são políticas e procedimentos que garantem a realização das diretivas da gestão, as quais devem ser estabelecidas e comunicadas através de toda a organização, em todos os níveis e através de todas as funções. Tais atividades devem ser diretamente ligadas ao tratamento dos riscos para alcance dos objetivos.

- Informação e Comunicação

Segundo o COSO (2007) o componente informação e comunicação de um sistema de controle interno compreende criar um ambiente onde as necessidades de informação organizacionais são satisfeitas. A informação é gerida em todos os níveis da organização, visando o alcance dos objetivos de negócio. A gestão comunica-se efetivamente com os agentes da organização. Há canais efetivos e métodos não retributivos para comunicar informações significantes para os níveis superiores da organização. Há também efetiva comunicação entre a gestão e o conselho, de modo que cada qual tenha conhecimento de seus papéis relativos à governança.

- Monitoramento

Segundo o COSO (2007), monitoramento é uma avaliação, por pessoal apropriado, acerca do desenho e operação de controles de uma forma adequadamente regular e a tomada de ações necessárias. O monitoramento pode ser efetuado por meio de atividades contínuas e avaliações separadas. Os sistemas de controle interno devem ser estruturados para monitorarem a si mesmos de forma contínua, até um certo de grau, de modo que quanto maior for o grau e a efetividade do monitoramento contínuo, menor a necessidade de avaliações separadas. Por fim, também conforme o COSO, usualmente, alguma combinação de monitoramento contínuo e avaliações em separado garantirá que o sistema de controle interno manterá sua efetividade ao longo do tempo. A auditoria é uma abordagem de avaliação em separado.

Texto complementar

No caso do Brasil, a Lei n° 10.180, de 2001, "organiza e disciplina os Sistemas de Planejamento e de Orçamento Federal, de Administração Financeira Federal, de Contabilidade Federal e de Controle Interno do Poder Executivo Federal, e dá outras providências." O Título V desta Lei descreve as finalidades, a organização e as competências deste controle interno, coordenado pela Secretaria Federal de Controle Interno da Controladoria Geral da União, e que, dentre outras atribuições deve "realizar auditorias nos sistemas contábil, financeiro, orçamentário, de pessoal e demais sistemas administrativos e operacionais."

1.3 Auditoria e Controle, Interno e Externo

Quem avalia o controle interno de forma regular e freqüente é a auditoria interna. Outra forma de controlar a organização é por meio de uma controladoria externa (não mostrada), que também compreende um sistema de controle da organização, mas que não está sob a responsabilidade do gestor da organização. A controladoria externa ou controle externo tem a vantagem de ser muito mais independente de influências do gestor que no caso do controle interno, mas apresenta como desvantagem a dificuldade no acesso às informações, visto que não se encontra embutida nos processos organizacionais. Parte da controladoria externa envolve a realização de auditorias externas. No Brasil, o exercício da controladoria externa da Administração Pública Federal é realizado pelo Congresso Nacional, com auxílio preponderante do Tribunal de Contas da União. Não será aprofundada neste texto a distinção entre controle interno e externo, nem entre auditoria interna e externa, mas é importante destacar que a auditoria interna também está sujeita ao controle feito por auditores externos. De outra forma, considerável parte das informações providas para auditorias externas é fornecida pela auditoria interna. Independentemente disso, o Auditor deve, acima de tudo, atuando de forma interna ou externa, ser capaz de emitir uma declaração em que analisa e avalia, com toda lisura, aquilo que se definiu como sensível à segurança da organização, lisura essa típica da atividade de auditoria. Tudo isto é feito em benefício dos intervenientes ou *stakeholders*, que no caso das organizações públicas se constituem a própria sociedade à qual devem atender.

Texto Complementar

Auditoria Contábil

O tema "Auditoria" herda um arcabouço conceitual sólido da área contábil, onde mais se desenvolveu. A auditoria contábil tem como objeto as contas públicas ou privadas, seja para verificar o desempenho da organização frente ao seus objetivos de lucros nas organizações privadas, seja na verificação da prestação de contas nas organizações públicas. Tem ainda a função de verificar que os registros contábeis estão em conformidade com as normas e procedimentos exarados nos marcos regulatórios da atividade contábil. A função da contabilidade não é só ser um instrumento de decisão, mas também de informação. Na medida em que a informação passa a ser o bem mais precioso das organizações na era da Sociedade da Informação, há tendência de convergência entre as atividades de auditoria contábil e de segurança da informação. Não é de somenos importância mencionar que o resultado de auditorias contábeis tem sérias implicações sociais e econômicas nas esferas públicas e privadas pelos impactos que podem provocar na vida das pessoas em função de sua natureza alocativa.

1.4 Porque é Necessária a Segurança da Informação?

A auditoria de segurança da informação só tem sentido por permitir melhoria do tratamento da informação na organização. Ela cumpre basicamente as mesmas funções de uma auditoria de sistemas de informação, tais como descritos por Imoniana (2004) e por Schmidt, dos Santos e Arima (2005). A informação é produzida, identificada, armazenada, distribuída, usada e processada em todos os níveis da organização, visando o alcance dos objetivos de negócio,

sejam eles públicos ou privados. Essas atividades constituem a gestão da informação, que tem suas práticas definidas pelos sistemas de informação que apóiam os processos de trabalho na organização, sejam eles manuais ou automáticos. A gestão da informação tem fundamentos na administração, na contabilidade, na arquivologia, nas tecnologias da informação e da comunicação, nas ciências da informação e da computação, entre outras. Como ferramenta de segurança, a gestão da informação lança mão de elementos organizacionais, humanos, físicos e tecnológicos, integrados por meio de arquitetura e engenharia de sistemas, ou de forma mais geral através de uma abordagem cibernética.

O objetivo da auditoria da segurança da informação, aderente ao componente de monitoramento do COSO (2007) é então o controle de informações relevantes para o relato da gestão, conforme tais informações são produzidas, identificadas, armazenadas, distribuídas, usadas e processadas, dentro dos parâmetros estabelecidos pelos processos de controle da organização, a fim de suportar o alcance dos objetivos de negócio.

Note que o controle, mesmo sendo necessário para o alcance de garantias para o desempenho organizacional, cria limitações às ações dos agentes que executam processos na organização. Ou seja, por sua própria natureza e necessidade, produz cerceamento de liberdade de ações dos agentes, que se não fossem feitas levariam ao caos. Desta forma é importante que todos estes agentes recebam uma clara mensagem da alta administração quanto à forma de tratar a informação com segurança, pois é central para o controle dos negócios e alcance da missão institucional. As responsabilidades individuais dos agentes devem ser alinhadas com essa mensagem (visão de segurança) e a questão da segurança da informação deve ser embutida na cultura organizacional.

A mensagem da necessidade de segurança da informação é usualmente estabelecida por uma política. A política de segurança da informação, tratada em detalhes no texto de Souza Neto (2010), deve tornar claro que cada participante ou colaborador na organização (agentes em geral) é um ator relevante quando se trata de proteger ativos de informação, principalmente aqueles considerados estratégicos ou críticos. Os agentes devem estar cientes dos riscos de segurança existentes e das medidas preventivas que devem ser tomadas (OECD, 2002). Além disso, responsabilidades claras devem ser atribuídas aos agentes, de modo que se possam distribuir tarefas específicas ou gerais para que se esteja sempre aperfeiçoando os mecanismos de segurança da informação implantados. De forma mais prática, a política de segurança da informação é o principal controle de segurança numa organização, e a ele se articulam (e na maioria dos casos se subordinam) todos os demais controles

1.5 Porque Auditar a Segurança da Informação?

Porque é importante auditar a segurança da informação? O objetivo é, basicamente, atestar que os controles de segurança em prática são eficientes e eficazes. Tal evita exposições da organização a riscos que podem provocar danos, se concretizados. Mair (1998) indica que a introdução de controles evita:

1. manter registros de informação que estão errados;
2. contabilizar informações que não são aceitáveis;
3. interromper o negócio;
4. decidir erroneamente sobre gerenciamento; e dentre outras razões
5. evitar fraudes.

No ambiente desregulado dos sistemas de informação expostos à Internet, é também importante destacar que os controles evitam que a organização esteja sujeita a ataque de *hackers*.

Esse texto apresenta uma introdução aos métodos, processos e técnicas de auditoria de segurança da informação, muitos dos quais tem sua origem na auditoria contábil. Complementa o texto informações básicas sobre normativos e organizações do serviço público vinculadas à questão. Para explorar esses e outros assuntos, o restante desse texto está organizado em mais 11 seções, que são:

- Seção 2: Descreve em linhas gerais um processo de auditoria de segurança da informação.
- Seção 3: Descreve os propósitos e a organização de uma uma auditoria de segurança da informação.
- Seção 4: Descreve o que é a Roteirização da Auditoria
- Seção 5: Descreve os principais objetos e pontos de controle gerais para a auditoria de gestão de segurança da informação.
- Seção 6: Descreve objetos e pontos de controle mais adequados à auditoria de desempenho operacional de segurança da informação.
- Seção 7: Descreve objetos e pontos de controle mais adequados à estratégia de auditoria de conformidade de segurança da informação.
- Seção 8: Apresenta um modelo de plano de segurança, orientador essencial à auditoria, bem como discute o papel da gestão de riscos de segurança.
- Seção 9: Apresenta instrumentos, ferramentas e serviços auxiliares que devem ser usados para organizar, automatizar e agilizar a atividade de auditoria.
- Seção 10: Descreve alguns produtos ou artefatos que são as entregas que um auditor de segurança da informação deve produzir após executar uma roteirização de auditoria.
- Seção 11: Descreve como se organiza um programa de auditoria, ou um conjunto de auditorias associadas
- Seção 12: Apresenta considerações Finais. Descreve as limitações do texto e da possibilidade de trabalhar com auditoria em segurança da informação de forma viável e organizada.

2. Processo de Auditoria de Segurança da Informação

Esta seção apresenta um processo simplificado de auditoria de segurança da informação. Vários modelos de processo e metodologias de auditoria de sistemas e de tecnologia da informação podem ser encontrados na literatura, alguns deles criados pelas organizações públicas que atuam como órgãos de controle interno e externo. O modelo descrito a seguir é composto por 9 passos:

- Gestão do projeto ou do programa de auditoria
- Decisão sobre o propósito da auditoria
- Identificação de objetos e pontos de controle
- Definição de técnicas para obter evidências e procedimentos de controle
- Montagem da roteirização de auditoria
- Coleta e registro de evidências em papéis de trabalho
- Verificação, validação e avaliação de evidências
- Produção de pareceres e outros entregáveis
- Acompanhamento pós-auditoria

Estes passos são detalhados a seguir.

2.1 Gestão do Projeto ou do Programa de Auditoria

Auditorias isoladas e esporádicas são pouco eficazes, além de dispendiosas. O primeiro passo numa auditoria é estabelecer a gestão do projeto ou dos projetos que constituem um programa de auditoria. Auditoria é, em geral, um trabalho de equipe, realizado na forma de um projeto, no qual estão envolvidas pessoas, que executarão uma série de atividades técnicas especializadas, produzindo um resultado demandado por um cliente, dentro de prazos, custos e qualidades esperadas. O escopo da auditoria precisa ser bem delimitado, as comunicações entre os membros do "projeto" e com os clientes precisam ser bem organizadas. É necessário fazer monitoramento da ação e tomada de ações corretivas.

O projeto de uma auditoria, como qualquer outro, é sujeito a desvios e riscos, que precisam ser monitorados e controlados visando à produção de resultados com qualidade. É preciso, então, que haja na equipe de auditoria um grupo responsável por planejar e gerenciar a atividade de auditoria *per se*. Recomenda-se usar o modelo do Guia PMBOK (PMI, 2004) como orientador geral de planejamento e gestão de projetos, bem como recorrer à norma ISO 19011 (ISO, 2002) acerca do processo de gestão de vários projetos de auditoria integrados, executados ao longo de vários anos na forma de um Programa de Auditoria.

Em suma, o planejamento consiste em amalgamar competências que tenham conhecimento especializado daquilo que se quer auditar e que tenham habilidade e autorização para acesso amplo às diversas fontes de informação necessárias. O planejamento deve produzir, ao final, um plano de gerenciamento de uma auditoria específica, ou de forma coletiva, um plano de gerenciamento do programa de auditoria, que servirá de referência para se executar várias auditorias correlacionadas. A Seção 11 deste texto detalha mais os resultados desta atividade.

2.2 Decisão sobre o Propósito da Auditoria

O segundo passo numa auditoria de segurança da informação é decidir acerca do propósito da auditoria, que pode variar entre verificar situações suspeitas, eventos ou ocorrências que merecem atenção acurada e entre analisar os riscos de segurança a que a organização pode estar exposta (ver seção 7).

Somente uma análise contextualizada, produzida por um auditor poderá indicar qual o melhor propósito da auditoria. Questões específicas sobre propósito de uma auditoria de segurança da informação são descritas na Seção 3.

2.3 Identificação de Objetos e Pontos de Controle

O terceiro passo numa auditoria de segurança da informação compreende analisar o sistema de controle interno do auditado, identificando onde os elementos do controle interno se encaixam nos objetos (ou objetivos) e pontos de controle, descritos de forma genérica no plano de auditoria que foi estruturado na fase de planejamento. Junto a estes objetos e pontos se espera obter evidências a respeito da situação atual da organização, quanto à segurança da informação. Para realizar exames aprofundados é preciso definir o que será auditado, que são os "objetos de auditoria" (OA). Tais objetos são elencados e selecionados de acordo com o contexto e os propósitos da auditoria. Em seguida são elencados "pontos de controle" (PC) para cada objeto de auditoria selecionado. Um PC caracteriza situações específicas que podem ser relacionadas a produtos, processos, procedimentos, eventos ou qualquer outro item observável e relevante para uma auditoria de segurança.

São os objetos de auditoria e pontos de controle itens que, uma vez categorizados, orientam as observações e testes da auditoria.

Destaque

Pontos de controle podem remeter a artefatos físicos, como placas de sinalização e instalações físicas ou artefatos lógicos tais como senhas de acesso a sistemas. Portanto, podem ser físico ou lógicos, tangíveis ou intangíveis. Desvios ou percepções de riscos devem ser examinados para se identificar quais pontos de controle têm relação com esses riscos, definindo seu grau de criticidade para a segurança. A busca de "indícios" e "evidências" de situações de insegurança que merecem atenção e sua correta interpretação pode levar a uma constatação ou achado importante, desde que executados com métodos claros e reproduzíveis, e, se for o caso, com métodos científicos. Veja, por exemplo Lopez (2010).

Modelos como o do COBIT (Control Objectives for Information Technology), descrevem um conjunto de objetivos (objetos) de controle e pontos de controle, típico de Organizações de Tecnologia da Informação. Note que nem todos os objetivos declarados no COBIT 4.1 são relacionados à segurança da informação. O modelo, em sua versão 4.1 (ITGI, 2007), apresenta 318 objetivos de controle agrupados em 34 arquétipos de processos de organização de TI. Os 34 processos organizacionais são agrupados em 4 domínios (Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte de Serviços de TI, além do Monitoramento e Avaliação). Os 318 objetivos de controle são subdivididos (implementados) com pontos de controle (chamados no COBIT de práticas de controle).

2.4 Definição de Técnicas para Obter Evidências e Procedimentos de Controle

Uma vez identificados objetos e pontos de controle é possível elencar as técnicas que serão usadas para a obtenção de evidências que sejam "suficientes, adequadas, relevantes e úteis para a conclusão dos trabalhos" (CPLP, 2009), bem como os procedimentos de controle (também chamados de testes) que serão efetuados junto aos pontos de controle, permitindo a montagem da roteirização detalhada. Estes conceitos são explicados a seguir.

2.4.1 Definição de Técnicas

Segundo o Manual de Controle Interno, criado pelos Organismos Estratégicos de Controlo/ Controle Interno da Comunidade de Países de Língua Portuguesa (CPLP, 2009), são exemplos de técnicas gerais para a obtenção de evidências numa auditoria: a entrevista e o questionário; a análise documental; a conferência de cálculos; a confirmação externa; o cruzamento ou correlação de informações; o exame ou inspeção física; a observação direta envolvendo identificação da atividade a ser observada, observação de sua execução, comparação entre o comportamento observado e os padrões, avaliação e conclusão; o corte das operações e o rastreamento.

Cada técnica tem elo direto com o propósito da auditoria, com a natureza do negócio e com o nível de maturidade da organização em matéria de segurança da informação.

2.4.2 Preparação ou Seleção de Procedimentos de Controle e Testes

Segundo CPLP (2009), os procedimentos de controle são um "conjunto de verificações e averiguações previstas num programa de ação [ex: auditoria], que permite obter evidências ou provas suficientes e adequadas para analisar as informações necessárias à formulação e fundamentação da opinião por parte dos auditores públicos." Os procedimentos de controle são específicos para cada ponto de controle, e descrevem os resultados que devem ser obtidos junto a cada ponto de controle, por meio de testes. Cabe ao auditor escolher que tipo de teste vai realizar, e os testes são estratificados em dois níveis de profundidade: os testes de controle ou observação; e os testes substantivos ou de sondagem.

Os testes de controle são executados por meio de observação do funcionamento dos controles existentes, e visam obter razoável confiança de que os controles estão em efetivo funcionamento e cumprimento.

Cabe ao auditor avaliar o nível de risco tolerado (DUNN, 1991, p.111) para emissão de sua própria opinião com o devido cuidado profissional, a fim de decidir em que momento parar os testes.

Os testes substantivos demandam mais criatividade e esforço do auditor e são aplicados quando há dúvidas acerca da adequação do controle já testado. Várias técnicas, analíticas, de simulação (CHAIM, 2010) ou de ensaio podem ser aplicadas para a realização de testes substantivos de segurança da informação, como teste de vulnerabilidade, testes de penetração. Todas as técnicas, na área de segurança da informação, estão de forma direta ou indireta associadas com a análise e avaliação de riscos de segurança. Segundo ITGI (2000), os testes substantivos visam documentar a vulnerabilidade e os riscos associados ao ponto de controle.

Modelos de auditoria como o antigo manual de auditoria do COBIT 3.0 (ITGI, 2000), o livreto de padrões, guias e procedimentos de auditoria e controle do ISACA (2009) apresentam um extenso conjunto de procedimentos que podem ser empregados em auditoria de segurança da informação, para orientar a execução de testes.

2.5 Montagem da Roteirização Detalhada

A roteirização detalhada de auditoria é o roteiro dos procedimentos e testes que serão ou poderão ser executados pelo auditor. A roteirização é montada para que o auditor use da forma mais eficaz o tempo em que estará no ambiente do auditado, bem como para uniformizar os procedimentos de uma equipe da qual participam diversos auditores.

Cada empresa ou organização de auditoria dispõe de *templates* ou esqueletos de roteirização padronizada, visando agilizar a montagem da roteirização para uma auditoria específica.

A roteirização descreve a sequencia de passos a seguir, e deve ser sucinta e objetiva, para facilitar a execução pelo auditor. Para facilitar a compreensão de conceitos complexos, que muitas vezes são articulados ou referenciados numa roteirização. A roteirização deve fazer referência a documentos mais detalhados e descritivos, como normas, guias e padrões, por exemplo: ISACA (2009) e ITGI (2000).

2.6 Coleta e Registro de Evidências

O sexto passo numa auditoria consiste em coletar e registrar evidências para fins de avaliação, e pode ser organizado em três aspectos.

2.6.1 Coleta de evidências

A coleta é feita no ambiente do auditado. A roteirização detalhada orienta as ações dos auditores em campo durante a coleta e análise de evidências, é em geral elaborada em formato de formulários, em papel ou meio digital, que quando preenchidos auxiliam e sumarizam dados para análise.

2.6.2 Papéis de trabalho

Os papéis de trabalho (documentos de trabalho ou *working papers*) constituem os registros das evidências, ações e decisões realizadas pelo auditor. São preparados no ambiente do auditado, mas são de propriedade do auditor e devem ser arquivados com obediência ao sigilo. São papéis de trabalho: (i) os formulários preenchidos com a execução da roteirização, (ii) os registros de análises e testes de controle e testes substantivos realizados pelo auditor e (iii) outras anotações de interesse. Os papéis de trabalho são a memória de cálculo da execução da roteirização, podendo ser usadas pelo auditor no esclarecimento de dúvidas futuras. As evidências, contidas nos papéis de trabalho, são entrecruzadas com os objetos de auditoria e seus respectivos pontos de controle pertinentes, e desta forma farão parte de uma lista elaborada pelo Auditor como de possível interesse para a análise. Para mais detalhes ver CPLP (2009).

2.6.3 Organização da informação

Para que a informação contida nos papéis de trabalho possa ser útil, inclusive durante a fase de análise, é essencial a organização adequada da documentação e das informações, por meio de instrumentos como índices, tabelas de conteúdo, inclusive porque outros auditores que não participaram da coleta de evidências deverão ter capacidade de avaliar ou participar do trabalho em momento posterior.

2.7 Verificar, Validar e Avaliar Evidências

O sétimo passo numa auditoria consiste em, rigorosamente, verificar, validar e avaliar as evidências obtidas. Muitas delas, que parecem desconectadas em um momento, devem começar a fazer sentido de acordo com os achados ou fatos constatados. Pode-se iterar e voltar a coletar e registrar novas evidências, conforme se mostrem insuficientemente conclusivos os dados coletados. Isto ocorre, sobretudo, quando não se tem experiência com o tipo de auditoria e os objetos de controle auditados. A conexão lógica entre evidências, achados e fatos pode ser estabelecida na roteirização detalhada, mas não deve ser considerada como única fonte de achados. A roteirização serve como instrumento para guiar o julgamento do auditor. Os papéis de trabalho organizado permitem a recuperação de informação.

2.8 Produção de Pareceres e outros Entregáveis

O passo final nesse modelo simplificado de processo de auditoria é a produção de pareceres com recomendações e conclusões do Auditor. Cada passo pode liberar entregas, como mostrado na Figura 2, destacando-se como produtos da auditoria: o plano de auditoria, os relatórios situa-

cionais de auditoria e os pareceres. O Auditor deverá produzir pelo menos um plano de auditoria, um relatório situacional e um parecer para cada engajamento de auditoria (ver Seção 8).

2.9 Acompanhamento Pós-Auditoria

Conforme orienta a norma ISO 19011 (ISO, 2002), o acompanhamento pós-auditoria ocorre sempre no âmbito de um programa de auditoria. É preciso ter bem definidas as competências e a forma de avaliação dos auditores, bem como as atividades que serão realizadas. Esse acompanhamento é uma atividade de gestão, seja para garantir mudanças, seja para sustentar boas práticas que devem persistir. A constituição de um programa de auditoria é descrita na Seção 11 deste texto.

3. Propósitos e Organização da Auditoria

Os conceitos de objetos de auditoria e pontos de controle organizam as situações, ocorrências e evidências que parecem merecer a atenção de uma auditoria de segurança da informação. Seguindo a tradição contábil, as auditorias de segurança são classificadas em três tipos: de gestão, operacional (Cruz, 97) e de conformidade, conforme mostra a Figura 2.

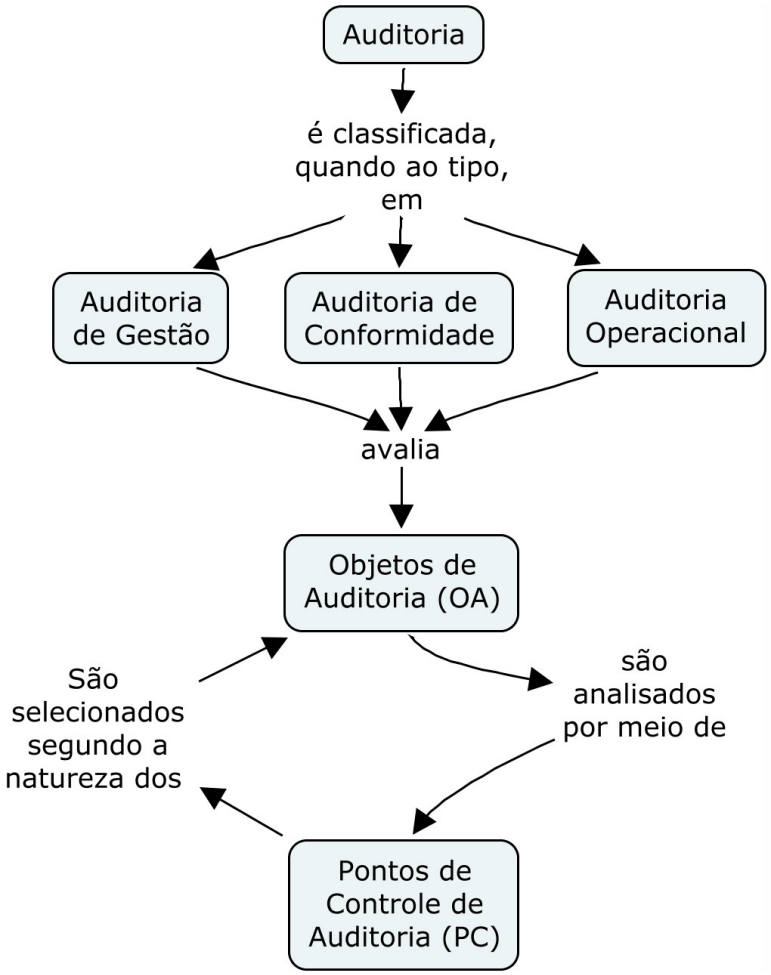

Figura 2. Tipos, objetos e pontos de controle de auditoria.

Cada um dos tipos de auditoria pode seguir métodos diferentes e possui um arcabouço conceitual e necessidades de especialização distintas.

3.1 Auditoria de Gestão

A auditoria de gestão verifica que as ações para acompanhar ou tomar decisões a respeito de itens de segurança estejam em plena execução. Tomando-se por base a Figura 1, a auditoria de gestão está mais relacionada com a avaliação das declarações efetuadas pelo gestor. Mais detalhes na Seção 5.

3.2 Auditoria de Desempenho Operacional ou Auditoria Operacional

A auditoria de desempenho operacional, por sua vez, se baseia essencialmente em indicadores de desempenho e na constatação de que as ações de segurança estão ou não funcionando, além de em descrições que informam sobre quão efetivos e eficazes são os controles para proteger os ativos de informação. Para essa auditoria, além dos pontos de controle, parâmetros de desempenho devem ser definidos para aferição de resultados esperados. Com base na Figura 1, a auditoria operacional se debrucaria sobre o funcionamento dos controles e os efeitos que tais controles produzem sobre a redução dos riscos de segurança da organização. A auditoria de desempenho operacional correlaciona, necessariamente, os controles e os processos que eles controlam (ver Figura 1). Mais detalhes na Seção 6.

3.3 Auditoria de Conformidade

A auditoria de conformidade pode ser realizada sem que o auditado seja solicitado a justificar ou opinar sobre o conteúdo obtido, já que o foco é sobre os controles de segurança. Com base na Figura 1, a auditoria de conformidade buscaria verificar que os controles de segurança que constituem parte do controle interno estão implementados e funcionais. A auditoria de conformidade também tem forte lastro no arcabouço normativo da organização. No caso de questões relacionadas à segurança e ao tratamento da informação no Brasil, o leitor é remetido à compilação produzida por Vieira (2009). Mais detalhes na Seção 7.

3.4 Qual Tipo de Auditoria Empregar?

Os três tipos de auditoria permitem planejar auditorias com enfoque determinado e devidamente contextualizado. Os tipos são úteis para organizar, de forma análoga à auditoria contábil, uma metodologia de trabalho para auditar segurança da informação. Observe, no entanto, que tal divisão é apenas uma convenção. Por exemplo, a auditoria de desempenho operacional poderia ser parte da auditoria de gestão, já que se preocupa com desempenho ou resultados. Destaca-se aqui o fato de que auditorias operacionais avaliam "o como" a segurança é implementada, enquanto que a auditoria de gestão destaca as decisões gerenciais e as prioridade resultantes que conduzem da melhor maneira possível essas operações de segurança.

Para cada ação de auditoria, objetos de auditoria devem ser demarcados, conforme mostra a Figura 2. Os pontos de controle devem ser selecionados segundo a natureza do objeto de auditoria. Considerando que um objeto de auditoria funciona normalmente dentro do comportamento esperado, por exemplo, uma política de segurança que é seguida, os pontos de controle correspondentes produzirão as informações esperadas para esse objeto. Todo o resultado culminará em um relatório de auditoria e um parecer com as devidas considerações e conclusões, conforme já mencionado.

Ao se trabalhar com segurança de informação se deve considerar as três atributos clássicos da segurança: integridade, disponibilidade e confidencialidade (ou sigilo). A verificação de integridade permite descobrir se a informação foi produzida de forma incoerente com a realidade, ou alterada por ações que apontam para possíveis fraudes que podem trazer impacto à organização. A verificação de disponibilidade permite avaliar possíveis riscos que emergem da indisponibilidade frequente de ativos de informação sensíveis. A verificação de confidencialidade, ponto de controvérsia na administração pública, merece muita atenção. Permite identificar o risco de que a informação seja acessada por agentes não autorizados, quando naquele determinado momento ela não deveria ser de acesso ao público. Existem um conjunto razoável de decretos e instruções (ver Anexo I) que demonstram uma crescente preocupação com essa questão. Essas três verificações devem permear os três tipos de auditoria, quando abordando segurança da informação.

4. Arcabouço de Roteirização de uma Auditoria

Tradicionalmente a auditoria tem o propósito de verificar categorias de controle gerais ou específicas de objetos de auditoria (TCU, 98). Os controles gerais são aqueles que de alguma forma aparecem com propriedades ou procedimentos gerais e que sempre são observados, por exemplo: controle de acessos físicos a instalações. Os controles específicos são aqueles que apontam para um determinado elemento de atenção, por exemplo, acesso de usuários a um determinado banco de dados.

Uma vez que a quantidade de informação a ser coletada pode facilmente fugir ao controle do auditor e exceder os custos e o tempo estimados, é preciso recorrer sempre a uma roteirização de auditoria em mãos.

Embora sejam possíveis outros tipos de auditoria para formatar uma roteirização, nos deteremos nos três tipos já descritos: de gestão, operacional e de conformidade.

Para cada tipo a roteirização terá um conjunto de objetos de auditoria e seus respectivos pontos de controle, ou seja, eventos, acontecimentos, ações, produtos, espaços ou qualquer coisa que mereça atenção em termos de segurança da informação e que seja de interesse auditar, dada a sua criticidade para os negócios da organização. O Quadro 1 mostra um exemplo simples de organização de pontos de controle para um objeto de auditoria chamado "política de segurança da informação."

Quadro 1. Trecho de roteirização para o objeto de auditoria "Política de Segurança da Informação".

Sequência de auditoria	Objeto(s) de auditoria	Pontos de Controle
	Política de Segurança da Informação	objetivo
		recursos
		riscos
		custos (análise econômica)
		responsabilidades
		perfis
		requisitos de acesso
		classificação de documentos
		ferramentas de segurança etc.

A sequência de auditoria do Quadro 1 corresponde aos pontos de controle de auditoria que serão verificados, segundo uma estratégia expressa em uma roteirização de auditoria. A Figura 3 mostra uma esquematização de um programa de auditoria, proposto aqui para ilustrar como uma auditoria de segurança da informação poderia ser organizada. A roteirização de auditoria lança mão dos três tipos de auditoria, conforme os objetos de auditoria melhor se acomodam aos propósitos de cada tipo.

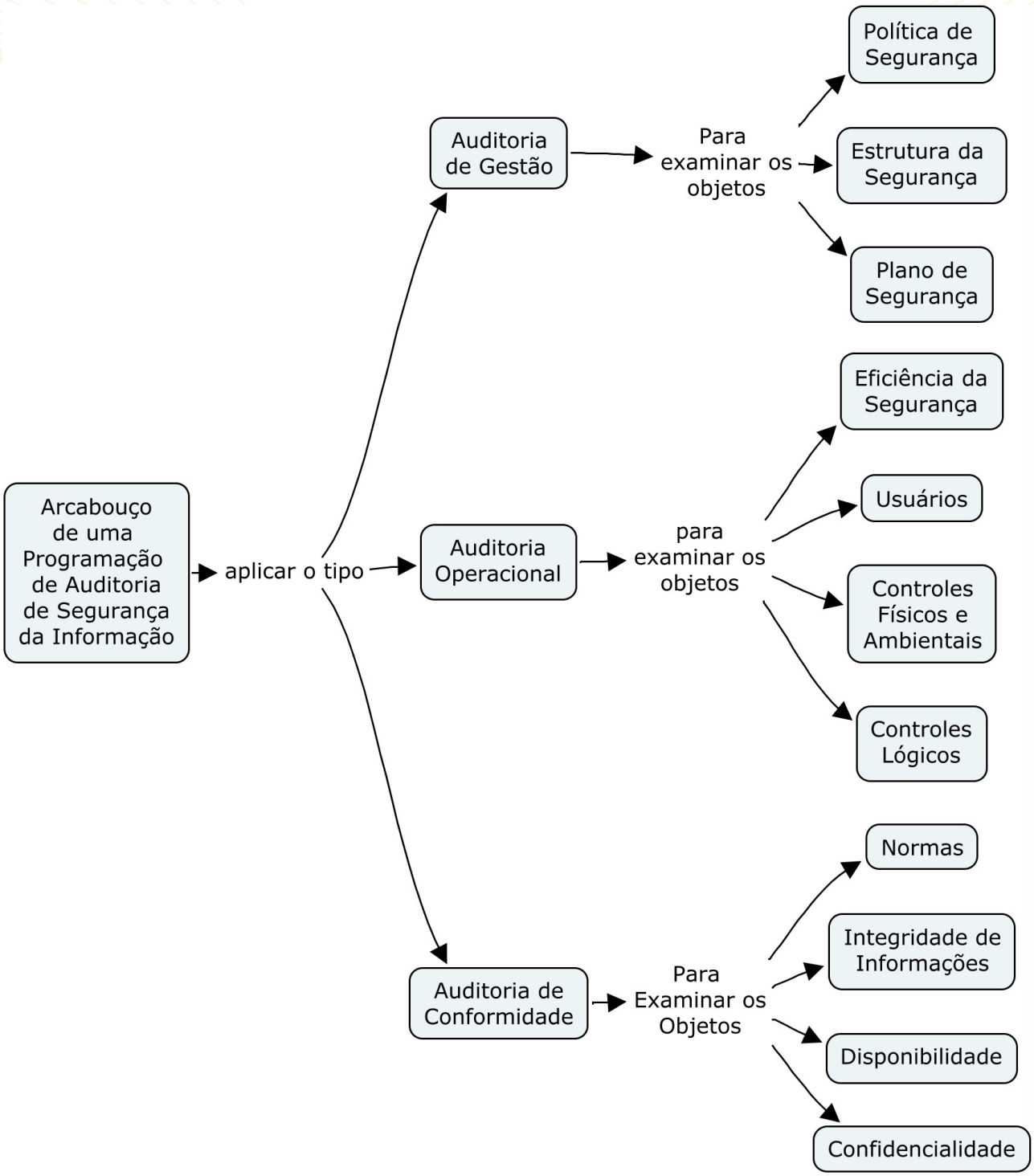

Figura 3. Um arcabouço de roteirização de auditoria de segurança da informação.

Na auditoria de gestão o foco é a estrutura organizacional e tópicos como segregação de funções, existência de política de segurança da informação e adequabilidade dos planos de segurança. A parte da documentação, como parte da política, diz respeito mais à forma de arquivamento, convenções de títulos para documentos e existência de controle de versões e revisões.

No caso da auditoria operacional, o interesse pode ser na segurança das operações implantadas e nos recursos físicos que suportam essas operações, tais como as instalações, equipamentos e dispositivos de redes. Também a segurança lógica pode ser avaliada com auditoria operacional e compreende avaliação do funcionamento dos sistemas, programas e processos com foco nos dados gerados e nas informações produzidas. A questão dos usuários também é parte dessa auditoria, pois se preocupa com o acesso de pessoas às instalações, a sistemas, a programas ou qualquer recurso relacionado com os ativos de informação. Ainda na auditoria

operacional se tem a preocupação com a eficiência e eficácia das operações, cuja inobservância compromete os resultados aumentando os riscos.

No caso da auditoria de conformidade, os objetos de auditoria têm como propósito garantir a integridade, a disponibilidade e a confiabilidade desses ativos conforme preconizam os padrões e especificações determinados pela e para a organização dos controles em prática. Pontos de controle requerem observância de regras que estão mais sujeitas a questões de consistência da regras ou de aderência das ações de segurança em face do que está determinado nas regras. Nas seções seguintes são apresentados detalhes de cada tipo de auditoria.

5. Auditoria de Gestão em Segurança da Informação

Como já abordado, a Auditoria de Gestão tem o propósito de verificar como as atividades de gestão da segurança da informação estão sendo realizadas. Consiste basicamente em verificar que os processos de segurança e suas atividades foram implantados plenamente e que as metas de segurança traçadas estão sendo alcançadas. Visa também verificar as atividades de apoio que lidam com incidentes, ameaças ou vulnerabilidades já identificadas; subsidiar novas ações necessárias ao atendimento de demandas; e alterar os controles previamente definidos. Por exemplo, investigar os serviços de atendimento de um *help desk* é tarefa da auditoria de gestão.

O que se quer alcançar com esse tipo de auditoria é a confirmação de que os procedimentos previstos no plano de segurança (Ver Seção 8) estão presentes ou, se não estão, quais foram os desvios que levaram a essa ausência. Em caso de desvios, deve-se relacionar o que ou quem está fora das diretrizes definidas no plano de segurança frente a um padrão de desempenho esperado pela gestão da segurança. Alguns objetivos de auditoria de gestão listados abaixo foram adaptados de Imoniana (Imoniana, 2005) e do manual de sistemas do TCU (TCU, 98), a saber:

- Estrutura organizacional
- Política de segurança
- Documentação
- Cultura de segurança
- Pesquisa sobre incidentes
- Sistema de segurança
- Registros de auditoria
- Plano diretor de tecnologia da informação (PDTI)

Estes objetivos são detalhados a seguir.

5.1 Estrutura Organizacional

Não é possível implantar segurança da informação sem que haja uma estrutura organizacional apropriada para tal. Um primeira providência é se preocupar com segregação de funções. Quem executa uma ação não pode ser aquele que controla os estágios dessa ação. O manual de auditoria de sistemas do TCU (TCU, 1998) enumera uma lista de elementos críticos (pontos de controle) para avaliação dos controle organizacionais, a saber:

- 5.1.1 As unidades organizacionais responsáveis por segurança devem ser bem definidas, com níveis claros de autoridade, responsabilidades e habilidades técnicas necessárias para exercer os cargos.
- 5.1.2 Atividades dos funcionários envolvidos com segurança devem ser supervisionadas e controladas através de procedimentos padrões devidamente documentados com políticas claras de seleção, treinamento e avaliação de desempenho desses profissionais.
- 5.1.3 Política de segregação de funções e controles de acesso deve ser constantemente perseguida para garantir na prática a idoneidade dos processos.
- 5.1.4 Indicadores de gestão para auscultar os recursos computacionais que estão sob procedimentos de segurança devem ser estabelecidos. Mecanismos de segurança não podem provocar mau desempenho dos recursos.

Note que a lista apresentada não é exaustiva.

5.2 Política de segurança para a organização

Sem uma política de segurança da informação (PSI) discutida por todos os setores, qualquer procedimento de segurança será aleatório e, provavelmente, irá entrar em conflito com outras iniciativas. A PSI pode trazer referências explícitas aos padrões definidos para os ativos de informação. Note que o DSIC/GSIPR usa o termo PSIC – Política de Segurança da Informação e Comunicações (DSIC, 2008) para a constituição de um documento de política de segurança da informação na Administração Pública Federal. Segundo a ISO/IEC 27002:2005, a política de segurança da informação deve contemplar os seguintes pontos de controle:

- 5.2.1 Objetivos, metas, escopo e a relevância da política de segurança da informação para toda a organização devem ser estabelecidas e positivadas em documentos;
- 5.2.2 Declaração da alta direção de que está compromissada com o que está definido na política deve ser de conhecimento de todos;
- 5.2.3 É preciso saber se existe um alinhamento da política de segurança da informação com os objetivos de negócio, no caso, com a missão institucional e a legislação;
- 5.2.4 Devem ser definidas responsabilidades gerais e específicas a respeito da segurança da informação, seja para indivíduos, seja para instâncias colegiadas: comissões, comitês, grupos de trabalho etc.
- 5.2.5 A política deve conter referência a documentações necessárias para apoiá-la, o que inclui normas e regras estabelecidas na legislação.
- 5.2.6 A política deve explicar os requisitos de segurança da informação, incluindo a conformidade com a legislação, regulamentos e contratos.

Note que a lista apresentada não é exaustiva.

5.3 Documentação atualizada

Documentos devem ser classificados e versionados para que seu conteúdo e finalidade estejam sob controle. Novas normas devem ser catalogadas, discutidas e disseminadas, principalmente aquelas que têm referências legais. Na questão do sigilo de documentos, convém acompanhar se os critérios definidos estão sendo implementados e se são aderentes à legislação em vigor.

5.4 Cultura de segurança

Devem ser produzidos materiais para divulgação e disseminação da cultura de segurança da informação. É um trabalho que possibilita internalizar entre todos os atores a necessidade de constante atenção aos ativos de informação, como uma forma de proteger o patrimônio e o próprio negócio público ou privado. Deve-se aplicar o princípio do "need to know" como a regra geral de segurança (Organisation for Economic Co-operation and Development, 2002). Este princípio indica que uma informação deve ser acessível apenas àqueles que tem necessidade de conhecê-la. Cabe ressaltar a controvérsia que segue este preceito quando tratando de informação gerida por órgão público, em contraste com o preceito da transparência.

5.5 Pesquisa sobre Incidentes

A organização deve providenciar constantes pesquisas sobre incidentes e falhas de segurança. Faz parte da gestão da segurança promover uma constante investigação nos ativos de informação, formulando novas programações de auditoria. Essa atividade também deve promover novas soluções de segurança para as novas ameaças e vulnerabilidades descobertas, bem como avaliar se é necessária a continuidade de aplicação de controles antigos.

5.6 Sistema de Segurança

O sistema de segurança da informação deve funcionar de acordo com a política de segurança implantada, e estar em constante atualização. Ver ISO/IEC 27001 (ABNT, 2006).

5.7 Registros de auditoria

Manter registros para fins de auditoria é uma atividade crucial para que exista auditoria. A ISO/IEC 27002:2005 (item 10.10.1) lista vários objetivos de controles para tecnologia da informação, adaptados na sequência abaixo, a saber:

- 5.7.1 Todos os usuários devem ser identificados. Nesse caso, o que mais interessa é registrar o acesso de novos usuários e observar mudanças no *status* de antigos usuários.
- 5.7.2 Cada detalhe de eventos-chave, como a entrada de pessoas, sejam nas instalações sejam em sistemas é registrado com hora e data. A saída de pessoas de instalações críticas também deve ser registrada igualmente.
- 5.7.3 Alterações em configurações dos sistemas devem ser registradas. Uma ferramenta de gestão de mudanças e versionamento poderá capturar essas alterações.
- 5.7.4 O acesso a arquivos nos bancos de dados precisa ser registrado. Uma forma de facilitar a auditoria é ter um único administrador do banco ou muito poucos. Qualquer problema pode ser rastreado de volta ao seus autores ou responsáveis.
- 5.7.5 Cada pessoa deve ter privilégios de acesso bem definidos. O uso desses privilégios deve ser registrado e acompanhado.
- 5.7.6 Todas as tentativas de acesso a qualquer objeto de auditoria que foram rejeitadas devem ser registradas para verificação.

Note que a lista apresentada não é exaustiva.

5.8 Plano Diretor de Tecnologia da Informação (PDTI)

Pressupõe-se que o PDTI foi previsto na política de segurança como fonte privilegiada de objetos de auditoria a serem tratados. A Instrução Normativa 04/2008 da SLTI/MP define características de um PDTI na APF. Assim o plano deve:

- 5.8.1 Prever que a segurança dos dados armazenados e em fluxo sejam previstas nos sistemas desde o início
- 5.8.2 Apresentar parâmetros de segurança para os sistemas de informação a serem desenvolvidos ou mantidos e os respectivos processos dos quais eles farão parte. Para mais detalhes ver Fernandes (2010a) e Veneziano (2010).
- 5.8.3 Estabelecer os critérios para aquisição de hardware, software e serviços. Neste caso o documento deve fazer referência a normas expedidas pelo governo federal. Para mais detalhes ver Rodrigues (2010).
- 5.8.4 Definir quais perfis de recursos humanos são necessários e a quantidade de pessoas para os projetos previstos no plano.
- 5.8.5 Apresentar o orçamento do custo da área de tecnologia de informação apontando o que é custo de apoio e o que é finalístico e qual o percentual a ser investido em segurança.
- 5.8.6 Definir as prioridades de segurança dos sistemas ou processos a serem automatizados com um cronograma estimativo. Para mais detalhes ver Fernandes (2010b)
- 5.8.7 Observar se os objetivos dos sistemas de informação estão alinhados com os objetivos estratégicos e de segurança da organização.

- 5.8.8 Padronizar relatórios gerenciais e sumários de informações para subsidiar a cúpula da organização em seus processos decisórios.

Note que a lista apresentada não é exaustiva.

Os pontos de controle apresentados não esgotam todas as possibilidades. O importante é ficar claro que uma auditoria de gestão permite verificar que a segurança está sendo administrada a contento. A ideia é manter uma gestão qualificada sem a qual não tem sentido montar um sistema de segurança da informação, pois são muitos e diversos os instrumentos e os controles que são utilizados. O TCU (1998) chama os controles dessa auditoria de controles organizacionais. Aquele Tribunal incorpora como pontos de controle a política de segurança, procedimentos e estruturas organizacionais, só para citar alguns. Também se inclui nessa auditoria as pessoas que fazem parte dos processos de gestão da segurança. Controles para admissão de pessoas podem ser encontradas também na ISO/IEC 27002:2005 e podem se adotados como parte da auditoria de gestão. Observar que a 27002, na realidade, procura, de forma coordenada com a ISO/IEC 27001:2006, montar um Sistema de Gestão de Segurança da Informação (SGSI), conceito que também é compartilhado pelos autores, mas que só é possível em organizações com nível elevado de maturidade em segurança.

6. Auditoria de Desempenho Operacional de Segurança da Informação

A Auditoria de Desempenho Operacional visa verificar principalmente parâmetros de eficiência, eficácia e efetividade, mas não está restrita a isso. Conforme definido no Manual de Auditoria de Natureza Operacional do TCU (2000), o objetivo desta auditoria é: "*examinar a ação governamental quanto aos aspectos da* economicidade, eficiência e eficácia*, enquanto a avaliação de programa busca examinar a* efetividade *dos programas e projetos governamentais.*". Na medida que os pontos de controles são implantados, a auditoria de desempenho operacional deve se certificar de que os mesmos são efetivos (resolvem o problema) diante do que se espera em termos de nível de segurança. Observe que a auditoria operacional também se preocupa se os controles que se definiu são robustos frente às vulnerabilidades e ameaças diagnosticadas numa análise/avaliação de riscos.

O sentido que este texto dá à auditoria de desempenho operacional é que esta faz um exame detalhado das operações de segurança implantadas na organização. Para apresentar alguns controles, sem exaurir as possibilidades, se usa uma categorização clássica que os autores consideram ainda útil, dada a quantidade de documentação de melhores práticas e propostas diversas, e baseada nas áreas de: (i) segurança física, (ii) segurança lógica, (iii) segurança de dados, (iv) segurança de usuários, (v) segurança de redes, (vi) eficiência da segurança e (vii) eficácia da segurança. Usamos como base a estrutura da Figura 2.

6.1 Segurança Física

Corresponde às seguintes diretrizes para controle de acesso a objetos que direta ou indiretamente se relacionam com os ativos de informação. Fonte: ISO/IEC 27002 (ABNT, 2005), com adaptações. Ver também Vidal (2010) e Araújo (2010).

- 6.1.1 É preciso definir claramente os perímetros de segurança. Esse perímetro precisa ser revisto para sempre cobrir o espaço físico onde se encontram ativos de informação que podem ser alvo de ameaças.
- 6.1.2 É preciso construir uma área de recepção para que se tenha um acesso controlado às instalações da organização, considerando uma ameaça qualquer acesso não autorizado por outras entradas ou saídas devidamente restritas.
- 6.1.3 É preciso implantar barreiras físicas para impedir acesso não autorizado a perímetros de segurança ou a áreas específicas demarcadas como tal.
- 6.1.4 Todas as portas corta-fogo devem ter alarmes e o material devem estar de acordo com normas internacionais de resistência a incêndios.
- 6.1.5 Todas as salas devem ter sistema de detecção de intrusos e todas as entradas e saídas das instalações devem estar o tempo todo protegidas.
- 6.1.6 As instalações de processamento de informação gerenciadas pela organização devem ficar fisicamente separadas daquelas que são gerenciadas por terceiros.
- 6.1.7 Devem existir procedimentos especiais para segurança física do parque de servidores:
  - 6.1.7.1 Controle de acesso a instalações dos computadores principais e seus periféricos, somente para pessoas autorizadas.
  - 6.1.7.2 Controle de acesso a dispositivos de redes, tais como roteadores, *switches*, Hubs, com sistema de detecção de intrusos.
  - 6.1.7.3 Controle de acesso a servidores, somente por administradores.
- 6.1.8 Devem existir procedimentos especiais para controle de acesso a *backups,* em dispositivos magnéticos ou não, devem ser implantados e rigorosamente controlados.
- 6.1.9 Deve existir controle sobre armazenamento em *pendrives* ou qualquer dispositivo móvel por meio de alerta de segurança contra cópias não autorizadas.

- 6.1.10 Todas as comunicações com os dispositivos que acessam a rede interna da organização devem ser criptografadas utilizando os protocolos adequados.

Note que a lista apresentada não é exaustiva.

6.2 Segurança Lógica

A segurança lógica compreende diretrizes de controle para os ativos intangíveis que incluem sistemas e informação. Para mais detalhes para desenvolvimento de sistemas seguros, ver Holanda e Fernandes (2011), OWASP (2011), Imoniana (2005), Mair, Wood e Davis (1978), além de Schmidt, Alencar e Villar (2007). São listados alguns pontos de controle, a saber:

6.2.1 Sistemas de informação

A auditoria de sistemas visa verificar problemas de processamento de dados e se as informações produzidas por esses sistemas são corretas e oportunas. Deve-se então:

- 6.2.1.1 Implementar sistemas corporativos utilizando a linguagem LL (deve ser escolhida como padrão) e o banco de dados BD (deve ser escolhido como banco corporativo).
- 6.2.1.2 Implementar páginas WEB utilizando a última versão atualizada de *javascript* ou linguagem WEB orientada a objetos (apenas exemplos).
- 6.2.1.3 Absoluta atenção a códigos que podem conter vulnerabilidades que permitem invasão, por exemplo, por meio de *SQL injection,* pois devem ser controlados.
- 6.2.1.4 Todos os sistemas, programas, *scripts*, folhas de estilo etc devem ser versionados e com autoria devidamente registrada.
- 6.2.1.5 Processamento (condicional): verificar a criação de novos dados (registros, objetos etc).
- 6.2.1.6 Processamento (cálculo): verificar o desempenho dos cálculos matemáticos nos sistemas, pois podem gerar informações erradas.
- 6.2.1.7 Processamento (cálculo): verificar mudanças de valores em tabelas de banco de dados ou arquivos.
- 6.2.1.8 Processamento (atualização): verificar mudanças de dados em arquivos ou banco de dados por meio de inclusão, atualização ou eliminação.
- 6.2.1.9 Processamento (condição): examinar dados usando lógica ou testes de condições, para identificar similaridades ou diferenças.
- 6.2.1.10 Transcrição: verificar cópia de dados de uma mídia para outra colocando o devido rótulo com classificação de segurança.
- 6.2.1.11 Ordenamento: colocar itens de dados em ordem ou sequência.
- 6.2.1.12 Transmissão: movimentação de dados de um lugar para outro via meios de comunicação disponíveis.
- 6.2.2 Verificar que os programas de computador são concebidos de acordo com metodologias de roteirização que favorecem a construção de sistemas seguros, com especial atenção a software para a WEB (OWASP, 2011).
- 6.2.3 Assegurar que programas ou sistemas novos não sejam colocados em produção sem teste e homologação. e
- 6.2.4 Verificar que as rotinas de funcionamento de procedimentos de teste de sistemas e programas estão em pleno uso.

Note que a lista apresentada não é exaustiva.

6.3 Acessos dos Usuários

Sistemas de informação podem ser acessados por um grande número de usuários que precisam ser controlados para responsabilização em caso de danos às pessoas e ao patrimônio público. São candidatos a pontos de controle:

- 6.3.1 Credenciais únicas que devem ser atribuídas a usuários individuais. Credenciais devem conter uma combinação de alguns requisitos a serem atendidos pelo usuário, como segue:
  - 6.3.1.1 Identificar quem é o usuário (nome, ID etc).
  - 6.3.1.2 Verificar alguma coisa que o usuário sabe (código secreto, senha).
  - 6.3.1.3 Verificar onde o usuário está (reconhece local do usuário). e
  - 6.3.1.4 Verificar alguma coisa que o usuário tem.
  - 6.3.1.5 Verificar alguma coisa que o usuário é (biometria).
- 6.3.2 Implantação de dispositivos biométricos para verificação automática de identidade baseados em características físicas do usuário como digitais, iris etc.
- 6.3.3 Deve existir uma única forma de acesso lógico aos sistemas de uma organização, mesmo que sejam sistemas diferentes, integrados ou não.
- 6.3.4 Cada usuário deve ser responsabilizado por aquilo que realiza com suas credenciais. Isso inclui inclusive técnicos que alterem configurações de hardware e software (ver texto complementar a seguir).
- 6.3.5 A área de segurança da informação deve ser informada a respeito dos desligamentos dos funcionários para que suas credenciais sejam desativadas.
- 6.3.6 A área de gestão de pessoas deve saber sobre os usuários que acessam os seus dados e o níveis de acesso atribuídos a esses usuários.
- 6.3.7 Acesso a programas utilitários que possam modificar dados corporativos deve estar absolutamente estrito a pessoas da área de Tecnologia e ao usuário responsável.
- 6.3.8 Devem ser realizadas varreduras periódicas de atributos de acesso, principalmente sobre aqueles usuários que estão com acesso ilimitado a um ou mais ativos de informação.

Note que a lista apresentada não é exaustiva.

Texto Complementar | Ministério da Educação, e-MEC, Termo de Compromisso de Usuário

Código de Conduta do Usuário

Efetuo, por meio deste compromisso, a solicitação de acesso ao sistema E-MEC, assumindo os encargos legais decorrentes do compromisso firmado e declaro estar de acordo com as seguintes condições que integram o presente termo: é de minha exclusiva responsabilidade a observância dos prazos para inserção de dados ou demais providências de sua competência; são de minha exclusiva responsabilidade as informações inseridas no sistema, assumo-as como verdadeiras, nos termos do art. 219 do Código Civil, assim como o uso do acesso ao sistema, incluindo qualquer transação efetuada, não cabendo ao provedor do sistema responsabilidade por eventuais danos decorrentes do uso indevido do acesso, ainda que por terceiros; o acesso ao sistema dado, mediante atribuição de identificação e senha, é pessoal e intransferível, salvo os casos de delegação admitidos, conforme disposto nos Arts. 12 a 14 da Lei no 9.784, de 1999; estou obrigado a informar imediatamente ao provedor do sistema a perda da chave de acesso ou da senha ou a quebra de seu sigilo para bloqueio do acesso; deverei dar o tratamento adequado às informações acessadas, com atenção às restrições sobre sigilo, mantendo-o quanto às informações obtidas sobre a instituição e seus cursos, evitando conceder entrevistas ou outras formas de exposição na mídia e utilizarei as informações coletadas somente para os objetivos da fase de tramitação do processo para a qual foi designado; assumo a responsabilidade pelos atos praticados mediante o acesso ao sistema, ainda que por terceiros até que o acesso seja bloqueado, tendo em vista as penalidades em caso de prática de atos ilícitos previstos na legislação penal e cível; tenho conhecimento de que os dados inseridos no sistema serão de conhecimento público, com exceção dos dados discriminados nos incisos III e IV do art. 16 do Decreto no. 5.773, de 2006, com o que concordo expressamente (...)

6.4 Segurança de dados

Devem ser examinadas diversas possibilidades de violação de dados quanto à sua integridade, disponibilidade e confidencialidade.

- 6.4.1 Deve existir um grupo muito restrito de administradores de banco de dados, cujas ações devem ser monitoradas.
- 6.4.2 Deve existir uma estratégia definida para utilização dos bancos de dados por sistemas de informação, pessoas ou programas.
- 6.4.3 Se deve manter rigoroso sigilo sobre informações sensíveis da organização, utilizando recursos de proteção automática ou manuais para dados operacionais sensíveis.
- 6.4.4 Ocorrência de perda de dados deve ser investigada, pois pode ser sintoma de ameaças aos ativos de informação: sabotagens, invasões, engenharia social etc.
- 6.4.5 Ocorrência de destruição de arquivos deve ser investigada, pois pode significar imprudência do responsável ou até sabotagem e fraudes.
- 6.4.6 Verificar ocorrência de falhas de hardware que provoquem erros de processamento, de informações erradas ou de distorção de integridade de dados.
- 6.4.7 Erro de entrada de dados. Esse é um dos eventos relacionados também a usuários. Os programas de entrada de dados permitem erros que "sujam" os bancos de dados tendo reflexo na qualidade das informações produzidas. A elevada superfície de exposição de aplicações de governo eletrônico à Internet demanda que este ponto de controle seja profundamente investigado.
- 6.4.8 *Backups* periódicos dos dados que devem ser realizados de acordo com um planejamento prévio e critérios diferenciados para diferentes graus de sensibilidade das informações.
- 6.4.9 Contas de usuários que acessam diretamente os bancos de dados ou por meio de utilitários em situação privilegiada devem ser observadas.
- 6.4.10 Atualizar os bancos de dados com as novas versões mais seguras. Ficar atento à lista de vulnerabilidades de cada versão, por meio de consulta periódica a bases de dados de vulnerabilidades.

Note que a lista apresentada não é exaustiva.

6.5 Eficiência da Segurança

Parâmetros de medida de eficiência podem indicar problemas de segurança ou sua iminência. Na lista abaixo são apresentados fortes candidatos a ponto de controle.

- 6.5.1 Tempo médio para reparo (MTTR - *Mean Time to Repair*). O MTTR identifica o lapso temporal médio entre o momento em que surgem a indisponibilidade de um serviço e o tempo que o serviço foi restaurado. O MTTR é um indicador de desempenho em horas e valores altos podem ser responsáveis por insatisfações gerais durante a prestação de serviço.
- 6.5.2 Tempo médio entre falhas (MTBF – *Mean Time Between Failures*). Indicador clássico, que consiste em identificar o tempo médio de disponibilidade dos serviços, sem a ocorrência de falhas. É possível assim medir o grau de disponibilidade dos ativos.
- 6.5.3 Tempo médio entre o aparecimento de um problema ou incidente e sua comunicação ao *Service Desk*. É preciso auditar os procedimentos que levam os problemas e incidentes a serem conhecidos pela organização. Esse tempo pode ser reduzido a zero se existirem sistemas automatizados que os detectam, usualmente chamados de monitores.
- 6.5.4 Razão entre a quantidade de vezes que um procedimento operacional de segurança foi realizado e quantidade de vezes que o mesmo deveria ter sido executado.

Permite verificar que os procedimentos operacionais estão sendo executados na periodicidade definida.

- 6.5.5 Percentual de sistemas cujos requisitos de segurança não estão sendo atendidos. Permite avaliar o sucesso da implantação de normas e políticas de segurança da informação e remete, para cada caso, no aprofundamento do porquê das regras não estarem sendo atendidas.
- 6.5.6 Percentual de incidentes causados por violações ou falhas de segurança. Analisar o volume de incidentes provenientes de problemas na implantação de políticas de segurança. Como será abordado na Seção 11, a própria auditoria pode ser objeto de auditoria.
- 6.5.7 Percentual de indicadores incorretos por serviço de segurança. Visa verificar que o nível de erro dos indicadores de cada serviço de segurança implantados na organização.
- 6.5.8 Dados os indicadores de segurança estabelecidos, um indicador de eficiência é calcular o tempo médio para análise dos indicadores dos serviços, a fim de verificar o desempenho da atividade.
- 6.5.9 Quantidade de indicadores avaliados no período. Verificar o cumprimento da análise de indicadores pela equipe de segurança da informação.
- 6.5.10 Quantidade de propostas de melhoria de serviços produzidos no período. Verificar a execução da atividade de análise de serviços e propostas de melhoria.
- 6.5.11 Quantidade de duplicidades de procedimentos e de resultados etc.

Note que a lista apresentada não é exaustiva.

6.6 Eficácia da Segurança

A eficácia da segurança diz respeito aos resultados esperados definidos no plano segurança em curso. O objetivo é saber se os ativos de informação estão mais ou menos seguros após implantados os controles de segurança da informação. São candidatos a ponto de controle:

- 6.6.1 Quantidade de informações geradas por usuário em relação a um nível esperado de volume de informações para um perfil específico.
- 6.6.2 Tempo médio de atendimento após um alarme de segurança ser disparado, envolvendo efetivação dos procedimentos de contingência ou de providências predefinidas.
- 6.6.3 Tempo médio para a solução de um problema de segurança, provida pela equipe de segurança da informação.
- 6.6.4 Percepção do usuário a respeito dos mecanismo de segurança implantados, enquanto garantia de segurança de que seus dados não estão sendo violados.

Note que a lista apresentada não é exaustiva.

6.7 Segurança de redes

A segurança de redes se preocupa com os riscos a segurança das redes de comunicação. Foram adaptados de Nakamura (Nakamura, 2009) os seguintes pontos de controle ou recomendações:

- 6.7.1 Acesso a computadores e a sistemas de informação utilizando celular deve ser protegido com a última versão de algoritmo de encriptação.
- 6.7.2 Redes sem fio devem ser protegidas usando o protocolo mais seguro e já relativamente bem testado no mercado.
- 6.7.3 Acesso remoto a computadores protegido com protocolo de segurança Secure Socket Layer (SSL) ou seu equivalente mais atualizado.

- 6.7.4 Acesso remoto a serviços não públicos é absolutamente controlado e somente para sistemas específicos.
- 6.7.5 Redes virtuais privadas (VPN) devem usar IPSEC.
- 6.7.6 Acesso a serviços críticos devem ser baseado no uso de certificado digital.
- 6.7.7 Configuração do firewall deve ser controlada.
- 6.7.8 Controle de acesso lógico ao ambiente.
- 6.7.9 Proteção dos dados armazenados na rede por meio de criptografia.
- 6.7.10 Proteção de cabos da rede. Necessidade de cuidados com o acesso de pessoas a quadros de rede ou caixas de proteção (Schmidt et alli, 2006).
- 6.7.11 Rotinas adequadas de proteção e controle do fluxo de dados com devida observância da sazonalidade dos eventos.
- 6.7.12 Uso de protocolos adequados à criticidade dos sistemas de informação.
- 6.7.13 Existência de analisadores de protocolos adequados para verificação de uso de portas.
- 6.7.14 Equipamentos de rede catalogados e protegidos fisicamente.

Novamente cabe destacar que a lista não é exaustiva, e que a todos os itens deve ser dada atenção conforme as necessidades de proteção da organização. Cada objeto de auditoria pode ser desmembrado em pontos de controle ainda mais detalhados. A Seção 9 apresenta um modelo de investigação desses objetos com seus respectivos pontos de controle, detalhando ainda mais o modelo da Figura 2.

7. Auditoria de Conformidade

A Auditoria de Conformidade em segurança da informação tem o propósito de verificar que as informações produzidas pela organização, seja por sistemas computacionais ou por registros manuais, estão em conformidade com os padrões de segurança definidos em documentos normativos reconhecidos. Dado que se está tratando de organizações que se apoiam fortemente em sistemas computacionais, esse tipo de auditoria centra em procedimentos para verificar que recursos tecnológicos, ou que as informações produzidas por sistemas computacionais ou armazenadas em banco de dados estão em conformidade com os normativos. Observe que se inclui, no caso do serviço público, o arcabouço legal referente à área de segurança (ver anexo I).

Segundo Juran e outros (1990), quando tratando de auditorias na área da qualidade, uma auditoria de conformidade é uma auditoria que examina se aquilo que está sendo auditado está de acordo com as especificações de produtos e serviços. Esse texto segue analogamente a mesma ideia, no sentido de que a auditoria de conformidade examina se os objetos de auditoria de segurança da informação estão de acordo com as especificações dos serviços ou bens relacionados à segurança da informação, desde que essas especificações, materializadas em normas, estejam homologadas pela gestão. Tais especificações podem estar em qualquer documento que tenha como propósito a padronização, o que inclui documentos externos à organização pública.

7.1 Normas da Administração Pública Federal

A política de segurança de informação é o documento mais importante de referência para a auditoria de conformidade, mas está subordinada aos decretos e portarias expedidas por órgãos públicos que tem função normativa, como: Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República; Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento Orçamento e Gestão; Controladoria Geral da União; Tribunal de Contas da União, além do arcabouço de Leis e Decretos, compilados por Vieira (2009) e ABIN (2011), a título de exemplo.

7.1.1 Normas do DSIC – Departamento de Segurança da Informação e Comunicações

O DSIC/GSIPR, em especial, produziu diversas normas relacionadas com a gestão da segurança da informação nos últimos três anos e que são:

Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que "Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências".

- 01/IN01/DSIC/GSIPR, de 13 de outubro de 2008, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.
- 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008, que define a metodologia de gestão de segurança da informação e comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta.
- 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, que estabelece diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (POSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
- 04/IN01/DSIC/GSIPR, de 14 de agosto de 2009, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF.

- 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
- 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009, que estabelece diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
- 07/IN01/DSIC/GSIPR, de 6 de maio de 2010, que estabelece diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
- 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.

A obediência ao conjunto de normas do DSIC tende a ser a principal direcionadora das auditorias de segurança da informação nos próximos anos.

7.1.2 Normas do Ministério do Planejamento

Também é importante destacar a IN 04 da SLTI/MP, de 19 de maio de 2008, que "Dispõe sobre o processo de contratação de serviços de Tecnologia da Informação pela Administração Pública Federal direta, autárquica e fundacional", incluindo a necessidade de aprovação de um Plano Diretor de Tecnologia da Informação para que seja feita a contratação de serviços. O planejamento de TI é uma importante fonte de informações sobre estratégias de sistemas de informação, e, portanto, critérios para auditoria e gestão de riscos.

7.1.3 Tribunal de Contas da União

No caso do TCU - Tribunal de Contas da União, é digno de nota a jurisprudência do órgão acerca do tema segurança da informação, subordinado ao tema Tecnologia da Informação, conforme ilustra a árvore de conhecimento mostrada na Figura 4.

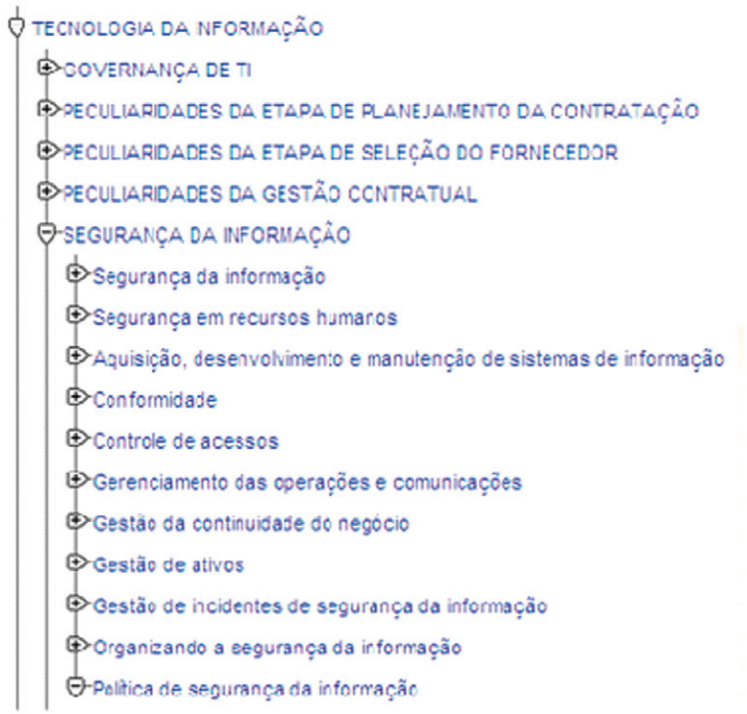

Figura 4. Árvore de conhecimento da Jurisprudência Sistematizada do TCU. Fonte: www.tcu.gov.br.

7.1.4 CGU – Controladoria Geral da União

Os manuais e normas de funcionamento do controle interno, produzidos pela CGU definem um arcabouço geral de auditoria na APF, e devem ser observados na criação de qualquer programa de auditorias. Para introdução o leitor é remetido aos trabalhos de Rocha (2008a) e Rocha (2008b).

7.1.5 Arquivos Públicos

Há que se destacar arcabouço normativo já desenvolvido no Brasil acerca do tratamento dos arquivos nacionais, na forma de Leis e Decretos, como a Lei 8159 de 08/01/1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências. No que se refere à gestão dos arquivos correntes das organizações públicas, existem implicações diretamente relacionadas com a segurança da informação, que precisariam ser mais profundamente avaliadas.

7.2 Propósitos e Limitações da Auditoria de Conformidade

Uma limitação de auditorias de conformidade é que elas apenas constatam níveis de aderência a normas ou especificações. Não é função de uma auditoria de conformidade ter certeza de que aquilo que está em conformidade é eficaz ou mesmo efetivo. Para isso seria necessário desenhar uma auditoria de desempenho operacional, para saber se os padrões de segurança das informações estão de fato protegendo os ativos de informação.

Assim, esse texto delimita auditoria de conformidade como tendo os seguintes propósitos:

a. examinar se os procedimentos de segurança da informação atendem aos requisitos que estão especificados na política de segurança da informação e outros documentos derivados dela, bem como ao arcabouço normativo vigente em níveis superiores à organização auditada. Aqui convém acessar, além do arcabouço normativo, as diretrizes da ISO/IEC 27002:2005, no item 15.2.1, mostrado na caixa abaixo como texto complementar.

TEXTO COMPLEMENTAR

15.2.1 conformidade com as políticas e normas de segurança de informação (ISO/IEC 27002:2005)

Controle
Convém que gestores garantam que todos os procedimentos de segurança da informação dentro de sua área de responsabilidade estão sendo executados corretamente para atender às normas e políticas de segurança da informação.

Diretrizes de implementação
Convém que os gestores analisem criticamente, a intervalos regulares, a conformidade do processamento da informação dentro de sua área de responsabilidades com as políticas de segurança da informação, normas ou qualquer outros requisitos de segurança.

Se qualquer não-conformidade for encontrada como um resultado da análise crítica, convém que os gestores:
a) determinem as causas da não-conformidade;
b) avaliem a necessidade de ações para assegurar que a não-conformidade se repita
c) determinem e implementem ação corretiva apropriada;
d) analisem criticamente a ação corretiva tomada.
(…)

b. verificar que as documentações expedidas que tratam de ativos críticos ou sensíveis obedecem ao decreto 4553/02 quanto à classificação de níveis de sigilo ou a outros regulamentos como uma portaria do próprio órgão que trate do assunto de forma mais específica; e

c. Verificar que todos os procedimentos de segurança, sejam de gestão, sejam operacionais, obedecem a padrões de segurança especificados.

7.3 Documentos de referência e objetos de controle

A auditoria de conformidade de segurança da informação deve examinar todos os tipos de documentos relacionados aos ativos de informação (MAIR ET AL, 1974). No entanto, documentos técnicos só podem servir como referência se forem considerados como normas técnicas.

Se uma auditoria de sistemas de informação tiver como propósito a conformidade, alguns dos seguintes documentos merecem atenção:

- Documentos de metodologias de desenvolvimento de sistemas adotadas pela organização. Pode-se verificar o seguimento de metodologias tanto como auditoria de conformidade, como enquanto parte de um auditoria de desempenho operacional. Note que o arcabouço metodológico da segurança da informação na APF é normatizado pelo DSIC/GSIPR.
- Documentos de projetos considerados críticos ao negócio e que precisam ser protegidos de acordo com critérios aprovados pela alta direção. O próprio documento é objeto de auditoria.
- Orçamentos detalhados de projetos sigilosos. Um caso típico é o orçamento da área militar e de órgãos de inteligência.
- Manual de versionamento e arquivamento de documentos. Servem para averiguar se a documentação está de acordo com as instruções para sua elaboração.

Um auditor de conformidade também não se envolve na gestão da segurança (auditoria de gestão), nem na implementação da segurança ou no seu funcionamento (auditoria operacional). Deve ser mantido o princípio da segregação de funções, que já mencionamos aqui.

Baseado nesses princípios, os seguintes objetos de controle, não exaustivos, podem ser usados como referência de auditoria de conformidade de segurança da informação.

- Normativos expedidos por órgãos de controle e normatização da esfera federal. GSIPR, MPOG, CGU e TCU.
- Melhores práticas como a ISO/IEC 27002, CMMI, COBIT e ITIL.

Se no âmbito da organização não estão em usos esses padrões ou melhores práticas então a organização pode criar suas próprias normas de segurança da informação, que sob o ponto de vista metodológico, estarão subordinadas às normas do DSIC/GSIPR. Essas normas devem estar referidas em uma política de segurança da informação válida para toda organização, como já discutido.

- A política de segurança da informação, para verificar que as atualizações das estratégias de segurança da informação ali previstas estão sendo seguidas;
- Os contratos com empresas de segurança, de onde deve se examinar procedimentos realizados com aqueles previstos em contrato ou na política de segurança que a empresa concordou em seguir,
- Os procedimentos de segurança já padronizados, de onde se deve procurar divergências entre o que foi auditado e o que está prescrito nas normas em que os procedimentos estão inscritos. Tais divergências são tradicionalmente chamadas de não-conformidades.
- Requisitos. Tanto os requisitos de segurança de informação quanto de sistemas de informação devem ser homologados ou formalizados em contratos.

- Normas de propriedade intelectual, são também referências importantes, pois a quebra de propriedade intelectual pode gerar uma insegurança jurídica, o que pode levar a indisponibilidade de serviços.
- Normas de atualização e retenção de backups. As unidades de armazenamento podem ser inspecionadas para verificação.
- Chaves Públicas. Verificar que os mecanismos de chave pública estão sendo utilizados de acordo com a ICP-Brasil para os casos assim exigidos.

Texto Complementar

Um modelo de política de segurança da informação

Politica de Segurança da Informação

Art. 1º. Entende-se por Política de Segurança da Informação o conjunto de princípios, orientações e regras formalmente declaradas a respeito do que deve ser seguido em termos de segurança dos ativos de informação.

Art. 2º. Considera-se ativos de informação todos os recursos tecnológicos que incluem documentos, dados e sistemas, procedimentos e processos, necessários ao atendimento das necessidades de negócio da organização.

Art. 3º. Esta política de segurança da informação tem o propósito de:
i) subsidiar o processo decisório quanto a riscos envolvidos com os ativos de informação e seu impacto nos negócios;
ii) traduzir em normas consensuadas as soluções de segurança definidas no comitê de segurança da informação;
iii) consolidar, a partir das diretrizes estabelecidas, uma estratégia de atuação que implemente as soluções de segurança selecionadas;
iv) orientar quanto ás tratativas adequadas para abordar questões emergenciais relativas a segurança da informação materializadas em planos de contingência;
v) ser instrumento norteador das ações de segurança da informação com abrangência por toda organização aos parceiros.

Art. 4º. Os pressupostos dessa política são
i) conformidade com o regimento interno da organização;
ii) regras e normas alinhadas com a missão e objetivos organizacionais;
iii) existência de trabalho cooperação com forte viés de integração dos diversos atores envolvidos com segurança de ativos de informação;
iv) registro de permanente de ameaças e vulnerabilidades superadas a aquelas a que a organização permanece sujeita;

Parágrafo Único. Mudanças neste documento só poderão ser realizadas pelo comitê de segurança da informação a e aprovadas pela alta direção.

Art 5º. Deverá se disponibilizado e divulgado para toda a organização um conjunto de orientações quanto ao ativos de informação.

Parágrafo Único. Em atendimento ao caput deste artigo deverão ser criadas regras que regulem ativos de informação quanto a:
i) coleta de informações;
ii) armazenamento de dados;
iii) publicação de informação;
iv) classificação de documentos;
v) sistemas de informação;
vi) processamento de dados;
vii) acesso físico;
viii) acesso lógico;
ix) fluxo de dados e documentos;
x) distribuição;
xi) formatação.
(…)

7.4 Classificação de Documentos e da Informação

Um item essencial da auditoria de conformidade é o que concerne à classificação de documentos. Quando se está trabalhando com segurança de informação de governo, a referência para verificação de conformidade se confunde com auditoria de legalidade. O Decreto Nº 4.553, de DE 27 DE DEZEMBRO DE 2002 "*dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal". Esse decreto pode auxiliar o gestor na definição de critérios de classificação de dados nas organizações públicas. O grau de sigilo é dado conforme "(...) gradação atribuída a dados, informações, área ou instalação considerados sigilosos em decorrência de sua natureza ou conteúdo;* ". O decreto cria as seguintes classificações de documentos:

i) OSTENSIVOS: "sem classificação, cujo acesso pode ser franqueado a qualquer interessado;"

ii) RESERVADOS: "dados ou informações cuja revelação não autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos."

iii) CONFIDENCIAIS: "dados ou informações que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado."

iv) SECRETOS: dentre outros, dados ou informações referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicos, cujo conhecimento não autorizado possa acarretar dano grave à segurança da sociedade e do Estado.

v) ULTRA-SECRETOS: "dentre outros, dados ou informações referentes à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado."

7.5 Conclusões

A auditoria de conformidade consiste então em examinar se objetos ou ações realizados ou em realização estão de acordo com normas pré-estabelecidas. Essas normas geralmente definem padrões de desempenho, de procedimentos, de processos, de execução, de produtos de sistemas e demais objetos ou ações que têm especificações normativas que servem de referência para exame da auditoria. As normas criam expectativas de que, uma vez seguida as regras, haverá maior previsibilidade de resultados proporcional ao grau de aderência a esses padrões.

8. Plano de Segurança da Informação

Já foi mencionado anteriormente o plano de segurança da informação, que é resultado de um planejamento organizacional de segurança e tem como principal referência a política de segurança da informação. Esse plano identifica tarefas de segurança específicas que deverão ser verificadas por meio de planos ou programas de auditoria. Adicionalmente, essas tarefas devem estar vinculadas a riscos associados, que devem ser eliminados ou controlados a um nível aceitável. As atividades de segurança da informação devem ser especificadas de forma consistente e de acordo com os requisitos de gestão, das operações e de conformidade.

Durante a fase de formulação do plano de segurança, devem ser conduzidos estudos sobre conceitos de segurança em geral e sobre as peculiaridades da segurança da informação em particular, típicos da organização. Deve-se realizar uma análise e avaliação dos riscos de segurança da informação para, em seguida, se selecionar medidas que garantam a segurança dos ativos de informação considerados sensíveis. Dessa forma, as tarefas de segurança devem guardar relação com esses ativos segundo critérios de níveis de riscos obtidos. A maior parte destas tarefas está descrita e é consequencia do desenvolvimento do um plano de tratamento dos riscos, efetuado por um processo de gestão de riscos de segurança da informação.

8.1 Gestão de riscos

A gestão de riscos de segurança da informação, abordada por Fernandes (2010), consiste em um processo contínuo e operacional, que busca antever a ocorrência de eventos danosos para os ativos de informação de uma organização, a fim de controlar suas consequencias e impactos, por meio da aplicação equilibrada de controles de segurança nessa organização, diante do seu perfil de riscos de segurança analisado.

A Figura 5 apresenta o modelo de gestão de riscos proposto pela norma ISO/IEC 27005:2008.

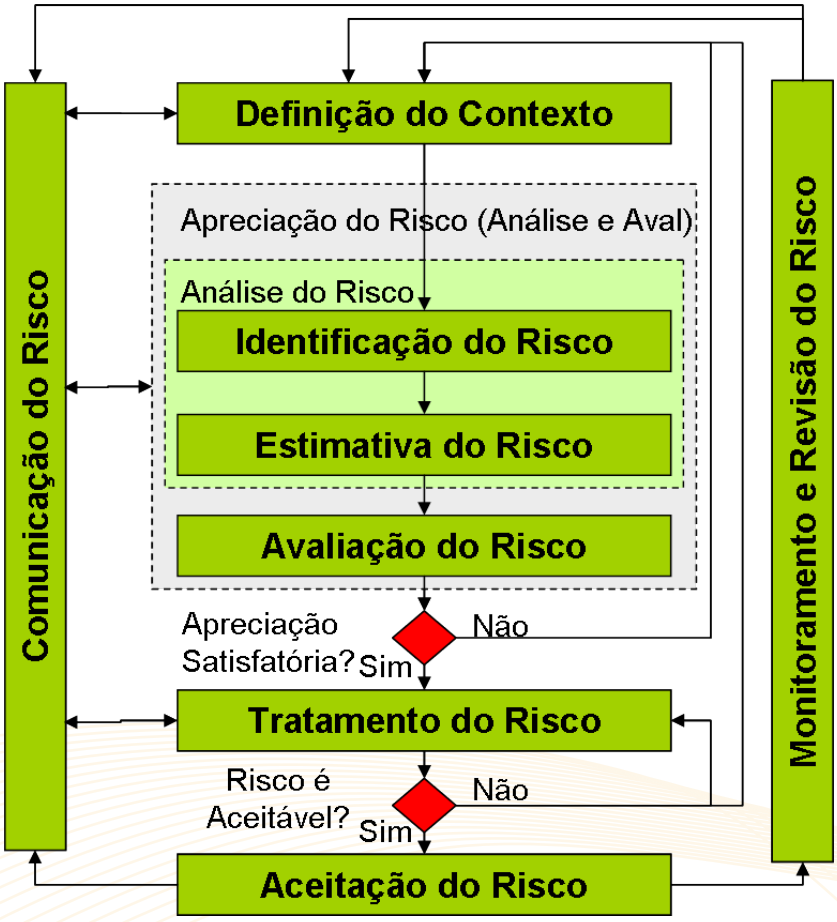

Figura 5. O processo de gestão do risco da ISO 27005:2008. Fonte: Fernandes (2010).

Segundo Fernandes (2010b), a gestão de riscos tem o efeito de tornar uma organização mais segura, isto é, que possui um grau satisfatório de garantia de que continuará a funcionar adequadamente conforme suas características estabelecidas, mesmo na presença de eventos negativos decorrentes da interação com agentes maliciosos ou na ocorrência de eventos decorrentes de acidentes ou desastres de origem natural ou ambiental. "Segurança significa continuar a cumprir seus objetivos de negócio, mesmo em face do sinistro." (Fernandes, 2010b).

A garantia de funcionamento da organização decorre da implementação de um plano de segurança da informação, cujo principal insumo é o Plano de Tratamento do Risco (PTR), produzido na fase de Tratamento do Risco (Ver Figura 4). O Tratamento do Risco ocorre após a Análise e Avaliação do Risco, também chamada de Apreciação. Do Plano de Tratamento do Risco deriva diretamente o Plano de Segurança da Informação, pois o primeiro precisa ser aceito pelo gestor da organização na fase de Aceitação do Risco (Ver Figura 4). Uma vez aceito, o Plano de Segurança passa a ser executado e continuamente monitorado e comunicado entre os agentes que constituem a organização.

O Quadro 2 apresenta um modelo de plano de tratamento do risco, usualmente desenvolvido na Fase de Tratamento do Risco na gestão do Risco.

Plano de Tratamento do Risco

Risco (Ameaça explorando Vulnerabilidade)	Nível do Risco	Controles Recomendados	Prioridade	Controles Planejados	Recursos Necessários	Times e Pessoas Responsáveis	Datas de início e fim	Requisitos de Manutenção e Comentários
Usuários não autorizados podem usar ftp anônimo e capturar informação sensível em arquivos	Baixo	Desabilitar ftp anônimo Limitar acesso externo ao serviço de ftp Atribuir um login difícil à conta de convidado	Média	Desabilitar ftp anônimo Limitar acesso externo ao serviço de ftp Remover a conta de convidado	10 horas para configurar os dispositivos e sistemas	Joaquim José, administrador da rede	21/fev/2011 a 28/fev/2011	Fazer escaneamento periódico de portas e serviços ftp externamente disponíveis, usando scanner
Usuário não autenticado pode navegar no sítio web e capturar informação sensível em arquivos	Alto	Remover arquivos sensíveis do sítio web Reconfigurar serviço web para impedir acesso a arquivos sensíveis	Alta	Remover arquivos sensíveis do sítio web	24 horas para fazer análise do sítio e identificar arquivos sensíveis	Ângela Freire, designer web	05/fev/2011 a 08/fev/2011	Fazer escaneamento periódico do conteúdo de arquivos no sítio web, usando scanner XYZ

Quadro 2. Esboço de um Plano de Tratamento do Risco. Adaptado do NIST 800-30 (NIST,

É importante destacar que a gestão do risco se inicia (ver topo da Figura) com uma Definição do Contexto para a gestão do risco, na qual são definidos os critérios para a gestão do risco. Para detalhes sobre o processo geral descrito na figura o leitor é remetido a Fernandes (2010).

Conforme a ISO/IEC 27005:2008, os benefícios decorrentes da adoção de uma abordagem de gestão de riscos aderente à norma compreendem:

- Riscos são identificados.
- Riscos são apreciados em termos de consequências e chances de ocorrência.
- As chances e consequências de riscos são comunicadas e compreendidas.
- Uma ordem de prioridade para tratamento de riscos é estabelecida.
- Uma ordem de prioridade para redução dos riscos é estabelecida.

- Os intervenientes são envolvidos em decisões sobre riscos e mantidos informados sobre o *status* da gestão de riscos.
- O monitoramento dos riscos é efetivo.
- Os riscos e o processo de gerência de riscos são monitorados e revistos regularmente.
- Captura-se informação que permite a melhoria da abordagem de gestão de riscos.
- Os gerentes e o *staff* são educados sobre riscos e ações tomadas para mitigá-los.

8.2 Critérios de auditoria

Outra característica dos planos de segurança é que eles devem ter critérios de auditoria bem definidos. E isso depende em parte das análises e avaliações de riscos realizadas na gestão do risco. Esses critérios, na realidade, são um conjunto de controles considerados adequados com os quais um auditor precisa trabalhar para busca de evidências. Quando listados os objetos de auditoria, especialmente numa auditoria de conformidade, não há consideração para com os critérios e decisões anteriormente envolvidas na escolha desses objetos, uma vez que esses podem ser bastante complexos, tendo sido definidos na gestão do risco. Mas o fato é que esses objetos de auditoria e os pontos de controle correspondentes são elencados conforme a percepção do grau de risco que sua violação tem para os negócios da organização. A escolha de padrões também determina esses critérios. Não há como definir critérios gerais para todos os casos, pois para cada plano de auditoria esses critérios podem ser delineados conforme a natureza e a finalidade da organização. A fase de Definição do Contexto da ISO/IEC 27005:2008 estabelece o referencial para obtenção da maioria desses critérios.

Se a auditoria é feita organizações públicas, que fazem uso intensivo sistemas de informação automatizados por computadores e software melhores práticas definidos nos modelos CMMI, ITIL e COBIT são também fontes relevantes, além é, claro, do atendimento às normas compulsórias do Serviço Público. Esses arcabouços conceituais e de melhores práticas podem guiar a formulação dos critérios de auditoria, porém, não têm uma relação direta com segurança, a não ser em alguma de suas partes. Mesmo assim, como o objetivo é garantir que a informação esteja preservada e protegida, questões como confidencialidade, disponibilidade e integridade, não podem prescindir de fontes valiosas como essas, pois requerem uma preocupação com vários aspectos da produção da informação, difíceis de encontrar em apenas uma proposta de melhores práticas.

É recomendado, tanto em organizações públicas quanto privadas, que se comece com a série ISO/IEC 27000, especialmente as normas 27001:2006 (ABNT, 2006), 27002:2005 (ABNT, 2005) e 27005:2008 (ABNT, 2008), todas adotadas pela ABNT, como fonte de critério de auditoria de segurança de informação. Dessas normas se podem retirar vários objetos de auditoria e pontos de controle. Com base nos normativos da ISO/IEC, a auditoria poderá ser realizada em dois momentos. O primeiro inicia-se com uma revisão da existência e completude de documentos-chave, tais como a política de segurança da organização, declaração de aplicabilidade, plano de tratamento de riscos (PTR) e, caso já esteja em prática a ISO/IEC 27005:2008, o conjunto de critérios previamente definidos no início da gestão do risco. O segundo momento deve se preocupar com um detalhamento dos riscos, e uma auditoria em profundidade envolvendo a existência e efetividade do controle ISMS (*Information Security Management System*), descrito na ISO/IEC 27001:2006, que estrutura a segurança da informação como um sistema.

9. Instrumentos e Ferramentas

A realização de uma auditoria eficaz não pode prescindir de instrumentos, ferramentas e eventualmente, trabalhos de técnicos especializados, descritos no restante desta seção.

9.1 Instrumentos de coleta e registro de evidências

Um auditor experiente provavelmente lança mão de vários modelos de instrumentos de coleta de dados, conforme o tipo de auditoria e os objetos verificados. Vários deles são formulários ou questionários impressos, alguns com suporte de *software* especializado ou planilhas eletrônicas customizadas. Esses instrumentos darão origem aos papéis de trabalho do auditor. O Quadro 2 sugere um modelo simplificado de instrumento de coleta de dados, devidamente preenchido com um exemplo fictício.

Quadro 3. Modelo de instrumento de coleta de dados para auditoria de segurança da informação.

AUDITORIA **( ) Gestão** **(X) Operacional** **( ) Conformidade**		**Data: ___/___/___** **Local:**	**Auditor: João da Silva**		
Objeto de Auditoria (OA)	Ponto de controle (PC)	Lista de Verificação: SIM (S) NÃO (N) NÃO E APLICA (N/A) ?	Em Andamento	Verificado ?	Validado ?
OA1 Computadores	PC1 Acessos a computadores e a sistemas de informação utilizando celular estão protegidos com a última versão de algoritmo de encriptação	S	-	S	N
	PC2 Equipamentos de rede catalogados e protegidos fisicamente	N	S	S	N
	PC3 Acesso a computadores protegidos com protocolo de segurança Secure Socket Layer (SSL)	N	N	N	N
	PC4 Checar efetividade do programa anti-virus	S	-	S	S
OA2 Rede sem Fio	PC1 Instalação do protocolo de criptografia atualizado	S	S	S	S
OA3 Criptografia	PC1 Acesso a serviços críticos através de certificados digitais	S	N	N	N
	PC2 Existência de medidas de proteção dos dados armazenados, por criptografia	N	N	N	N
OA4 Rede LAN	PC1 Configuração do *firewall controlada e periodicamente revisada*	S	S	S	S
	PC2 controle de acesso ao ambiente de rede	S	N/A	S	S
	PC3 Acesso remoto absolutamente controlado e somente para sistemas específicos	N	S	N	N
	PC4 Redes virtuais privadas (VPN) usam IPSEC	S	N	S	S
	PC5 Proteção de cabeamento da rede	N	S	N	N
OA5 Protocolos	PC1 Existência de rotinas adequadas de proteção e controle do fluxo de dados	N	N	N/A	N/A
	PC2 Observância de protocolos adequados de acordo com a criticidade dos sistemas de informação	N	S	N/A	N/A
	PC3 Existência de scanners de redes para verificação de uso de portas	S	N/A	S	S

Observe que o Quadro 1 lista os objetos e os pontos de controle e faz três perguntas. A primeira indica se o controle existe para cada objeto e ponto de controle. A resposta vem de uma lista de verificação respondida com SIM, NÃO e Não se Aplica (N/A). A coluna "em Andamento" indica que providências já estão sendo tomadas para a análise. A coluna "Verificado" indica se o ponto de controle foi testado. A coluna "Validado" indica se o controle referente ao PC foi

validado, ou seja, se foi testado e está em pleno funcionamento. O formulário *per se* permite abordagens diferenciadas, envolvendo testes de controle e testes substantivos, onde for o caso. Na coluna "Lista de Verificação", por exemplo, o objetivo é perguntar sobre a existência ou não do controle. Uma entrevista poderá ser suficiente, se o propósito é fazer um levantamento da situação para saber se certos controles já foram elencados. Responder SIM ou NÃO apenas confere se a organização já iniciou o processo de segurança de seus ativos de informação. Algumas combinações obtidas no Quadro levam a providências e procedimentos diferentes. Se um ponto de controle, já catalogado como sensível à segurança dos ativos de informação ainda não foi implantado, uma auditoria de gestão é recomendada.

Razões diversas como falta de profissionais qualificados, custos elevados, ou mesmo a inexistência de ferramentas cuja aquisição não foi priorizada, podem determinar essa ausência. Outros controles precisam ser testados. Por exemplo, a sequência OA1/PC3 => N,N,N,N indica que não existe o controle em prática, e, portanto, nada pôde ser verificado ou validado. Neste caso, é preciso consultar as decisões relacionadas a este ponto de controle quanto a prazos, custos, pessoal, dentre outras auditorias. Ou seja, a auditoria deve ser aprofundada e considerada prioritária para o OA1/PC3.

Agora, caso seja constatada a existência do controle e sua operação já tenha sido implantada, a auditoria recomendada é a de desempenho operacional, desde que se queira checar indicadores de eficácia do controle. O exemplo OA4/PC4 => S,S,S,S significa que o PC foi validado. Para que tal validação aconteça, o funcionamento do IPSEC deve ser demonstrado, seja por um analisador de protocolos, seja por verificação da configuração da VPN (*Virtual Private Network*), mesmo que seja óbvio que o IPSEC esteja sendo utilizado. Em segurança mesmo o que é óbvio não pode ser negligenciado. É óbvio que agentes de uma organização não a sabotariam. A Engenharia Social está aí para mostrar que isso pode ser feito até mesmo sem haver intenção de fazê-lo.

Para finalizar, não se pode deixar de mencionar a gestão e os planos de continuidade. Esse plano não será tratado aqui por questão de espaço, mas verificar a sua existência e seus parâmetros já é por si só objeto de uma auditoria que merece muita atenção. Planos de continuidade devem ser testados, pois descrevem em detalhes os procedimentos de manutenção dos negócios críticos e a restauração de plena capacidade operacional da organização em caso de crises e catástrofes. É, portanto, um elemento indispensável para a segurança.

9.2 Automação de Auditoria Serviços Técnicos Especializados

À medida que seja preciso verificar muitos pontos de controle, automação precisa ser utilizada para agilizar o processo. De outra forma, devido à complexidade e à dinamicidade de certos ambientes tecnológicos, podem ser necessários serviços de assistentes especializados em determinadas tecnologias e ambientes.

A quantidade de dados e informações coletadas e os papéis de trabalho demandam esforço de organização de informação e documentação.

As atividades de testes de controle e testes substantivos também podem demandar grande esforço intelectual e conhecimento especializado e atualizado.

Para efeito de implementação de uma política de segurança de fato, é provável que se tenha que utilizar muitas ferramentas e assistentes para cada caso, pois as ações de verificação e validação requerem demonstração de que, comprovadamente, os controles estão funcionando e os resultados são válidos para os propósitos traçados no plano de segurança. Para aprofundamento nesta questão pode-se consultar o guia do ISACA (2009), o sítio do Instituto de Auditores Internos (http://www.theiia.org), o sítio Audit Net (http://auditnet.org/), entre outros.

9.2.1 Batimento de dados e CAATS

No caso de verificação ou batimentos de dados (testes substantivos), por exemplo, ferramentas como ACL (*Auditing Command Language*) e outras utilizadas na área de auditoria financeira e de análise estatística podem ser usadas para apoiar o processo de análise. Tais ferramentas se enquadram na classe de Computer Aided Audit Tools (CAATS). Uma lista das mais usadas pode ser encontrada em http://en.wikipedia.org/wiki/CAATS.

9.2.2 Auditoria de ambientes computacionais e bancos de dados

No caso de verificação de máquinas com sistemas operacionais específicos, sejam Windows ou Linux, bem como de sistemas de bancos de dados devem ser usados procedimentos padronizados por plataforma, juntamente com ferramentas específicas para as versões de sistemas operacionais ou bancos de dados, que se sucedem rapidamente. Para maior detalhamento podem ser consultadas as fontes

9.2.3 Redes de computadores

Para a verificação de redes de computadores as ferramentas mais comumente usadas são:

- Nessus, um scanner de vulnerabilidades usado para, por exemplo, verificar quais serviços estão abertos em quais portas nos servidores de uma rede.
- Wireshark, um front end para sniffing de rede, que realiza análise de comunicações entre computadores em vários protocolos.
- Snort, um sistema para prevenção e (ou) detecção de intrusos.

Algumas verificações são mais elementares, como o análise do *firewall* e suas configurações. Essas análises, automatizadas ou não, dão visibilidade a evidências escondidas.

9.2.4 Hacker Ético

Caso os riscos de segurança e a confiabilidade demandada em um ambiente de rede ou mesmo no ambiente organizacional sejam elevados, o auditor pode recorrer a testes especializados e detalhados como a análise de vulnerabilidades, também conhecida como teste de penetração. Um serviço de Ethical Hacking pode ser usado, com o consentimento expresso do cliente. O Certificado CEH Certified Ethical Hacker, expedido pela organização Norte-Americana EC-Council (E-Commerce Consultants International Council, https://www.eccouncil.org/about_us/about_ec-council.aspx) atesta habilidades de profissionais nesta área, bem como descreve o conjunto de habilidades e ferramentas que devem ser conhecidas e podem ser empregadas por um hacker ético, conforme demanda:

- Conhecimento da legislação
- Reconhecimento do terreno
- Hacking usando o Google
- Escaneamento e Enumeração
- Engenharia Social
- Hacking de computadores
- Cavalos de Tróia e Backdoors
- Vírus e Vermes
- Phishing

- Hacking de contas de email
- Negação de serviço
- Roubo de sessões
- Hacking de servidores web
- Vulnerabilidades de aplicações web
- Quebra de senhas na web
- Injeção de SQL
- Hacking de redes sem fio
- Segurança física
- Evasão em Sistemas de Detecção de Intrusão e Firewalls
- Estouro de Buffers
- Criptografia
- Metodologias de teste de penetração

A atividade de um hacker ético deve seguir os seguintes passos, conforme indica Graves (2007):

- Discussão de necessidades com o cliente
- Preparação e assinatura de acordo de confidencialidade
- Organização do time de ethical hacking
- Condução de testes, comumente chamados de testes de penetração ou análise de vulnerabilidades
- Análise de resultados
- Preparação e apresentação do relatório

Note, no entanto, que o serviço de um Hacker Ético não é considerado uma auditoria propriamente dita.

10. Entregas da Auditoria

O fim básico da auditoria é investigar problemas e ter propostas e recomendações de melhoria dos serviços e publicá-los em relatórios e pareceres chamados de entregas. Por isso a seguir o modelo da Figura 1 é mais detalhado, agora que há mais informações sobre o trabalho de um auditor. Cada entrega deve apresentar a situação encontrada: as deficiências de cada serviço, as melhores práticas implantadas para superar as deficiências encontradas, as fragilidades (vulnerabilidades) e as ameaças. Quando se decide realizar uma auditoria com auditores internos ou externos toda a ação deve ter alguma roteirização de auditoria que pode ser feita de várias maneiras. Antes que isto ocorra, várias providências já devem ter sido tomadas:

1. Todos os objetos de auditorias e seus respectivos pontos de controle já devem ter sido definidos e codificados.
2. A política de segurança da informação deve está aprovada e em curso.
3. O plano de segurança da informação baseado na Política de Segurança da Informação já está elaborado, conforme esboçado no Quadro 1.

11. Programas de Auditoria

Como já dito, várias auditorias devem ser realizadas durante a vigência do plano de segurança ou da política e se desenvolverão conforme as estratégias definidas nesses documentos. Estas várias auditorias são agrupadas sob a denominação de um programa de auditoria, onde cada auditoria é projeto.

11.1 Um Modelo de Programa de Auditoria

O Quadro 3 mostra um possível modelo para se registrar as intenções de um programa de auditoria. Observe que cada quadro com OC.PC (Objeto de controle. Ponto de controle) tem como atributos a justificativa, parâmetros de medida, prioridade e a abordagem a ser usada, ou seja, o tipo de auditoria.

Quadro 3. Modelo de registro de um programa de auditoria.

PROGRAMA DE AUDITORIA			
Nº Programa _____	Auditor(res) _____		Datas Início __/__/___ Fim __/__/___
Código Pontos de Controle	Descrição	Prioridade (severidade)	Tipo de Auditoria
OC.PC	XXXXXXXXXXX	(1,2,3 ou 4)	Gestão (G) Operacional (O) Conformidade (C)
Justificativa	Parâmetros	Objetivo	Obs.
xxxxxxxxxx	xxxxxxxxx	xxxxxxxxx	xxxxxxxxx

Se o modelo do Quadro 3 for usado, considere as seguintes instruções de preenchimento:

1. Numere o plano, pois será preciso acompanhar o andamento de cada um deles. Planos podem ser iniciados paralelamente.
2. Para cada plano deve haver um auditor responsável. É sempre recomendável ter mais de um auditor, pois pode ser preciso cotejar opiniões diferentes na hora de emitir o parecer.
3. É preciso saber em que data se iniciou e terminou a auditoria. Dificuldades na segurança da informação podem ser detectadas acompanhando-se o tempo que se leva para realizá-las.
4. Um plano pode conter um ou mais objetos de auditoria com um ou mais pontos de controle. A sigla "OC.PC "significa objeto de controle com seu ponto de controle a ser auditado. Se houver necessidade de mais detalhes, pode-se assinalar datas de início e términos para cada ponto de controle.

5. Cada ponto de controle deve ser descrito tal qual ele foi elencado. Importante que todos os objetos de controle e pontos de controle façam parte de um catálogo onde estejam definidos o que fazer (procedimentos e testes) para cada um deles.

6. O nível de risco e severidade da situação é determinante do nível de prioridade que se deve dar à auditoria para cada ponto de controle. Se um sítio eletrônico está sob constante ataque, é provável que o nível de severidade seja máximo, portanto, com prioridade máxima de atendimento.

7. Deve-se justificar porque determinado ponto de controle está merecendo atenção ou se é apenas parte de uma rotina de auditoria.

8. O objetivo da auditoria deve ser claramente definido. Observar que existe um custo associado a cada projeto e sua utilidade deve ser avaliada. O nível de risco é um parâmetro importante na decisão de prosseguir com a auditoria.

9. Observar que para um mesmo ponto de controle podem ser realizados vários tipos de auditoria.

Um relatório técnico de auditoria de segurança da informação deve sugerir as penalidades a ser aplicadas em caso de descumprimento dos acordos de nível de serviços pactuados e contratados ou das normas legais a que se referem de cada um dos serviços de segurança da organização, quando assim for caso. Esses relatórios devem levar em consideração os resultados da auditoria dos indicadores ou dos pontos de controle selecionados.

Os relatórios técnicos de auditoria devem ser elaborados em prazos determinados a contar do recebimento do início da execução do plano de auditoria, pois tais relatórios são usados como insumos para análise do resultado da gestão, das operações e dos testes de conformidade realizados pela equipes de segurança da informação. Devem ser elaborados periodicamente, contendo o resultado dos indicadores dos serviços de auditoria realizados. Tal informação servirá de insumo para a avaliação dos serviços realizados e dos indicadores alcançados no período.

Finalmente, outro relatório importante é o que define uma escala de quais auditores irão fazer ou fizeram quais auditorias. Poderá ser necessário recuperar a experiência de cada auditoria como uma forma de aprendizagem para organização. As providências adotadas e aquelas mais eficazes devem ser compartilhadas e registradas, pois podem ser um insumo importante para se realizar uma gestão do conhecimento gerado pelos auditores.

Com base no plano de segurança, renovado regularmente, será preciso formular uma roteirização de auditoria para cada ação de auditoria prevista dentro de uma rotina de trabalho.

11.2 Gestão de Programa de Auditorias baseada na ISO 19011

Esta subseção descreve os principais elementos contidos nas recomendações da norma ISO 19011, produzida para organizar programas de auditorias para exame de conformidade de programas de gestão de qualidade. A norma pode ser adaptada para usada para fins de auditoria junto à família de normas ISO/IEC 27000. A Figura 5 apresenta um fluxograma geral de gestão de um programa de auditoria baseado na ISO 19011:2002, que adota o modelo PDCA, de melhoria contínua. Este modelo pode ser usado por um gestor de segurança que deseja fortalecer o seu sistema de controles por meio de implementação de um programa de auditorias regulares.

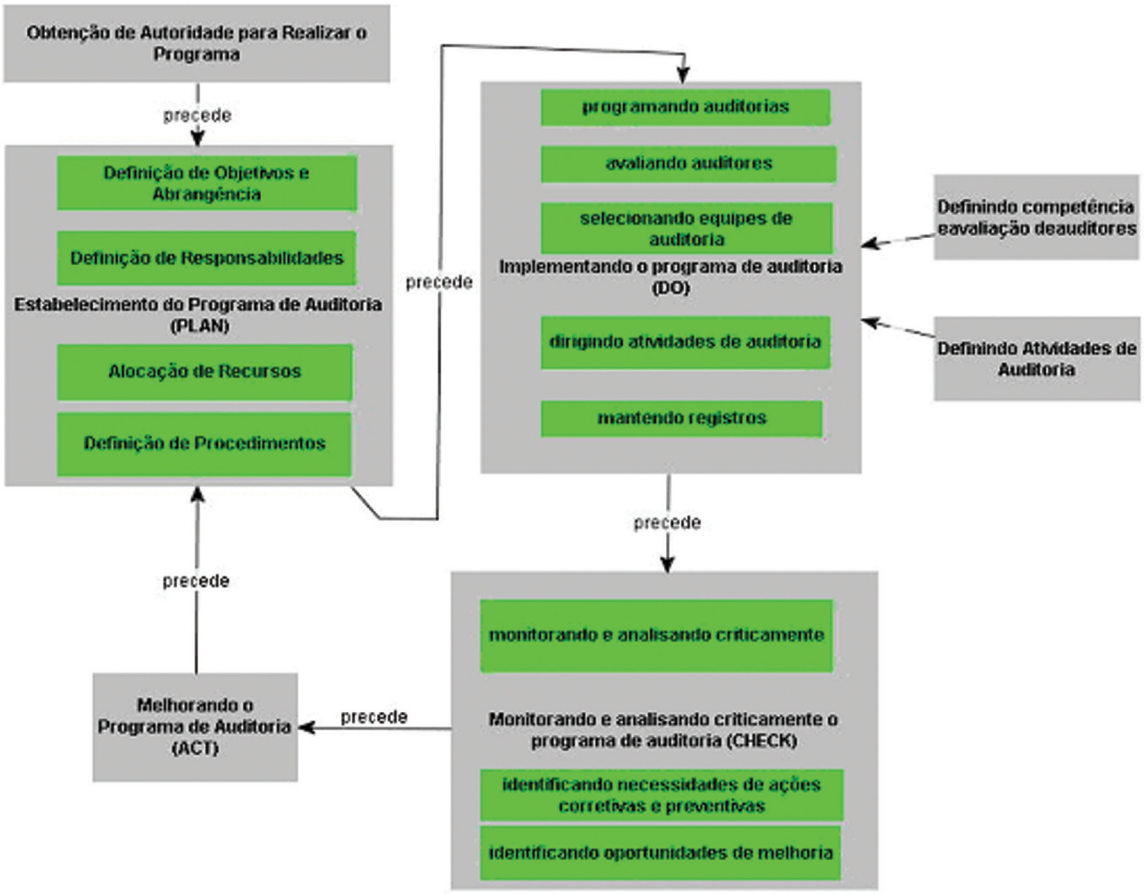

Figura 5. Modelo de Organização de um Programa de Auditorias. Fonte: Fernandes (2009).

11.2.1 Obtenção de autoridade

Um programa de auditoria inicia-se com a obtenção de autoridade, por parte do gestor, para a realização do programa de auditorias. No caso da Administração Pública Federal, isto deve envolver articulação com o Sistema de Controle Interno coordenado pela CGU, bem como pode envolver articulação com o DSIC/GSIPR.

11.2.2 Estabelecimento do programa

O estabelecimento do programa envolve: (i) definir objetivos e abrangência da auditoria, já discutido nas seções 2 e 3; (ii) a definição de responsabilidades, que pode estar num plano de tratamento de riscos, discutido na Seção 8.1; (iii) a alocação de recursos, que também pode estar num plano de tratamento de riscos; e (iv) a definição de procedimentos e tipos de auditoria, discutidos nas seções 2.3 e 2.4.

11.2.3 Implementando o programa de auditorias

A implementação envolve: (i) a roteirização de auditorias, discutida nas seções 4, 5, 6 e 7; (ii) a avaliação de auditores que no passo (iii) constituirão o time de auditoria. Para tal, deve-se estudar os atributos profissionais de um auditor, como discutidos em Imoniana (2005) e Duhn (1991); a direção de atividades de auditoria (foco maior de todo este texto); e a manutenção dos registros, que foi discutida na Seção 2.6.3.

11.2.4 Monitoramento e análise crítica

O monitoramento e a análise crítica do programa de auditoria busca avaliar a eficiência e eficácia das auditorias, e pode ser baseada no uso de indicadores de auditoria operacional discutidos na Seção 6; A identificação de oportunidades de melhoria depende da realização de revisões periódicas da atividade, de sua eficácia e do uso da criatividade para tornar a auditoria mais ágil e eficaz aos propósitos da organização.

11.2.5 Melhoria do Programa de Auditoria

Depende da alocação de recursos, necessariamente apoiados por um processo de planejamento e orçamento.

12. Considerações Finais

Deve-se destacar que não há pretensão de firmar a organização de auditoria aqui mostrada como sendo um modelo ideal a ser seguido na Administração Pública Federal para Auditorias de Segurança da Informação. Apenas foi organizada uma forma conveniente de apresentar o tema para propósitos didáticos. Vários autores usam formas diferentes de organização, convencionando inclusive os conceitos e metodologias que lhes parecem mais adequados. Inclusive os termos usados divergem bastante. Por exemplo, o que foi chamado de objeto de auditoria é também chamado de diretriz, parâmetro, controle ou objetivo de controle por alguns autores da área.

A principal mensagem é a sugestão de organização de auditorias de segurança da informação em três tipos: de gestão, de operações e de conformidade. Trata-se de uma convenção que ilustra que segurança da informação demanda gestão profissional, controle e acompanhamento das operações e aderência às regras para garantir conformidade e previsibilidade das operações. Mas deve-se ter certos cuidados. Vários objetos de auditoria e pontos de controle podem permear os três tipos de auditoria, mudando apenas o enfoque e a ênfase de cada um. Temas como Política de Segurança, Segurança Física e Lógica, Segurança em Sistemas, Usuários, entre outros podem ser auditados do ponto de vista da gestão, das operações ou de sua conformidade com padrões, dentre outras convenções possíveis. O que se deve ter em mente é que as organizações precisam desenvolver uma cultura de segurança para que qualquer projeto de auditoria tenha êxito.

Finalmente se deve observar que atividades de auditorias só são possíveis se a organização estiver preparada. Para ser auditada, organizações públicas devem criar, por exemplo, mecanismos que registrem eventos relevantes e diversos que acontecem no dia-a-dia da organização. É fundamental registrar os fluxos de informação para dentro e para fora da organização, seja qual for o meio de comunicação utilizado. Só assim se podem estabelecer controles e construir instrumentos que possam identificar esses eventos como sendo ou não gerador de vulnerabilidades ou ameaças para os ativos da organização. Se criam as condições que tornam possível um acurado exame dos pontos de controle desses ativos, essencial para que qualquer auditoria de segurança da informação seja eficaz.

Fica aqui a ressalva de que controle excessivo pode prejudicar o dia-a-dia das organizações tornando as atividades reféns desse mesmo controle que pretende qualificar o resultado dessas tarefas. Existe a percepção, no serviço público federal brasileiro, que uma boa parte do tempo útil dos agentes organizacionais é dedicada a preparar registros que se adequem ao Controle. Mas isso tem um custo, não só financeiro, mas também moral. Surge o risco de estar em risco por qualquer coisa. O controle *ex post* seria um caminho, desde que o Estado consiga criar um sistema punitivo justo e eficaz. Uma maneira de saber os limites disso é envolvendo todos os atores no processo. Instrumentos - tais como políticas e planos - são produtos desse envolvimento e da necessidade de todas as organizações implantarem formas seguras de proteger seu ativo mais importante e crítico: a informação.

Referências

ABIN – Agência Brasileira de Inteligência. Compilação de legislação relacionada com informação. Disponível: http://www.abin.gov.br/modules/mastop_publish/?tac=Legisla%E7%E3o. Último acesso em fevereiro de 2011.

ABNT - Associação Brasileira de Normas Técnicas. NBR ISO 19011: Diretrizes para auditorias de sistema de gestão da qualidade e/ou ambiental. Rio de Janeiro: ABNT. Novembro de 2002. 25 p.

ABNT - Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27001 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos. Rio de Janeiro: ABNT. 2006.

ABNT - Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 - Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT. 2005.

ABNT - Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27005 - Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. Rio de Janeiro: ABNT. 2008.

ARAÚJO, A. P. F. Infraestrutura de Tecnologia da Informação (Notas de Aula). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2010. 40 p.

BRASIL. Constituição da República Federativa do Brasil de 05/10/1988 - Constituição da República Federativa do Brasil. (Excertos).

BRASIL. Decreto 1171 de 22/06/1994 - Aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal.

BRASIL. Decreto 3505 de 13/06/2000 - Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

BRASIL. Decreto 4553 de 27/12/2002 - Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.

BRASIL. Decreto 4915 de 12/12/2003 - Dispõe sobre o Sistema de Gestão de Documentos de Arquivo - SIGA, da Administração Pública Federal, e dá outras providências.

BRASIL. Lei 7170 de 14/12/1983 - Define os Crimes contra a Segurança Nacional, a Ordem Política e Social, Estabelece seu Processo e Julgamento e dá outras Providências.

BRASIL. Lei 8027 de 12/04/1990 - Dispõe sobre normas de Conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas, e dá outras providências.

BRASIL. Lei 8159 de 08/01/1991 - Dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências.

BRASIL. Lei 9279 de 14/05/1996 - Regula direitos e obrigações relativos à propriedade industrial.

CHAIM, R. M. Modelagem, Simulação e Dinâmica de Sistemas (Notas de Aula). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2010. 48 p.

COSO - Committee of Sponsoring Organizations of the Treadway Commission. Internal Control – Integrated Framework: Guidance for Smaller Public Companies: Reporting on Internal Control over Financial Reporting: Executive Summary: Guidance. EUA: COSO. October 2005. 207 p.

COSO - Committee of Sponsoring Organizations of the Treadway Commission. Internal Control — Integrated Framework: Guidance on Monitoring Internal Control Systems: Discussion Document. EUA: COSO. September 2007. 52 p.

CPLP - Organismos Estratégicos de Controlo/Controle Interno da Comunidade de Países de Língua Portuguesa. Manual De Controlo/Controle Interno. Brasília: Controladoria Geral da União. Dezembro 2009. Disponível: http://www.cgu.gov.br/eventos/SFC2009_CPLP/Arquivos/ManualControle.pdf. Último acesso em fevereiro de 2011.

CRUZ, Flávio. Auditoria Governamental. Editora Atlas, 1997. Descreve como realizar uma auditoria contábil na esfera governamental.

DSIC – Departamento de Segurança da Informação e Comunicações. 01/IN01/DSIC/GSIPR, de 13 de outubro de 2008 - Estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta. Disponível http://dsic.planalto.gov.br/. Último acesso em Fevereiro de 2011.

DSIC – Departamento de Segurança da Informação e Comunicações. 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008. Define a metodologia de gestão de segurança da informação e comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta. Disponível http://dsic.planalto.gov.br/. Último acesso em Fevereiro de 2011.

DSIC – Departamento de Segurança da Informação e Comunicações. 03/IN01/DSIC/GSIPR, de 30 de junho de 2009- Estabelece diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (POSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Disponível http://dsic.planalto.gov.br/. Último acesso em Fevereiro de 2011.

DSIC – Departamento de Segurança da Informação e Comunicações. 04/IN01/DSIC/GSIPR, de 14 de agosto de 2009 - Estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF. Disponível http://dsic.planalto.gov.br/. Último acesso em Fevereiro de 2011.

DSIC – Departamento de Segurança da Informação e Comunicações. 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009 - Disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Disponível http://dsic.planalto.gov.br/. Último acesso em Fevereiro de 2011.

DSIC – Departamento de Segurança da Informação e Comunicações. 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009 - Estabelece diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Disponível http://dsic.planalto.gov.br/. Último acesso em Fevereiro de 2011.

DSIC – Departamento de Segurança da Informação e Comunicações. 07/IN01/DSIC/GSIPR, de 6 de maio de 2010 - Estabelece diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Disponível http://dsic.planalto.gov.br/. Último acesso em Fevereiro de 2011.

DSIC – Departamento de Segurança da Informação e Comunicações. 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010 - Disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta - APF. Disponível http://dsic.planalto.gov.br/. Último acesso em Fevereiro de 2011.

DUNN, John. Auditing: Theory and Practice. UK: Prentice-Hall. 1991.

FERNANDES, J. H. C. GSIC050: Sistemas, Informação e Comunicação (Notas de Aula). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2010. 51 p.

FERNANDES, J. H. C. Gestão de Riscos de Segurança da Informação (Notas de Aula). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2010. 33 p.

FERNANDES, J. H. C. Controle de Acessos (Notas de Aula). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2010. 32 p.

FERNANDES, J. H. C (Organizador). Gestão da Segurança da Informação e Comunicações – Volume I (Série Segurança da Informação). Brasília: Faculdade de Ciência da Computação da Universidade de Brasília. 2010. ISBN: 978-85-88130-07-4. 123 p.

GAO - General Accounting Office. Management Planning Guide for Information Systems Security Auditing. EUA: National State Auditors Association and the U. S. General Accounting Office. December 2001.

GIL, Antônio L. Auditoria de Computadores. São Paulo: Editoras Atlas. 1989. É um dos livros pioneiros em segurança de computadores. Muitas das preocupações são ainda autuais.

GONDIM, J. J. C., GSIC602: Gerenciamento das Operações e Comunicações (Notas de Aula). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2010. 23 p.

GONDIM, J. J. C., GSIC651: Tratamento de Incidentes de Segurança (Notas de Aula). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2011. 23 p.

GRAVES, Kimberly. CEH: Official Certified Ethical Hacker Review Guide: Exam 312-50. EUA: Sybex. 2007.

GSIPR – Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 - Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Disponível http://dsic.planalto.gov.br/. Último acesso em Fevereiro de 2011.

HOLANDA, M. T; FERNANDES, J. H. C., GSIC701: Segurança no Desenvolvimento de Aplicações(Notas de Aula). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2011. 43 p.

IMONIANA, Joshua O. Auditoria de Sistemas de Informação. São Paulo: Editora Atlas, 2005. Livro de um autor que tem grande experiência com auditoria contábil. Existem várias pontos de controle que podem ser de grande utilidade na elaboração de planos de auditoria.

INTOSAI - International Organization of Supreme Audit Institutions. Guidelines for Internal Control Standards for the Public Sector. Austria: INTOSAI. 2004. 81 p. Disponível URL: http://www.intosai.org.

INTOSAI - International Organization of Supreme Audit Institutions. Internal Control: Providing a Foundation for Accountability in Government. Austria: INTOSAI. 2001. 8 p. Disponível URL: http://www.intosai.org.

ISACA - Information Systems Audit and Control Association. IS Standards, Guidelines and Procedures For Auditing and Control Professionals: Code of Professional Ethics, IS Auditing Standards, Guidelines and Procedures, IS Control Professionals Standards. EUA: ISACA. January 2009.

ITGI - IT Governance Institute. COBIT® 3rd Edition Audit Guidelines. EUA: ITGI. 2000.

ITGI - IT Governance Institute. COBIT® 4.0. Control Objectives, Management Guidelines and Maturity Models. EUA: ITGI. 209 p. 2005.

ITGI - IT Governance Institute. COBIT ® MAPPING: Overview of International IT Guidance. EUA: ITGI. 2004.

JURAN, J. M.; GRYNA, M. Frank. Controle da Qualidade - volume III. São Paulo: Makron Books, 1990. Esse é um excelente livro que descreve várias técnicas de auditoria de qualidade. Embora se refira mais a ideia de produtos e serviços, Juran mostra várias técnicas que são gerais o suficiente para serem usadas na área de segurança da informação.

LOPEZ, André A. P. GSIC905: Diretrizes para o Desenvolvimento de Projetos de Cunho Científico (Notas de Aula). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2010. 24p.

MAIR, W. C.; WOOD, Donald ; DAVIS, Keagle W. Computer Control Audit. Minnesota:Touche Ross & Co. 1978. Um livro avançado para seu tempo. Descreve técnicas de auditoria com uso de computadores com bastante detalhe.

MS - Ministério da Saúde. Portaria MS 3207, de 20 de outubro de 2010, que Institui a Política de Segurança da Informação e Comunicações do Ministério da Saúde. Disponível: http://bvsms.saude.gov.br/bvs/saudelegis/gm/2010/prt3207_20_10_2010.html. Acessado em 10 de janeiro de 2011. Pode ser usado como referência de política de segurança de informação.

NASCIMENTO, A. C., GSIC250: Criptografia e Infraestrutura de Chaves Públicas (Notas de Aula). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2011. 44 p.

NIST - National Institute of Standards and Technology. Risk Management Guide for Information Technology Systems: Special Publication 800-30. EUA: NIST. 2002. Disponivel: http://www.nist.org.

OECD - Organisation for Economic Co-operation and Development. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Europa: OECD. 30 p. 2002. Disponível http://www.oecd.org/dataoecd/16/22/15582260.pdf. Acessado em janeiro de 2011.

OWASP – Open Web Application Security Project. The Open Web Application Secutity Project. EUA: OWASP. http://www.owasp.org/index.php/Main_Page. Acessado em fevereiro de 2011.

PETER, Maria G. A.; MACHADO, M. V. V., Manual de Auditoria Governamental. São Paulo: Editora Atlas, 2003. Disponibiliza várias técnicas de auditoria que podem ser muito úteis como modelo.

PMI - Project Management Institute. PMBOK: Guide to the Project Managament Body of Knowledge. EUA: PMI. 2004.

ROCHA, R. X., Proposta de procedimento simplificado de auditoria de gestão em segurança da informação em órgãos do Poder Executivo Federal (Monografia de Especializaçã Lato Sensu). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2008.

ROCHA, H. A. da, Proposta de Cenário para Aplicação da Norma NBR ISO/IEC 27002 em Auditorias Governamentais do Sistema de Controle Interno (Monografia de Especializaçã Lato Sensu). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2008.

RODRIGUES, R. W. da S. Aquisição e Implementação, Entrega e Suporte de Serviços de TI (Notas de Aula). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2010. 46 p.

SOUZA NETO, João. GSIC331: Política e Cultura de Segurança (Notas de aula). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2010. 33p.

SCHMIDT, A. ; ALENCAR, A J. ; VILLAR, C. B. Modelos qualitativos de Análise de Risco para Projetos de Tecnologia da Informação. sl:Brasport, 2007. Descreve várias técnicas de análise de riscos pra projetos de tecnologia de informação.

TCU – Tribunal de Contas da União. Manual de Auditoria de Natureza Operacional. Brasília: Tribunal de Contas da União - Secretaria-Geral de Controle Externo - Coordenadoria de Fiscalização e Controle, 2000.

TCU – Tribunal de Contas da União. Manual de Auditoria de Sistemas. Brasília: TCU, 1991. Descreve formas de organizar auditorias de sistemas e se aplica bem a ideia da auditoria como uma atividade de controle.

VENEZIANO, W. GSIC051: Organizações e Sistemas de Informação(Notas de Aula). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2010. 13 p.

VIDAL, F. B. GSIC202: Controles de Segurança Física e Ambiental (Notas de Aula). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2010. 29 p.

VIEIRA, Tatiana Malta. Direito da Sociedade da Informação. (Notas de Aula). Brasília: Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade de Brasília. 2009. 59 p.