GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Editora da Faculdade de Ciência da Informação
Universidade de Brasília
Série Segurança da Informação

A Série Segurança da Informação visa à publicação de produção bibliográfica desenvolvida junto à Universidade de Brasília e relacionada à pesquisa, ao ensino e à extensão na área da segurança da informação. É editada por Jorge Henrique Cabral Fernandes, professor do Departamento de Ciência da Computação do Instituto de Ciências Exatas e da Pós-Graduação em Ciência da Informação da Faculdade de Ciência da Informação, ambas da Universidade de Brasília. Jorge Fernandes foi coordenador do Curso de Especialização em Gestão da Segurança da Informação e Comunicações – CEGSIC 2007-2008. Possui títulos de Doutor (2000) e Mestre (1992) em Informática pelo Centro de Informática da Universidade Federal de Pernambuco. É Especialista em Engenharia de Sistemas pelo Departamento de Informática e Matemática Aplicada da Universidade Federal do Rio Grande do Norte (1988) e Bacharel em Ciências Biológicas pelo Centro de Biociências da Universidade Federal do Rio Grande do Norte (1987). Servidor público de universidades federais desde 1984, atualmente se dedica à pesquisa, ensino e extensão nas áreas de informação e computação, com ênfase em fundamentos, gestão e governança da segurança.

Jorge Henrique Cabral Fernandes

GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Série Segurança da Informação

2010

Volume I

Editado pela Faculdade de Ciência da Informação
Universidade de Brasília
Brasília - Brasil

Desenvolvido em atendimento ao de trabalho do Programa de

Disponível também em formato e-book: <http://cegsic.unb.br>

Ficha Catalográfica
Dados Internacionais de Catalogação na Publicação (CIP)

G393 Gestão da segurança da informação e comunicações : volume 1 / Jorge Henrique Cabral Fernandes, organizador.- Brasília : Faculdade de Ciência da Informação, c2010.
125 p. ; 23 cm.

Inclui bibliografia.

1. Gestão da informação. 2. Segurança da informação e comunicações. I. Fernandes, Jorge Henrique Cabral (org.).

CDU 004.056

Arte gráfica e impressão: Gráfica da ABIN

Luiz Inácio Lula da Silva
Presidente da República

Fernando Haddad
Ministro da Educação

UNIVERSIDADE DE BRASÍLIA
José Geraldo de Sousa Junior
Reitor

João Batista de Sousa
Vice-Reitor

Pedro Murrieta Santos Neto
Decano de Administração

Rachel Nunes da Cunha
Decana de Assuntos Comunitários

Márcia Abrahão Moura
Decana de Ensino de Graduação

Ouviromar Flores
Decano de Extensão

Denise Bomtempo
Decana de Pesquisa e Pós-graduação

Noraí Romeu Rocco
Diretor do Instituto de Ciências Exatas

Priscila Barreto
Chefe do Departamento de Ciência da Computação

Jorge Henrique Cabral Fernandes
Coordenador do CEGSIC 2007-2008

Alex Harlen
Revisor de Língua Portuguesa

Mônica Regina Peres
Revisora Normativa

Jorge Armando Félix
Ministro-Chefe 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

AGRADECIMENTOS

O resultado apresentado neste livro não poderia ter sido produzido sem a valiosa contribuição e suporte de muitos colegas, a maioria de servidores públicos que atuam dentro e fora da Universidade de Brasília. Estendo meus agradecimentos aos técnicos e alunos do Departamento de Ciência da Computação da UnB, que forneceram o apoio logístico à realização do curso. Aos professores colegas do Instituto de Ciências Exatas, do Departamento de Ciência da Computação e da Universidade de Brasília, tanto pelo envolvimento de alguns na realização do curso, quanto pelos valiosos comentários e críticas construtivas na condução e ajustes do CEGSIC 2007-2008. Embora sujeito a inevitáveis omissões, expresso meus agradecimentos pessoais a Alan Correa, André Ancona Lopez, Arthur Nóbrega, Célia Ghedini Ralha, Cesar Fonseca, Cláudia Canongia, Fabrício Braz, Fernanda Fernandes, Fernando Schelb, Georgina Mandarino, Gilberto de Oliveira Netto, Guilherme Marques, Honório Crispim, Humberto Abdalla, Indiana Kosloski de Medeiros, Isabella Tavares, João José Costa Gondim, Kenia Alvarenga, Leidiane Cardoso, Leonardo Lazarte, Maísa Pieroni, Magda Fernandes, Marco Carvalho, Marcos Allemand, Maria Nilza Mendonça, Maria do Carmo Mendonça, Maria Helena do Carmo, Nathalia Alvarenga, Norai Romeu Rocco, Odacyr Luiz Timm Júnior, Paula Fernandes, Paulo Gondim, Paulo Hidaka, Pedro Freire, Polyana Souza, Raphael Mezzomo, Ricardo Sampaio, Tarcísio Freire Junior, Ulysses Machado e Vitor Fujimoto.

Agradeço também ao apoio da Editora da Faculdade de Ciência da Informação (FCI) da UnB, na pessoa da Professora Elmira Simeão, pela oportunidade de publicar, pela editora citada, esta obra e pela oferta de serviços profissionais que melhoraram a qualidade dos resultados, atestando a importância do profissional de informação na disseminação do conhecimento.

Agradeço a confiança no Departamento de Ciência da Computação da UnB, depositada pelo General Jorge Armando Félix, Ministro-Chefe do Gabinete de Segurança Institucional; pelo Sr. Raphael Mandarino Júnior, Diretor do Departamento de Segurança da Informação e Comunicações, que construiu uma visão de que seria possível a realização do CEGSIC; pelos Coronéis Reinaldo Silva Simião e Macarino Freitas, responsáveis pela co-gestão e ajustes no curso, sempre na forma de um proveitoso diálogo. Também agradeço à Doutora Claudia Canongia, pesquisadora do INMETRO cedida ao DSIC/GSIPR, pelo estímulo e orientações essenciais para a publicação deste livro.

Agradeço também a gentil colaboração das organizações públicas a seguir citadas, que nos receberam durante os seminários de gestão da segurança, pois do contato com seus representantes pudemos ter a oportunidade de discutir situações práticas vivenciadas por cada órgão público no trato de suas informações e comunicações: Banco do Brasil (BB), Caixa Econômica Federal (CEF), Departamento de Polícia Federal (DPF), Exército Brasileiro (EB), Ministério da Defesa (MD), Ministério da Agricultura, Pecuária e Abastecimento (MAPA), Departamento de Segurança de Informações e Comunicações (DSIC), Superior Tribunal Eleitoral (TSE), SERPRO e Estação de Rádio da Marinha do Brasil (ERMB).

Por fim, não poderia deixar de agradecer e homenagear alunos e alunas que participaram do CEGSIC 2007-2008, que são autores deste trabalho, pelo empenho e entusiasmo demonstrados durante os quase dois anos de intensas atividades do curso. Sem o espírito valoroso de vocês, mesmo nos momentos de grande cansaço devido à dupla carga de trabalho quando da realização do curso, não teríamos avançado tanto nesses últimos 4 anos, na discussão desse

atuação de vocês, por vossas organizações, pelo serviço público e pela sociedade brasileira.

Jorge Fernandes

Brasília, Distrito Federal
Novembro de 2010

. . .

Quando conheces a ti
mesmo e aos outros,

a vitória não está
ameaçada.

quando conheces o céu
e a terra,

a vitória é inesgotável.

Sun Tzu, em A Arte da Guerra

LISTA DE TABELAS

SUMÁRIO

APRESENTAÇÃO

É com satisfação que apresento este Livro, o qual reúne produções intelectuais, de alto nível, nos mais variados assuntos acerca de Gestão de Segurança da Informação e Comunicações (GSIC), tema consideravelmente importante ao Estado brasileiro, em face de sua complexidade nos panoramas nacional e internacional.

Investir em capacitação sempre foi prioridade do Gabinete de Segurança Institucional da Presidência da República. Este Livro concretiza tal ação, pois o resultado aqui apresentado vem ao encontro dos níveis insatisfatórios de investimento e conhecimento, sobre Segurança da Informação e Comunicações, apresentados, em 2003, pelos órgãos da Administração Pública Federal, direta e indireta.

Uma Doutrina Nacional de Gestão da Segurança da Informação e Comunicações, no âmbito dos órgãos e entidades da APF compreende: conceitos, princípios, diretrizes, métodos, técnicas, habilidades e competências no plano gerencial. Tal cultura deve ser disseminada junto aos servidores públicos, bem como junto às organizações nas quais atuam.

Não tenho dúvidas que este Livro é fundamento essencial para a concepção de metodologia de Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, e para a elaboração de normas e padrões mínimos necessários para assegurá-la.

Recomendo, portanto, a leitura deste Livro, cuja publicação considero

incidentes de segurança da informação e comunicações e para a implantação de processos concisos, que garantam a continuidade do negócio nos momentos de crise.

Boa leitura!

Jorge Armando Felix

Ministro Chefe do Gabinete de Segurança Institucional

da Presidência da República

CAPÍTULO 1

PRÓLOGO

Este livro é um registro parcial da produção intelectual desenvolvida pela primeira turma do Curso de Especialização em Gestão da Segurança da Informação e Comunicações, realizado pelo Departamento de Ciência da Computação da Universidade de Brasília, CEGSIC 2007-2008.

O curso foi realizado em resposta ao convite, seguido de colaboração, apoio e aporte de recursos organizacionais e financeiros pelo Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil, mais especificamente pelo Departamento de Segurança da Informação e Comunicações (DSIC/GSIPR). Foi produzido para atendimento à Portaria 17/2007 GSIPR.

O CEGSIC 2007-2008, iniciou-se formalmente em novembro de 2007 e sua conclusão ocorreu em meados do ano de 2009. O CEGSIC 2007-2008 teve carga horária de 375 horas aula, realizadas em regime presencial, nas dependências da Universidade de Brasília. Contou com a participação e apoio de docentes e técnicos dos Departamentos de Ciência da Computação, Engenharia Elétrica e Ciências da Informação e Documentação da UnB, bem como com professores e pesquisadores de fora da UnB.

A parte I deste livro descreve em mais detalhes as motivações e conceitos subjacentes à realização do CEGSIC 2007-2008.

Os alunos e alunas do CEGSIC 2007-2008 foram selecionados por meio de entrevistas realizadas pela coordenação do curso. O horário de realização das aulas do curso foi principalmente o noturno, visto que não havia ssibilidade de realizá-lo integralmente durante o horário de expediente dos

servidores públicos que nele ingressaram. Visitas a organizações diversas, públicas e privadas, localizadas em Brasília, foram realizadas nos horários matutino ou vespertino.

Os 40 servidores ingressantes no CEGSIC 2007-2008 pertenciam aos seguintes órgãos:

- Advocacia Geral da União (AGU)
- Agência Brasileira de Inteligência (ABIN)
- Banco Central do Brasil (BACEN)
- Casa Civil da Presidência da República
- Controladoria Geral da União (CGU)
- Departamento de Segurança da Informação e Comunicações (DSIC)
- Exército Brasileiro (EB)
- Força Aérea Brasileira (FAB)
- Gabinete de Segurança Institucional da Presidência da República (GSIPR)
- Marinha do Brasil (MB)
- Ministério da Previdência Social (MPS)
- Ministério da Defesa (MD)
- Ministério da Saúde (MS)
- Departamento de Polícia Federal (DPF)
- Secretaria da Receita Federal (SRF)

Após conclusão com sucesso das 25 disciplinas do curso, seguida de pesquisa, elaboração de monografia, defesa bem sucedida e entrega da versão final da monografia impressa e em formato digital, os 35 servidores que concluíram o curso em seu prazo regulamentar receberam o título de especialista pela Universidade de Brasília.

As 35 monografias sumarizadas nas Partes II e III deste livro estão disponíveis para consulta, de forma plena ou parcial, e constituem rico acervo de conhecimento sobre segurança da informação no serviço público federal. Espera-se que venham auxiliar na construção dos elementos de uma metodologia brasileira de gestão da segurança da informação e comunicações.

Os 35 resumos foram produzidos pelos autores listados a seguir, por ordem alfabética: Alessandro de Sá Barbosa, Antônio Carlos Pereira de Britto, Antônio Magno Figueiredo de Oliveira, Danielle Rocha da Costa, Edílson Fernandes da Cruz, Everardo de Lucena Tavares, Gerson Ben-Hur Mayer, Gerson Charbel Costa, Gilberto Dias Palmeira Júnior, Henrique Aparecido da Rocha, Idilson Alexandre Palhares Cassilhas, Iná Lúcia Cipriano de Oliveira Monteiro, Jorge Euler Vieira, Juscelino Kilian, Kleber Ferreira Rangel, Liliana Suzete Lopes de Queiroz Campos, Lindeberg Pessoa Leite, Luiz Guilherme Sá da Silva, Mônica Costa Tkaczyk Martins, Marcelo Paiva Fortenele, Marcos Ambrogi Leite, Newton Daltro Santos, Paulo César Cardoso Rocha, Paulo Hideo Ohtoshi, Pedro Jorge Sucena Silva, Raphael Mandarino Júnior, Reinaldo Silva Simião, Renato do Carmo das Neves Alves, Roberto Moutella Pimenta, Roberto Ribeiro Bastos, Rogério Xavier Rocha, Rubem Ribeiro Veloso, Sergio Roberto Fuchs da Silva, Silvana Crispim Loureiro e Vitor Friedenhain.

PARTE I

MOTIVAÇÕES, PLANEJAMENTOS E AÇÕES

CAPÍTULO 2

A SEGURANÇA DOS SISTEMAS NA ADMINISTRAÇÃO PÚBLICA

A evolução tecnológica contribui para que as organizações automatizem seus serviços, em direção a maior eficiência e eficácia. Mas há uma contrapartida do processo, que demanda cuidados frente às ameaças a que se tornam expostos os sistemas de informação e comunicação, especialmente quando conectados à rede mundial de computadores.

O NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR - NIC.br (2010) apresenta resultados de uma pesquisa sobre o tamanho da web brasileira no domínio .gov.br, isto é, no domínio onde se supõe encontrar a presença, na Internet, da maioria das organizações da administração pública direta do Brasil. Segundo a pesquisa, realizada em outubro de 2009, foram identificados 18.796 sítios sob o domínio .gov.br, sendo que cerca de 25% desses sítios são vinculados à esfera federal, e os demais às esferas estaduais ou municipais.

2.1 TECNOLOGIA E APERFEIÇOAMENTO DA ADMINISTRAÇÃO PÚBLICA

A administração pública brasileira, assim como os governos de muitos países em franco desenvolvimento, encontra-se sob intensa pressão por aperfeiçoamento, visando atender à demanda por serviços com maior qualidade, em resposta à pressão de cidadãos cada vez mais integrados à

Sociedade da Informação[1]. Um dos reflexos desse desenvolvimento é o conjunto de ações em torno da Gestão Pública do MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO (2009).

Supõe-se que a adoção de sistemas computadorizados na administração pública forneça um considerável apoio ao aperfeiçoamento da gestão pública, seja devido à transparência na qual se ofertam seus serviços, seja no apoio a operações em volume e extensão geográfica compatíveis com as dimensões populacional e territorial brasileiras. Tais medidas, quando combinadas com ações de formação de recursos humanos, podem produzir um ciclo virtuoso, que aumenta o desempenho e estimula novas demandas por atuação do governo, especialmente necessárias no atendimento à redução das desigualdades sociais ainda muito grandes no país.

Os sistemas computadorizados constituem parte essencial dos Sistemas de Informação[2] e Sistemas de Comunicação[3] (coletivamente chamados de SICs), e são cada vez mais críticos à atuação das organizações, inclusive da administração pública.

Os SICs, sejam eles pertencentes a organizações públicas ou privadas, são também mais complexos e automatizados que seus antecessores, e visam incrementar a eficiência operacional e gerencial dos processos de trabalho, de produção, de prestação de serviços e de realização de negócios pelas organizações que os implantam.

2.2 RISCOS À SEGURANÇA

Em contrapartida à melhoria em decorrência do aporte tecnológico, surge a demanda por maior nível de segurança das informações e dos processos de

[1] Veja informações recentes e históricas sobre a constituição da sociedade de informação no Brasil em obras como CENTRO DE ESTUDOS SOBRE AS TECNOLOGIAS DA INFORMAÇÃO E DA COMUNICAÇÃO - CETIC.br (2009) e TAKAHASHI (Org.) (2000).

[2] Segundo a Wikipedia (http://pt.wikipedia.org/wiki/Sistema_de_informaçao) um Sistema de Informação é um sistema automatizado (que pode ser denominado como Sistema de Informação Computadorizado) ou manual, que abrange pessoas, máquinas e/ou métodos organizados para coletar, processar, transmitir e disseminar dados que representam informação para o usuário e/ou cliente.

[3] Sistemas de Comunicação são sistemas que permitem a comunicação, seja ela entre humanos ou entre máquinas. Ver http://en.wikipedia.org/wiki/Communication.

comunicações, a fim de garantir o adequado funcionamento dos sistemas, frente a um grande número de ameaças[4].

Avaliando-se superficialmente a situação dos órgãos públicos brasileiros, no que se refere à Gestão da Segurança de seus sistemas computadorizados, detecta-se um conjunto de características únicas e preocupantes. Há grande heterogeneidade de soluções no plano tecnológico, bem como de métodos e processos no plano gerencial[5]. No plano da segurança física e lógica, a sociedade brasileira não passou pelas mesmas experiências históricas de outros países nos quais já houve forte desenvolvimento de tecnologias, e, desta forma, nossa cultura[6] parece não se adequar aos métodos e conceitos de segurança já desenvolvidos nesses países.

Em contraponto a um pequeno volume de investimentos em pesquisa e inovação em segurança, há um alto volume de investimentos em aquisições no desenvolvimento de sistemas de informação e comunicações. No entanto, estes investimentos em aquisições de tecnologias para sistemas de informação e sistemas de comunicação ainda ocorrem com pouco planejamento e acompanhamento de resultados, além de pouco planejamento para manutenção e evolução, sobretudo no que concerne à segurança da informação e comunicações. Além das várias instruções normativas lançadas pelo DSIC/GSIPR nos últimos anos, a Instrução Normativa 04 da SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO DO MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO (2008) é uma importante resposta a essa situação.

Dessa forma, configura-se um cenário de riscos crescentes para o Estado e governos, e consequentemente para a própria sociedade brasileira. Esses riscos se apresentam tanto como oportunidades, quanto também como ameaças, sendo que a gestão da segurança ocorre no plano das ameaças, isto é, dos riscos à segurança.

2.3 CAPACIDADES GERENCIAIS EM SEGURANÇA

Os riscos à segurança dos sistemas de informação públicos parecem decorrentes da combinação entre aumento da conectividade dos SICs públicos à Internet, especialmente na busca por ofertar serviços de Governo Eletrônico, e o descompasso entre o rápido avanço da complexidade dos

[4] Veja em http://www.net-security.org/secworld.php?id=8709 uma lista das 10 principais ameaças à segurança da informação, segundo a empresa Perimeter E-Security.
[5] Veja, por exemplo, os resultados das pesquisas sobre Governança de TI feitas pelo TRIBUNAL DE CONTAS DA UNIÃO (2008).
[6] Veja um manifesto sobre a cultura de paz no Brasil em http://www.cultura.gov.br/site/2003/03/10/o-brasil-quer-paz-por-gilberto-gil/.

sistemas e o lento avanço das capacidades gerenciais das organizações que os desenvolvem.

Configura-se uma lacuna na capacitação de servidores públicos voltados à Gestão da Segurança da Informação e que sejam comprometidos com a eficácia dos SICs públicos. O preenchimento dessa lacuna demanda soluções imediatas, que não se encontram disponíveis "em prateleiras", mas tão somente são possíveis através de processos de educação, treinamento e conscientização de pessoal permanente dos quadros de servidores da Administração Pública Federal, envolvendo gestão de conhecimento e comunidades de prática[7].

Para redução dos riscos se faz também necessário melhorar as percepções, atitudes, capacidades técnicas e ações gerenciais dos servidores públicos no que concerne ao valor estratégico da informação e da comunicação públicas, e aos cuidados com a gestão da segurança dessas informações, de suas tecnologias de suporte. Tais competências devem ser combinadas com o contínuo alinhamento ao interesse público, inclusive à transparência.

Os gestores públicos da segurança devem ser capazes de planejar, organizar, adquirir, implantar, implementar, dirigir e controlar, de forma efetiva, os programas, projetos, ações e sistemas de segurança que contribuam para o funcionamento adequado dos SICs públicos[8].

2.4 CONSTRUÇÃO DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Desenvolve-se no Brasil, sob os auspícios do Gabinete de Segurança Institucional da Presidência da República, GSIPR, mais especificamente no Departamento de Segurança da Informação e Comunicações, DSIC[9], o conceito de Segurança da Informação e Comunicações. A abordagem de SIC (Segurança da Informação e Comunicações) considera como pilares da ação da segurança o alcance primário da Disponibilidade, Integridade, Confidencialidade e Autenticidade da informação, conhecida como

[7] Ver Wenger, McDermott e Snyder (2002) sobre propostas de como proceder à gestão do conhecimento por meio da construção de comunidades de prática.

[8] O conceito de sistema de gestão da segurança da informação proposto nas normas da ISO/IEC (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2006), bem como adotado nas normas do DSIC/GSIPR como GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA (2008) e DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR (2008) contemplam as ações citadas.

[9] Veja na página http://dsic.planalto.gov.br as ações relacionadas ao conceito.

“D.I.C.A. de Segurança da Informação” e a questão da Segurança Cibernética, entre outras.

O conceito de Segurança da Informação e Comunicações surge no momento que o país amadurece e a administração pública federal aperfeiçoa-se, pondo dúvidas quanto à conveniência, ou não, de se adotar integralmente as “doutrinas” desenvolvidas em outros países, considerando que possuímos diferentes necessidades de proteção, bem como cultura e história próprias.

CAPÍTULO 3

PANORAMA INTERNACIONAL DA SEGURANÇA DA INFORMAÇÃO

A Gestão da Segurança da Informação e a Garantia da Informação são duas das abordagens internacionalmente conhecidas para a busca da integridade, disponibilidade, confidencialidade e autenticidade de sistemas de informação. Note que abordagens "de gestão" estendem as de segurança computacional tecnológica. Enquanto que a segurança computacional (ANDERSON, 2001; SCHNEIER, 1996), a segurança de redes (SYSTEMS AND NETWORK ATTACK CENTER - SNAC, 2006; CONVERY, 2004; STALLINGS, 2008) a segurança de dados (LITCHFIELD et al., 2005) e a segurança de código ou software (HOGLUND; MCGRAW, 2004) ocorrem por meio da implantação e operação da criptografia, dos mecanismos de autenticação, dos sistemas de defesa de redes de computadores e de tolerância a falhas, entre outros, a gestão da segurança da informação busca o alinhamento entre as necessidades organizacionais de segurança e o gerenciamento dos sistemas de informação, não apenas no que concerne ao emprego de tecnologias, mas com ênfase em aspectos de risco (DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR, 2009b; STONEBURNER; GOGUEN; FERINGA, 2002; PELTIER, 2001; ISO/IEC, 2007; ALBERTS; DOROFEE, 2002), política organizacional (GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, 2008; DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR, 2009a; CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA, 2001; BRASIL, 2000), recursos humanos

na área de segurança (DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR, 2009c; LEACH, 2003), segurança física e ambiental (DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR, 2010a), processos e métodos de gestão aplicáveis ao desenvolvimento, operação e manutenção de sistemas (DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR, 2008; DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR, 2010b; SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO DO MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO, 2008; HOWARD; LIPNER, 2006), além de foco na continuidade dos serviços e negócios das organizações (DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR, 2009d; ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2008).

O estado da prática da Gestão da Segurança da Informação é fruto do desenvolvimento de métodos oriundos do Ministério de Indústria e Comércio do Reino Unido[10], e consolida-se nas normas desenvolvidas pelo órgão britânico de padronização BS (British Standards), posteriormente incorporadas pela ISO/IEC. A abordagem da ISO/IEC à segurança da informação, representada sobretudo na série de normas 27000[11], alinha-se com uma ação mais ampla de melhoria na gestão da informação, e seu desenvolvimento inevitavelmente incorpora o princípio da Governança (THE INTERNATIONAL BANK FOR RECONSTRUCTION AND DEVELOPMENT and THE WORLD BANK, 2006). A governança de TI, a mais conhecida dos modelos de governança, busca o alinhamento entre a área de tecnologia da informação de uma organização e as necessidades de informação organizacionais, e é amplamente divulgada por meio do modelo COBIT (IT GOVERNANCE INSTITUTE, 2007). A governança da segurança da informação, conceito emergente no cenário internacional, busca o alinhamento entre a área da segurança da informação e as necessidades organizacionais de segurança[12].

Outra corrente de práticas de gestão da segurança da informação é a Garantia da Informação (Information Assurance) estabelecida por meio da NSA -

[10] Ver mais alguns comentários em http://www.anupnarayanan.org/ism3andiso27001.pdf.

[11] A série ISO/IEC 27000 foi adotada no Brasil pela ABNT, e suas normas podem ser obtidas em língua portuguesa através do sítio http://www.abnt.org.br/.

[12] Veja mais detalhes em http://www.isaca.org/Knowledge-Center/Research/Documents/InfoSecGuidanceDirectorsExecMgt.pdf.

National Security Agency do Governo dos EUA[13]. A abordagem de Information Assurance[14] é também baseada na gestão de riscos (STONEBURNER; GOGUEN; FERINGA, 2002), só que complementa, aos aspectos normativos, ações visando formação de servidores públicos e redes de escolas e universidades para atuação na proteção de infraestruturas de informação, no combate ao ciberterrorismo e na proteção dos sistemas de informação estratégicos do Governo dos EUA. Os aspectos tecnológicos normativos da gestão da segurança foram consolidados pelos trabalhos da Divisão de Segurança Computacional (CSD - Computer Security Division) do NIST[15] (National Institute of Standards and Technology[16]), por meio de suas responsabilidades estabelecidas na Lei de Reforma da Gestão da Tecnologia da Informação (Information Technology Management Reform Act) do ano de 1996 e da Lei Federal de Gestão da Segurança da Informação, conhecida como FISMA - Federal Information Security Management Act[17].

Em ambas correntes doutrinárias, seja a da ISO/IEC, seja a da NSA, a prática da gestão da segurança da informação depende da atuação dos agentes humanos nas organizações, contribuindo com visões multidisciplinares para solucionar a questão da segurança, empregando conhecimentos de tecnologias da informação e comunicação, bem como da gestão da qualidade e da governança. Mais informações podem ser obtidas em Fernandes (2009).

[13] Um glossário dos termos relacionados à Information Assurance pode ser visto em COMITTEE ON NATIONAL SECURITY SYSTEMS (2010).

[14] Veja a página que apresenta a abordagem em http://www.nsa.gov/ia/ia_at_nsa/index.shtml.

[15] Ver http://csrc.nist.gov/.

[16] Ver http://www.nist.gov/index.html.

[17] Para uma introdução ao FISMA ver http://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002.

CAPÍTULO 4

EM BUSCA DE UMA DOUTRINA

Considerando que:

- o desenvolvimento de habilidades gerenciais em segurança da informação demanda formação tipicamente presente nos profissionais de nível superior que atuam nas organizações públicas federais;
- os problemas de segurança da informação manifestam-se de forma bastante prática no seio das organizações;
- os fenômenos subjacentes à segurança não são tão bem compreendidos quanto as manifestações de incidentes de segurança, descontinuidades de processos e crises organizacionais;

mostra-se conveniente formular um programa de formação de gestores em segurança com caráter de aplicação prática, bem como de investigação sistemática de problemas de Gestão da Segurança da Informação e Comunicações baseado no método científico[18].

Diante desse cenário, a Universidade de Brasília (UnB), por meio de seu Departamento de Ciência da Computação, atendendo à demanda do Departamento de Segurança da Informação e Comunicações, propôs e

[18] Veja em Descartes (1962) as justificativas para a adoção de abordagem científica à compreensão das coisas que nos cercam.

executou um Curso de pós-graduação Lato Sensu, baseado no envolvimento de docentes, pesquisadores e alunos de pós-graduação e graduação na UnB, para a investigação e proposição de elementos de uma Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

Uma Doutrina Nacional de Gestão da Segurança da Informação e Comunicações aplicável nos órgãos e entidades da Administração Pública Federal deveria compreender a definição de um conjunto de conceitos, princípios, diretrizes, métodos, técnicas, habilidades e competências no plano gerencial da segurança dos SICs públicos, a ser desenvolvido junto aos servidores públicos, bem como junto às organizações nas quais estes atuam.

Uma doutrina[19] pode ser definida como um código de crenças, um corpo de ensinamentos ou instruções que são professadas em uma determinada área do conhecimento. Segundo a Wikipedia, doutrina tem sua origem na palavra grega doctrina, que possui significado análogo a catecismo. O termo doutrina é empregado em áreas como Política Externa[20], Religião[21], Militar[22], Política Interna (DOCKHORN, 1999) e Direito[23].

Embora o termo doutrina possa ser usado com a conotação de um conjunto de dogmas, é possível, e necessário, que uma doutrina seja desenvolvida segundo uma abordagem dialética[24] para permitir o aperfeiçoamento contínuo do estado da prática dos grupos que a empregam.

No âmbito das organizações públicas atuais, o termo metodologia[25] apresenta melhor adequação que o termo doutrina. Uma metodologia

[19] Ver várias definições alternativas para o termo doutrina em http://en.wikipedia.org/wiki/Doctrine.
[20] Veja a Doutrina de Política Externa da Alemanha, após 1955, em http://en.wikipedia.org/wiki/Hallstein_Doctrine.
[21] Veja verbete sobre doutrina na Enciclopédia Britânica em http://www.britannica.com/EBchecked/topic/167440/doctrine.
[22] Veja, por exemplo, a doutrina de operações de paz da ONU em http://pbpu.unlb.org/pbps/Library/Capstone_Doctrine_ENG.pdf
[23] Veja uma grande compilação de doutrina jurídica em http://jus.uol.com.br/doutrina/.
[24] Dialética consiste em considerar argumentos sob pontos de vista conflitantes, visando a construção de uma síntese de melhor qualidade que as anteriores. Para maiores detalhes veja a definição do método dialético em http://pt.wikipedia.org/wiki/Dialética.
[25] Ver em http://en.wikipedia.org/wiki/Methodology, http://www.merriam-webster.com/dictionary/methodology e

descreve, em linguajar técnico ou científico[26], uma compilação de métodos, técnicas, processos e ferramentas em uso e constante aperfeiçoamento por uma comunidade ou grupo social para solução de um determinada questão.

4.1 ELEMENTOS DE UMA METODOLOGIA OU DOUTRINA

Uma metodologia, ou doutrina, que seja aplicável à Gestão da Segurança da Informação e Comunicações deve conter os seguintes elementos:

- prescrição de adoção, isto é, onde e sob quais condições sua aplicação é adequada;
- prescrição sobre a organização do espaço de atuação das pessoas da segurança;
- prescrição sobre a organização do espaço tecnológico de automação da segurança;
- prescrição sobre a atuação operacional do pessoal da segurança;
- prescrição para gestão dos elementos organizados.

Se considerarmos que o objetivo de uma metodologia de Gestão da Segurança da Informação e Comunicações é gerenciar a segurança nas organizações públicas brasileiras, aplicam-se à definição dos elementos acima, as características e restrições que regulam o funcionamento de órgãos públicos no país, que podem ser sumarizados pelo atendimento aos preceitos constitucionais[27] da legalidade, impessoalidade, moralidade, publicidade e eficiência, dentre outros.

---

http://www.google.com/search?q=define:methodology algumas definições mais detalhadas para o termo metodologia.

[26] Ver em http://pt.wikipedia.org/wiki/Ciencia um conjunto de definições bastante completo sobre o que é ciência.

[27] Ver no caput do Artigo 37 da Constituição (http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm) o enunciado dos princípios da administração pública.

CAPÍTULO 5

CEGSIC: PESQUISA E ENSINO EM GESTÃO DA SEGURANÇA

O Curso de Especialização em Gestão da Segurança da Informação e Comunicações (CEGSIC) foi criado para atender à necessidade de consolidação de uma metodologia brasileira de GSIC, sobre demanda do DSIC/GSIPR.

O curso foi concebido a partir de desenvolvimentos pré-existentes no panorama internacional da segurança da informação, bem como no nascente conceito de Segurança da Informação e Comunicações, criado no Gabinete de Segurança Institucional da Presidência da República. Adota abordagem baseada na integração entre teorias e práticas gerenciais de segurança da informação. É um curso voltado para turmas de gestores, com foco relacionado à gestão de sistemas de informação e sistemas de comunicação.

O Curso exige que os servidores públicos que o frequentam, alunos e alunas, possuam experiência prévia e interesse na gestão de sistemas de informação públicos, seja no referente ao aspecto tecnológico (bases de dados, software ou rede e sistemas de computadores), procedimental e organizacional (atividades em equipes), bem como do ambiente corporativo normativo (legislação e ambiente).

Dentro desta perspectiva, além de empreenderem estudo voltado para os tópicos apresentados em disciplinas de um curso de pós-graduação típico, os servidores públicos são expostos a relatos de estudos de caso e experiências apresentadas por praticantes da área, vinculados a organizações públicas, privadas, mistas e da área de defesa. Muitos desses relatos decorrem da

formação das redes de troca de informações estabelecidas entre os servidores durante o curso. Desse modo, são fortalecidas as ligações entre a realidade na qual muitos trabalham e as teorias e métodos de gestão, tecnologia e relações humanas discutidos em sala de aula. Esta abordagem visa criar experiências de aprendizagem significativa.

Para que o curso seja concluído com sucesso é necessário que os servidores públicos realizem uma pesquisa de caráter científico, a partir da qual elaboram e defendem uma monografia de caráter individual, acerca de um problema de gestão da segurança associado à sua atividade profissional, às vezes com proposição de soluções.

O Capítulo 6 e a Parte III deste livro apresentam visões gerais e resumos das monografias que foram defendidas com sucesso pelos alunos e alunas da turma 2007-2008.

Na turma de 2007-2008, as disciplinas do CEGSIC foram divididas em seis trilhas. As trilhas de disciplinas realizadas abordaram: (i) Teoria; (ii) Indivíduo e Sociedade; (iii) Reflexão e Pesquisa; (iv) Tecnologias; (v) Gestão da Segurança da Informação e (vi) Seminários de Gestão.

Na trilha Teoria, foram apresentadas teorias multidisciplinares da segurança da informação, por meio da abordagem sistêmica.

Na trilha Indivíduo e Sociedade, foram apresentados aspectos teóricos e práticos da sociologia, psicologia, administração e legislação relacionadas à segurança da informação e comunicações.

Na trilha Reflexão e Pesquisa, foram fornecidos os suporte crítico e metodológico que favoreceu a elaboração de estudos científicos voltados para o tema multidisciplinar da Gestão da Segurança.

Na trilha Tecnologias, foram abordadas algumas das principais tecnologias de suporte à gestão da informação e comunicações, juntamente com os problemas de segurança relacionados ao uso destas.

Na trilha Gestão da Segurança da Informação, foram abordados os temas usuais da gestão da segurança das tecnologias da informação e comunicação.

Na trilha Seminários de Gestão, foram apresentados e discutidos estudos de caso relacionados com segurança da informação, ocorridos em empresas públicas e privadas. Muitas das informações foram coletadas durante visitas às próprias organizações.

Devido à premência da discussão sobre o tema e elaboração da metodologia já referenciada, as disciplinas do curso foram realizadas de forma intensiva, sendo um módulo por semana. Foi intensivo o suporte à discussão e à retenção de conhecimentos por meios de um ambiente de educação à

distância baseado na plataforma Moodle[28] e seus vários instrumentos de apoio à aprendizagem, como Tarefas, Wikis, Fóruns, Questionários, além do uso de mapas conceituais[29] e textos de apresentação conceitual (CANONGIA, 2008; FERNANDES, 2007; BORDIM, 2009; GONDIM, 2008a; GONDIM, 2008b; NASCIMENTO, 2008; REZENDE, 2009; MALTA, 2007; HARGER, 2008; BERGER, 2008; BARRETO, 2008; COSTA, 2008b; RALHA, 2008; NETTO; ALLEMAND; FREIRE, 2007; NETTO et al., 2008; BORDIM, 2008a; BORDIM, 2008b; BRAZ, 2008; CARNIELLI, 2008; FERNANDES, 2008d; FERNANDES, 2008b; FERNANDES, 2008a; FERNANDES, 2008c) com referências para leituras adicionais. O áudio da maioria das aulas presenciais também foi gravado em meio digital, para que fosse possível a compensação de aulas perdidas em caso de viagem a trabalho de algum aluno durante o curso.

A Tabela 5.1 apresenta a lista das disciplinas ofertadas durante o CEGSIC 2007-2008 e a lista dos docentes, pesquisadores e consultores que atuaram nas mesmas.

TABELA 5.1: Docentes, pesquisadores e (ou) consultores que participaram de disciplinas do CEGSIC 2007-2008.

DISCIPLINA OU TRILHA	DOCENTES, PESQUISADORES E (OU) CONSULTORES
Ataques, Intrusões e Investigação Forense em Sistemas de Computação	MSc. João José Costa Gondim
Auditoria e Certificação de Segurança da Informação	Dr. Jorge Henrique Cabral Fernandes
Direito na Sociedade da Informação	Me. Tatiana Malta Vieira
Controles de Acesso Lógico	Dra. Priscila America Solis Mendez Barreto
Controles de Segurança da Informação	PhD Jacir Luiz Bordim
Criptografia e Infraestrutura de Chaves Públicas	PhD Anderson Clayton Alves Nascimento
Estratégias e Doutrinas para Governança da Segurança da Informação e Comunicações	Dr. Jorge Henrique Cabral Fernandes
Gestão Operacional da Segurança da Informação	Me. Gilberto de Oliveira Netto, Esp. Marcos Allemand e Esp. Pedro André

[28] Ver mais detalhes sobre o Moodle em http://moodle.org.
[29] Veja mais sobre a importante técnica de mapas conceituais em http://pt.wikipedia. org/wiki/Mapa_conceitual.

	Faria Freire
Gestão de Riscos	Dr. Edgard Costa Oliveira
Gestão por Processos e Projetos	PhD Célia Ghedini Ralha
Gestão de Crise e Continuidade	Dr. Jorge Henrique Cabral Fernandes e Dr. Hervaldo Sampaio Carvalho
Inteligência Competitiva	Dra. Claudia Lyrio Canongia e Esp. Celina Maria Lamb
Metodologia Científica	Dr. Mamede Lima-Marques
Modelos de Confiança em Informática	Ms. Pedro Antonio Dourado de Rezende
Pensamento Crítico	Dr. Walter Alexandre Carnielli
Projeto de Monografia	Dr. Jorge Henrique Cabral Fernandes
Políticas, Procedimentos e Normas de Segurança da Informação	Ms. Gilberto de Oliveira Netto, Esp. Marcos Allemand, Esp. Pedro André Faria Freire e Ms. Maria do Carmo Mendonça
Redes de Computadores	PhD Jacir Luiz Bordim
Segurança em Aplicações	Me. Fabríçio Ataídes Braz
Segurança Física de TI	Dr. Pedro Azevedo Berger e Esp. Vera Parucker Harger
Seminários de Gestão da Segurança da Informação e Comunicações (Trilha)	Dr. Jorge Henrique Cabral Fernandes e Me. Odacyr Luiz Timm Júnior
Sistemas Complexos	Dr. Jorge Henrique Cabral Fernandes
Sociedade da Informação	Dra. Magda Fernanda Medeiros Fernandes

PARTE II

MONOGRAFIAS E ÁREAS TEMÁTICAS

CAPÍTULO 6

MONOGRAFIAS DO CEGSIC 2007-2008 E SUAS ÁREAS TEMÁTICAS

As pesquisas realizadas no CEGSIC 2007-2008, e as correspondentes monografias desenvolvidas pelos alunos e alunas, servidores públicos, podem ser organizadas conforme os temas apresentados na Tabela 6.1. A riqueza de trabalhos demonstra o caráter multidisciplinar do problema e algumas possibilidades de abordagens que podem ser desenvolvidas para estudo da questão.

Algumas áreas de estudos estão associadas a corpos de conhecimento internacionalmente reconhecidos, como os propostos pela ISO/IEC ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2006) e ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2005) e mais propositivamente no modelo de certificação profissional CISSP - Certified Information Systems Security Professional (HARRIS, 2005), mantido pelo International Information Systems Security Certification Consortium e alinhado ao conceito de Information Assurance[30]. São exemplos dessas áreas:

- Controle de Acessos
- Segurança em Aplicações

[30] Para mais detalhes sobre o modelo CISSP ver http://en.wikipedia.org/wiki/Certified_Information_Systems_Security_Professional e https://www.isc2.org/default.aspx.

- Planejamento de Continuidade de Negócios e Recuperação de Desastres
- Criptografia
- Gestão da Segurança da Informação e do Risco
- Aspectos Legais, Regulatórios, de Conformidade e Investigações
- Segurança Operacional
- Segurança Física e Ambiental
- Arquitetura e Desenho de Segurança
- Segurança em Telecomunicações e Redes

Temas como Pessoas e Segurança estão mais alinhados com normas como ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2006) e ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2005). A Segurança em Compras e Contratos está alinhada a modelos de Governança de TI como IT GOVERNANCE INSTITUTE (2007). A Gestão de Crises, apresentada nos vários artigos contidos em Smith e Elliot (2006), fundamenta-se no estudo de questões teóricas como os fenômenos emergentes que surgem em sistemas complexos (HOLBROOK, 2006) para estudar o comportamento de organizações e da sociedade em situações de stress. A Defesa e Segurança Cibernéticas também possuem componentes diversos, apoiando-se em aspectos tecnológicos como segurança em aplicações (HOGLUND; MCGRAW, 2004), segurança em redes e telecomunicações (HANSMAN; HUNT, 2005), para construir investigações relacionadas ao Direito Internacional, à Ciência Política e às Ciências Militares.

TABELA 6.1: Enquadramento das Pesquisas conforme Área Temática.

ÁREA TEMÁTICA	ALUNO(A)S E SEÇÕES DO LIVRO
(18) Auditoria e Controle	Alessandro de Sá Barbosa (18.6), Henrique Aparecido da Rocha (18.2), Newton Daltro Santos (18.3), Roberto Ribeiro Bastos (8.3), Rogério Xavier Rocha (18.5), Rubem Ribeiro Veloso (18.4)
Classificação da Informação	Silvana Loureiro (16.1)
(18) Conformidade e Certificação	Alessandro Barbosa (18.6), Henrique da Rocha (18.2), Idilson Cassilhas (19.1), Kleber Rangel (18.1), Rubem Veloso (18.4)
(14) Controle de Acessos	Sergio da Silva (14.1)
(13) Criptografia e Infra	Edílson da Cruz (13.2), Jorge Vieira (13.1),

Estrutura de Chaves Públicas	Sergio da Silva (14.1)
(7) Fundamentos da Segurança	Liliana Campos (7.1), Reinaldo Simião (7.2)
(19) Gestão da Continuidade	Antônio de Oliveira (19.3), Idilson Cassilhas (19.1), Vitor Friedenhain (19.2)
12) Gestão de Crises	Gerson Costa (12.1), Gilberto Palmeira Júnior (12.2)
(16) Gestão da Segurança	Antônio de Britto (16.2), Antônio de Oliveira (19.3), Danielle da Costa (9.1), Juscelino Kilian (16.4), Kleber Rangel (18.1), Mônica Martins (16.3), Pedro Silva (10.2), Silvana Loureiro (16.1)
(10) Gestão do Risco de Segurança	Marcos Leite (15.2), Paulo Ohtoshi (10.1), Pedro Silva (10.2)
(11) Incidentes de Segurança	Roberto Pimenta (11.1)
(8) Pessoas e Segurança	Paulo Rocha (8.1), Renato Alves (8.2), Roberto Bastos (8.3)
(9) Política de Segurança	Danielle da Costa (9.1), Iná Monteiro (9.2)
Processos de Segurança	Roberto Pimenta (11.1)
Segurança Física e Ambiental	Marcos Leite (15.2)
(20) Segurança e Defesa Cibernética	Marcelo Fontenele (20.1), Raphael Mandarino Junior (20.2)
(17) Segurança em Compras e Contratos	Gerson Mayer (17.1)
(15) Segurança em Redes e Telecomunicações	Everardo Tavares (15.1), Lindeberg Leite (15.3), Marcos Leite (15.2)

PARTE III

RESUMOS DAS MONOGRAFIAS DO CEGSIC 2007-2008

TABELA 6.2: Orientadores de Monografias do CEGSIC 2007-2008.

ORIENTADORE(A)S DE MONOGRAFIAS DO CEGSIC 2007-2008
Célia Ghedini Ralha
Edgard Costa Oliveira
Gilberto de Oliveira Netto
Jacir Luiz Bordim
João José Costa Gondim
Jorge Henrique Cabral Fernandes
Magda Fernanda Medeiros Fernandes
Mamede Lima-Marques
Priscila America Solis Mendez Barreto
Ricardo Camelo
Tatiana Malta Vieira

Os resumos das monografias produzidas durante o CEGSIC 2007-2008 são apresentados nos próximos capítulos, precedidos de breve comentário que situa as áreas temáticas nas quais foram agrupados. As apresentações dos resumos foram organizadas conforme a data de defesa. Pequenas edições foram realizadas em alguns resumos, visando dar maior clareza ao texto, mas com o cuidado de preservar o sentido original.

A Tabela 6.2 apresenta, ordenados alfabeticamente, os nomes dos pesquisadores que atuaram na orientação das pesquisas e elaboração de monografias pelos alunos e alunas do curso.

CAPÍTULO 7

FUNDAMENTOS DA SEGURANÇA DA INFORMAÇÃO

Pesquisas sobre fundamentos de um determinado conceito ou prática são usualmente de natureza exploratória e teórica. Buscam o desenvolvimento de uma teoria do conhecimento[31] sobre um determinado assunto.

No CEGSIC 2007-2008, duas monografias abordaram o estudo dos fundamentos da segurança da informação e comunicações. O trabalho de Liliana Suzete Lopes de Queiroz Campos (CAMPOS, 2008) apresenta uma proposta de conceito para "comunicações", fundamentada na necessidade de considerar a comunicação como um elemento formador da cultura. O segundo trabalho, elaborado por Reinaldo Silva Simião (SIMIÃO, 2009), formulou uma interpretação para o conceito de Segurança da Informação e Comunicações, e que passou a ser utilizado pela Administração Pública Federal brasileira com a edição da Instrução Normativa No. 1 do GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA (2008).

A defesa da monografia de pesquisa de Liliana Campos ocorreu no dia 15 de dezembro de 2008, e foi avaliada pela banca composta por Mamede Lima-Marques (orientador), Magda Fernanda Medeiros Fernandes e Jorge Henrique Cabral Fernandes.

[31] Uma teoria do conhecimento é denominada epistemologia. Ver http://en.wikipedia.org/wiki/Epistemology.

A defesa da monografia de Reinaldo Silva Simião ocorreu no dia 23 de junho de 2009, e foi avaliada pela banca composta por Jorge Henrique Cabral Fernandes (orientador), Edgard Costa Oliveira e Jacir Luiz Bordim.

7.1 **UMA PROPOSTA DE CONCEITO PARA "COMUNICAÇÕES" NO TERMO SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES**, por Liliana Suzete Lopes de Queiroz Campos

O trabalho apresenta proposta para conceituar "Comunicações", no termo Segurança da Informação e Comunicações, de modo a justificar sua adoção e aplicabilidade no âmbito da Administração Pública Federal, área de abrangência da atuação do Departamento de Segurança da Informação e Comunicações, do Gabinete de Segurança Institucional da Presidência da República. Também mostra que o verbete "Comunicações" pode ser aplicado e entendido em relação aos indivíduos sob um aspecto pouco explorado nos processos de implementação de Sistemas de Segurança da Informação: a formação de uma Cultura Organizacional de Segurança da Informação, por meio de processos de conscientização com foco nas comunicações. Com essa associação, atribui-se ao tema uma abordagem na qual foco e nível de atenção na pessoa sejam semelhantes aos dispensados à tecnologia, no processo que envolve Segurança da Informação.

Palavras-chave*: Segurança da Informação e Comunicações, Administração Pública Federal, Comunicação Organizacional, Cultura Organizacional.*

7.2 **SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: CONCEITO APLICÁVEL EM ORGANIZAÇÕES GOVERNAMENTAIS**, por Reinaldo Silva Simião

Os órgãos e entidades governamentais são organizações complexas e possuem alcance amplo em suas atividades, lidando com informações importantes, tanto para a prestação de serviço público ao cidadão, como para tomada de decisões estratégicas de Estado. Problemas decorrentes da falta de disponibilidade, integridade, confidencialidade e autenticidade em sistemas de informação levam à necessidade de desenvolver ações de segurança nas organizações governamentais. As ações de segurança baseadas em modelos de segurança da informação, não encontram eco no serviço público como solução eficaz. A eficácia do serviço público exige intensa cooperação entre as organizações para troca de informações. Como será comprovado no trabalho, os modelos atuais de segurança da informação são baseados em ambiente competitivo de mercado, a fim de maximizar o retorno sobre investimentos e as oportunidades de negócio. O status e a abrangência da segurança da informação nos órgãos públicos precisam ser aperfeiçoados, demandando nova abordagem do problema. O trabalho analisa o novo conceito de segurança da informação e comunicações, que passou a ser

utilizado pela Administração Pública Federal brasileira com a edição da Instrução Normativa No. 1 do Gabinete de Segurança Institucional da Presidência da República do Brasil. À luz da análise efetuada, o trabalho demonstra a melhor adequação do novo conceito e destaca as diferenças relativas aos conceitos de segurança da informação pesquisados na literatura.

Palavras-chave*: Segurança, Informação, Comunicações, Inteligência, Confiança, Organizações Governamentais, Disponibilidade, Integridade, Confidencialidade, Autenticidade.*

CAPÍTULO 8

PESSOAS E SEGURANÇA DA INFORMAÇÃO

Uma busca no Google contendo a expressão "pessoas elo mais fraco" retorna mais de 80.000 resultados[32]. São muitas as imagens que fazem alusão às pessoas como sendo o elo mais fraco da cadeia de segurança da informação, embora o mais correto talvez seja dizer que as pessoas são o elo essencial.

Três pesquisas realizadas no CEGSIC 2007-2008 abordaram a relação entre as pessoas e a segurança da informação organizacional. O primeiro dos trabalhos, desenvolvido por Paulo César Cardoso Rocha (ROCHA, 2008b), aborda as razões para o comportamento inapropriado de usuários de TI. O segundo trabalho, desenvolvido por Renato do Carmo das Neves Alves (ALVES, 2009), apresenta um modelo de análise quantitativo para medição do comportamento de segurança, que pode ser aplicável a servidores públicos. O terceiro trabalho, realizado por Roberto Ribeiro Bastos (BASTOS, 2009), realiza uma análise da política de segurança da informação na Marinha e sua relação com o componente humano.

A defesa da monografia de Paulo Rocha ocorreu no dia 15 de dezembro de 2008 e foi avaliada pela banca composta por Priscila America Solis Mendez Barreto (orientadora), Jorge Henrique Cabral Fernandes e Pedro de Azevedo Berger. A defesa da monografia de Renato Alves ocorreu no dia 22 de junho

[32] Tente por exemplo
http://www.google.com/search?q=pessoas+elo+mais+fraco

de 2009, e foi avaliada pela banca composta por Jorge Henrique Cabral Fernandes (orientador), João José Costa Gondim e Magda Fernanda Medeiros Fernandes. A defesa da monografia de Roberto Ribeiro Bastos ocorreu no dia 16 de julho de 2009, e foi avaliada pela banca composta por Jorge Henrique Cabral Fernandes (orientador), João José Costa Gondim e Magda Fernanda Medeiros Fernandes.

8.1 **SEGURANÇA DA INFORMAÇÃO: UMA QUESTÃO NÃO APENAS TECNOLÓGICA**, por Paulo César Cardoso Rocha

O foco do trabalho, ao abordar a área de segurança da informação, é discutir razões para o comportamento inapropriado dos funcionários e apresentar soluções para mitigar as vulnerabilidades organizacionais em razão do comportamento humano. De forma específica, busca-se listar e exemplificar condutas comportamentais que tornam o sistema de segurança vulnerável; abordando a padronização de condutas para mitigar o risco. Desta forma, o trabalho pretende salientar a importância do componente comportamental nos processos de Aprendizagem Organizacional nas instituições públicas, assim como a preponderância da mudança comportamental. Os resultados obtidos sugerem um modelo para a formulação de políticas de segurança da informação baseadas em moldes afeitos ao domínio das ciências sociais e construídas com ênfase na observação dos sistemas de informação e no contexto em que se inserem.

Palavras-chave: *Segurança da Informação; Políticas de Segurança da Informação; Componente Comportamental.*

8.2 **UM MODELO DE ANÁLISE DO COMPORTAMENTO DE SEGURANÇA DE SERVIDORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL BRASILEIRA**, por Renato do Carmo das Neves Alves

O trabalho propõe um modelo de análise do comportamento de segurança dos servidores públicos da Administração Pública Federal, estabelecendo uma relação entre o nível de conhecimento e conscientização dos servidores das organizações públicas, em relação às normas e práticas de segurança da informação no ambiente de trabalho, devendo mensurar o grau de comprometimento de cada servidor para com os ativos da organização e a sua preocupação com a segurança da informação. Pretende-se demonstrar que para o sucesso na implantação de um modelo de análise do comportamento dos servidores públicos, os responsáveis pela organização pública, bem como pela segurança da informação na organização, terão como responsabilidade desenvolver, melhorar e construir mecanismos que

possam reforçar a importância de se ter um programa de conscientização para todos os servidores da organização.

Palavras-chave: *Comportamento de Segurança, Servidores Públicos, Administração Pública Federal, Práticas de Segurança da Informação.*

8.3 **ANÁLISE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA MARINHA QUANTO AOS CONTROLES VOLTADOS PARA O RISCO DO COMPONENTE HUMANO EM AMBIENTES E SISTEMAS CRÍTICOS**, por Roberto Ribeiro Bastos

É inegável o impacto que a presença e a contínua evolução da tecnologia da informação (TI) provoca na vida das sociedades, das organizações e dos indivíduos. Este impacto é observado na absorção da TI nos mais diversos processos dos quais aquelas entidades são partícipes. Esta aderência da TI aos processos traz, além dos benefícios óbvios, uma variedade enorme de potenciais riscos para o desempenho ou a própria existência desses processos e, em consequencia, para as entidades envolvidas. Dessa sinergia identificam-se seus elementos principais: a tecnologia, o processo e o homem, todos orbitando em torno dos principais ativos: informação e conhecimento. Desses três elementos, o agente humano, diferentemente dos outros dois, caracteriza-se pela sua imprevisibilidade, sendo considerado, portanto, o fator intangível na problemática da segurança da informação e comunicações. Na maioria dos incidentes de segurança é observada a importância do componente humano, seja por ação ou omissão, seja por intencionalidade positiva ou negativa. Os programas de sensibilização, conscientização e treinamento são encarados como as medidas iniciais indicadas para se mitigar a participação negativa do homem nos incidentes de segurança. No entanto essas medidas por si só são insuficientes para a previsão, detecção e neutralização de ações propositalmente deletérias contra ambientes computacionais críticos. Este estudo propõe enfatizar a importância da adoção de controles efetivos, balizados pela pertinente análise de risco, destinados a auxiliar na antecipação dos riscos potenciais atinentes à ação humana em ambientes computacionais críticos existentes na Marinha do Brasil, testando a sua conformidade e eficácia com as recomendações observadas pelas normas vigentes.

Palavras-chave: *Comportamento Humano, Controles, Ambientes Críticos, Marinha do Brasil.*

CAPÍTULO 9

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

A experiência de praticantes e pesquisadores de segurança da informação tem demonstrado que o estabelecimento e manutenção de políticas de segurança é uma árdua tarefa (NETTO et al., 2008; TRIBUNAL DE CONTAS DA UNIÃO, 2008; PELTIER, 1998). Hoje já há normas federais que disciplinam o desenvolvimento de políticas de segurança da informação e comunicações em órgãos da APF, como a criada pelo DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR, (2009a), que confere direitos e deveres ao gestor público, no que concerne à proteção dos sistemas e da informação públicos.

Duas pesquisas do CEGSIC 2007-2008 abordaram de forma explícita o desenvolvimento de políticas de segurança da informação e políticas de segurança da informação e comunicações. O trabalho de Danielle Rocha da Costa (COSTA, 2008a) pesquisou os fatores críticos de sucesso que devem ser considerados por gestores durante o estabelecimento de políticas de segurança da informação. O trabalho de Iná Lúcia Cipriano de Oliveira Monteiro (MONTEIRO, 2009) apresenta uma proposta de guia para elaboração de políticas de segurança da informação e comunicações para órgãos da APF.

A defesa da monografia de Danielle Rocha ocorreu no dia 15 de dezembro de 2008, e foi avaliada pela banca composta por Gilberto de Oliveira Netto (orientador), Jorge Henrique Cabral Fernandes e Mamede Lima-Marques. A defesa da monografia de Iná Monteiro ocorreu no dia 25 de junho de 2009, e

foi avaliada pela banca composta por Gilberto de Oliveira Netto (orientador), Magda Fernanda Medeiros Fernandes e Jorge Henrique Cabral Fernandes.

9.1 **FATORES CRÍTICOS DE SUCESSO PARA ELABORAÇÃO DE POLÍTICAS DE SEGURANÇA NA APF**, por Danielle Rocha da Costa

Considerando a importância de uma política de segurança da informação e comunicações como instrumento estratégico para as organizações, o trabalho propõe um modelo de formulação de políticas no âmbito da Administração Pública Federal, baseado na adoção de um conjunto de fatores considerados críticos para o sucesso dessa atividade. Os resultados obtidos originaram um conjunto de Fatores Críticos de Sucesso, os quais foram identificados por uma sequencia de procedimentos que fazem parte de um processo de elaboração de uma política de segurança da informação e comunicações.

Palavras-chave: *Segurança da Informação, Políticas, Fatores Críticos de Sucesso, Administração Pública Federal.*

9.2 **PROPOSTA DE UM GUIA PARA ELABORAÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES EM ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA FEDERAL (APF)**, por Iná Lúcia Cipriano de Oliveira Monteiro

A necessidade de segurança é um fator que vem transcendendo os limites de uma organização, pois pode ser aplicada a pessoas, processos, tecnologia e à própria informação. Apesar de vários trabalhos relacionados ao tema Segurança da Informação, pouco enfoque tem sido dado à definição de um conjunto de diretrizes e procedimentos coerentes, que auxiliem a elaboração de uma Política de Segurança da Informação e Comunicações. Uma Política deve indicar como as coisas devem acontecer em uma organização no que se refere à segurança da informação, ou seja, quais as regras, normas e procedimentos que determinam qual deve ser o comportamento das pessoas que se relacionam com a organização. Visando suprir esta deficiência, o trabalho apresenta uma proposta de um guia para auxiliar na elaboração de Políticas de Segurança da Informação e Comunicações em Organizações da Administração Pública Federal, baseado em uma série de padrões, normas e bibliografias de referência, cuja contribuição é a de um controle essencial em assuntos relacionados com segurança da informação.

Palavras-chave: *Segurança da Informação, Política de Segurança da Informação, Normas e Padrões de Segurança, Guia de Política de Segurança da Informação e Comunicações.*

CAPÍTULO 10

GESTÃO DO RISCO DE SEGURANÇA DA INFORMAÇÃO

A gestão do risco de segurança da informação (ISO/IEC, 2007) é um processo sistemático, adotado na gestão da segurança da informação, que realiza a identificação dos eventos potencialmente negativos para a segurança de uma organização, chamados de riscos de segurança, e em seguida formula um ou mais planos que permitam o tratamento destes riscos de forma custo-efetiva, por meio da adoção de controles e outras ações gerenciais.

Hoje a aplicação da gestão de riscos de segurança da informação na administração pública federal é disciplinada pela Norma Complementar 04 do DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR (2009b).

No CEGSIC 2007-2008 foram desenvolvidas duas monografias que abordam de forma explícita os métodos e processos de gestão do risco de segurança. A monografia de Paulo Hideo Ohtoshi (OHTOSHI, 2008) realiza uma análise comparativa entre várias metodologias de gestão e análise de riscos. A monografia de Pedro Jorge Sucena (SILVA, 2009) apresenta uma proposta de metodologia de alto nível para a análise e avaliação do risco, que possa ser empregada por organizações da APF.

A defesa da monografia de Paulo Ohtoshi ocorreu no dia 10 de dezembro de 2008, e foi avaliada pela banca composta por Edgard Costa Oliveira (orientador), José Carlos Ralha e Jorge Henrique Cabral Fernandes. A monografia de Pedro Sucena foi defendida e aprovada no dia 23 de junho de

2009, perante uma banca composta por Jorge Henrique Cabral Fernandes (orientador), Edgard Costa Oliveira e Jacir Luiz Bordim.

10.1 **ANÁLISE COMPARATIVA DE METODOLOGIAS DE GESTÃO E DE ANÁLISE DE RISCOS SOB A ÓTICA DA NORMA ABNT NBR ISO/IEC 27005**, por Paulo Hideo Ohtoshi

O trabalho de pesquisa visa ao aprimoramento da Gestão de Segurança de Sistemas de Informação e Comunicações da Administração Pública Federal. Reúne os conceitos recentes de gestão de riscos, descreve as principais metodologias e ferramentas de gestão e de análise de riscos existentes no mundo. Apresenta um estudo comparativo entre as principais metodologias e ferramentas e serve como instrumento de avaliação que pode ser utilizado na escolha da metodologia a ser aplicada pelos órgãos Administração Pública Federal. Os resultados do trabalho são um inventário de metodologias e ferramentas e quadros comparativos que destacam algumas qualidades e benefícios que cada uma delas oferece. O estudo dessas normas, metodologias e ferramentas demonstra uma tendência de convergência e de integração entre essas metodologias.

Palavras-chave: *Gestão de Riscos, Normas, Metodologias, Ferramentas, Inventário, Análise Comparativa, Riscos, Ameaças, Vulnerabilidades, Conformidade.*

10.2 **ANÁLISE/AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO PARA A ADMINISTRAÇÃO PÚBLICA FEDERAL: UM ENFOQUE DE ALTO NÍVEL BASEADO NA ABNT NBR ISO/IEC 27005**, por Pedro Jorge Sucena Silva

O trabalho apresenta um modelo preliminar de análise/avaliação de riscos de segurança da informação, capaz de identificar os riscos com alto potencial de impacto em uma organização pública. A análise/avaliação de riscos é uma atividade do processo de gestão de riscos em que são identificados os riscos e seus componentes (ativos, ameaças, vulnerabilidades e consequências). A probabilidade de ocorrência do cenário de risco e suas consequências são avaliadas, resultando em um nível de risco. Esse risco é então avaliado segundo critérios pré-definidos que determinarão a sua importância para a organização. A norma ISO/IEC 27005 recomenda iniciar o processo de gestão de riscos com uma análise/avaliação com um enfoque de alto nível, isto é, uma abordagem mais global que vise os principais riscos que envolvem o negócio. É uma abordagem simplificada que considera os aspectos tecnológicos de forma independente das questões de negócio. A partir dos resultados dessa primeira iteração é possível definir as prioridades, os riscos que precisam ser detalhados em uma segunda iteração e uma

cronologia para a execução de ações. O trabalho propõe um modelo com essas características, tendo como base a Norma ABNT ISO/IEC 27005 e considerando algumas especificidades da Administração Pública Federal.

Palavras-chave: *Segurança da Informação, Gestão de Riscos, Administração Pública.*

CAPÍTULO 11

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A prática da segurança da informação é fortemente associada ao tratamento de incidentes, pois é por meio desse tratamento que os praticantes da segurança oferecem auxílio direto aos usuários de sistemas de informação e plataformas tecnológicas, bem como é por meio da análise das informações coletadas durante o tratamento de incidentes que se pode compreender, de forma mais precisa, as condições da segurança da informação num espaço organizacional ou tecnológico.

Hoje já há pelo menos duas normas federais que disciplinam o tratamento de incidentes de segurança da informação em órgãos da APF: Norma Complementar 05 do DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR (2009c), que orienta a criação de equipes de tratamento de incidentes; e Norma Complementar 08 do DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR (2010b), que define diretrizes para gerenciamento de redes computacionais.

No CEGSIC 2007-2008, a monografia desenvolvida por Roberto Moutella Pimenta (PIMENTA, 2008) foi diretamente relacionada ao tema gestão de

incidentes de segurança. O foco do trabalho foi a modelagem dos processos de tratamento de incidentes do órgão CTIR.Gov[33].

A monografia de Roberto Pimenta foi defendida no dia 10 de dezembro de 2008, perante uma banca composta por Célia Ghedini Ralha (orientadora), João José Costa Gondim e Indiana Belianka Kosloski de Medeiros.

11.1 **PROPOSTA DE MODELO DE MELHORIA DE QUALIDADE BASEADO EM PROCESSOS PARA TRATAMENTO DE INCIDENTES COMPUTACIONAIS NA APF**, por Roberto Moutella Pimenta

A complexidade das infraestruturas de redes computacionais da Administração Pública Federal, como consequência do fenômeno da convergência, gerou a criação de equipes de resposta de incidentes conhecidas genericamente por Computer Security Incident Response Teams (CSIRTs). Na atualidade, percebe-se a necessidade de troca de informações entre estas equipes, com a finalidade de melhor desenvolver o trabalho de segurança das infraestruturas supracitadas. Uma resposta rápida e eficiente a um evento computacional já não é mais suficiente. Há que se impedir incidentes com as experiências já vivenciadas por outras equipes. O foco do trabalho é remeter à troca de informação e compartilhamento do conhecimento entre os colaboradores e o público-alvo (stakeholderes) de um CSIRT. Tendo este foco como meta, o trabalho primeiramente tratou da documentação dos fluxos de trabalho de um CSIRT de coordenação - o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR.Gov), que utiliza como base os modelos adaptados do Computer Emergency Response Team Coordination Center (CERT-CC) e do MANDIA. Com a documentação dos macroprocessos do CTIR Gov tornou-se possível definir um modelo de melhoria de qualidade dos serviços prestados, o qual permitiu um maior fluxo de informação entre os stakeholders.

Palavras-chave: *CTIR.Gov, CSIRT, Modelo de Qualidade, Tratamento de Incidentes, Integração.*

[33] O CTIR.Gov (http://www.ctir.gov.br/) é um centro responsável pela coordenação do tratamento de incidentes computacionais que ocorrem nas redes de computadores dos órgãos da APF.

CAPÍTULO 12

GESTÃO DE CRISES ORGANIZACIONAIS

Segundo Smith e Elliot (2006), crises são fenômenos emergentes e erráticos, que se movimentam dentro do sistema complexo que é uma organização, e que normalmente são disparadas por um incidente ou outro conjunto de circunstâncias de origem interna ou externa à organização. Crises não ocorrem "da noite para o dia". Pelo contrário, expõem uma vulnerabilidade inerente que foi incubada dentro da organização durante um longo período de tempo.

No CEGSIC 2007-2008 duas pesquisas versaram sobre o assunto Gestão de Crises. A monografia de Gerson Charbel Costa (COSTA, 2008c) propôs uma abordagem para a Gestão de Crises no Âmbito da APF, visando a redução de prejuízos ao erário devidos a demandas judiciais decorrentes. A monografia de Gilberto Palmeira (PALMEIRA JÚNIOR, 2008) explorou a aplicabilidade da tipologia de crises de Mitroff (MITROFF; PAUCHANT; SHRIVASTAVA, 2006) para o enquadramento de uma série de fenômenos danosos que ocorreram de forma vinculada a organizações da APF nos últimos anos e que foram enquadrados como sendo crises.

A monografia de Gerson Charbel foi defendida no dia 10 de dezembro de 2008, perante uma banca composta por Tatiana Vieira Malta (orientadora), João José Costa Gondim e Jorge Henrique Cabral Fernandes. A monografia de Gilberto Palmeira foi defendida no dia 15 de dezembro de 2008, perante uma banca composta por Jorge Henrique Cabral Fernandes (orientador), João José Costa Gondim e Magda Fernanda Medeiros Fernandes.

12.1 **GESTÃO DE CRISES NO ÂMBITO DA ADMINISTRAÇÃO PÚBLICA FEDERAL E SUA RELAÇÃO COM A RESPONSABILIDADE CIVIL OBJETIVA EM DEMANDAS JUDICIAIS DECORRENTES**, por Gerson Charbel Costa

As crises, como é sabido de todos, ameaçam as organizações em seus objetivos fundamentais naquilo que se refere ao cumprimento da sua missão estratégica e, em termos de Administração Pública, pode acarretar na reparação dos danos provocados às vítimas, por exemplo, do sistema de controle de tráfego aéreo, de vez que circunscrita à teoria da responsabilidade civil objetiva. A gestão de crises, por conseguinte, objetiva limitar os impactos causados por incidentes, sejam eles previstos ou inesperados, integrando-se a outros processos da organização, dentre eles, os relacionados à segurança da informação, gestão de riscos, gestão de incidentes e continuidade de negócios. O presente estudo tem como foco principal extrair do episódio que culminou no chamado "caos aéreo" lições que visam disseminar a necessidade de implementação de uma política de gestão de crises no âmbito da administração pública federal cujas decisões terão reflexo direto nas demandas judiciais de responsabilidade civil objetivando a reparação de danos, ao mesmo passo em que irá propor um modelo de defesa judicial baseado nas excludentes de responsabilidade a fim de minimizar ou mesmo excluir o dever de reparação.

Palavras-chave: *Crise, Gestão de Crises, Responsabilidade Civil, Administração Pública Federal.*

12.2 **GESTÃO DE CRISES NA ADMINISTRAÇÃO PÚBLICA FEDERAL: UM ESTUDO SOBRE A TIPOLOGIA DE MITROFF**, por Gilberto Dias Palmeira Júnior

O objetivo do trabalho é experimentar o modelo teórico de tipologias de crises proposto por Mitroff, aplicando-o na classificação das crises que afligem ou afligiram a Administração Pública Federal do Brasil. A pesquisa é considerada exploratória, aplicada, qualitativa e documental, com características bibliográficas, por envolver o exame de materiais já publicados que serviram de subsídio para análise e classificação das crises estudadas. O estudo produzido poderá auxiliar no desenvolvimento da área de gestão de crises aplicada na APF, baseado nos estudos de Mitroff em agrupar crises em tipos definidos. Com o "agrupamento" de crises, espera-se, em vez de serem envidados esforços no gerenciamento específico de uma crise, que possam ser desenvolvidos "portfólios" de ações aplicáveis a várias crises do mesmo tipo. Foram selecionados alguns dos fenômenos complexos e danosos mais relevantes relacionados à APF nos últimos dez anos e que podiam ser caracterizados como crises. A todos eles pôde ser aplicado o

modelo de tipologias de Mitroff. Com os resultados, é possível verificar a aderência do modelo proposto por Mitroff às crises estudadas.

Palavras-chave: *Gestão de crise, Tipologias de Crises, Modelo de Mitroff, Administração Pública Federal.*

CAPÍTULO 13

CRIPTOGRAFIA E INFRAESTRUTURA DE CHAVES PÚBLICAS

Os métodos, técnicas, processos, ferramentas e sistemas criptográficos, conceitualmente expostos em livros como Stallings (2008) e Schneier (2001), são frequentemente usados como blocos construtores de soluções mais complexas de segurança computacional, como sítios de comércio eletrônico, que dependem de uma infraestrutura de chaves públicas.

No CEGSIC 2007-2008, duas monografias abordaram questões relativas à proteção ao sigilo da informação quando em trânsito ou durante armazenamento, por meio da criptografia. O trabalho de Jorge Euler Vieira (VIEIRA, 2008) propôs uma Solução de Certificação Digital para o Exército Brasileiro. O trabalho desenvolvido por Edilson Fernandes da Cruz (CRUZ, 2009) apresentou uma revisão histórica do papel da criptografia na proteção das comunicações no Brasil e no mundo.

A monografia de Jorge Euler foi defendida em 15 de dezembro de 2008, perante uma banca composta por José Ricardo Camelo (orientador), Jorge Henrique Cabral Fernandes e João José Costa Gondim. A defesa da monografia de Edilson da Cruz ocorreu no dia 31 de julho de 2009 e foi avaliada pela banca composta por João José Costa Gondim (orientador), Priscila America Solis Mendez Barreto e Jorge Henrique Cabral Fernandes.

13.1 **PROPOSTA DE UMA SOLUÇÃO DE CERTIFICAÇÃO DIGITAL PARA O EXÉRCITO BRASILEIRO**, por Jorge Euler Vieira

O trabalho descreve uma solução de certificação digital que atende aos requisitos de segurança do Exército Brasileiro, mantendo uma compatibilidade com a Infraestrutura de Chaves Públicas Brasileira. Para isso, propõe uma metodologia que busca, por meio de instrumentos de pesquisa junto a usuários do Exército Brasileiro, os requisitos operacionais para uma solução de certificação digital. Estes requisitos foram transformados em requisitos técnicos, que norteiam a descrição da solução proposta.

Palavras-chave: *Certificação Digital, Assinatura Digital, LCR, AR, AC, ICP.*

13.2 **A CRIPTOGRAFIA E SEU PAPEL NA SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES (SIC): RETROSPECTIVA, ATUALIDADE E PERSPECTIVA**, por Edilson Fernandes da Cruz

O trabalho apresenta um estudo sobre a Criptografia e seu papel na Segurança da Informação e das Comunicações (SIC), considerando sua retrospectiva, atualidade e perspectiva. Começa pela definição de criptografia, na tentativa de explicar o que vem a ser essa técnica. A seguir, apresenta breve história da criptografia e discute a sua evolução, desde as mais remotas origens. Também mostra a importância da criptografia para a segurança da informação e das comunicações. Na sequência, analisa os tipos de criptografia em uso nos dias de hoje e examina onde e como estão sendo usados. Finalmente, apresenta a evolução da criptografia no Brasil e, antes de concluir, investiga o que o futuro reserva para a criptografia e que avanços ainda pode incorporar.

Palavras-chave: *Cifra, Código, Criptoanálise, Criptografia, Escrita Secreta, Espionagem, Esteganografia, Segurança da Informação e das Comunicações, Sigilo.*

CAPÍTULO 14

CONTROLE DE ACESSOS LÓGICO

O controle de acessos é a primeira linha defensiva de controles de segurança de um sistema. O controle de acessos envolve a análise, desenho, implementação e manutenção de mecanismos e métodos usados para permitir a gestores de segurança controlar quais objetos podem ser acessados por quais sujeitos. São mecanismos centrais do controle de acessos a identificação, autenticação, autorização, monitoramento, contabilização e auditoria.

Hoje há um norma que disciplina o controle de acesso de segurança da informação em órgãos da administração pública federal, que é a Norma Complementar 07 do DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR (2010a).

No CEGSIC 2007-2008, a monografia de Sergio Roberto Fuchs da Silva (DA SILVA, 2008) abordou o tema controle de acesso em ambiente computacional.

A monografia de Sergio da Silva foi defendida no dia 1 de dezembro de 2008, perante uma banca composta por Jacir Luiz Bordim (orientador), João José Costa Gondim e Jorge Henrique Cabral Fernandes.

14.1 **PROPOSTA DE MODELO DE CONTROLE DE ACESSO LÓGICO POR SERVIDORES PÚBLICOS AOS RECURSOS COMPUTACIONAIS DA ADMINISTRAÇÃO PÚBLICA**, por Sergio Roberto Fuchs da Silva

A Administração Pública, braço operacional do Estado, por intermédio de seus servidores e funcionários, desempenha suas atividades precípuas em benefício do cidadão brasileiro, utilizando sistemas de informação e recursos computacionais como forma de aperfeiçoar e alcançar de maneira mais competente seus objetivos. Nesses sistemas estão contidos dados e informações, em sua maioria, sigilosas, cabendo ao Estado, inclusive no cumprimento de determinações legais, o dever de zelar pela sua guarda e proteção. Esse zelo deve abranger todo o ciclo de vida da informação, desde sua coleta até sua destruição, passando pela disponibilização de acesso para sua utilização, em especial, por parte de seus servidores, que devem fazê-lo no estrito cumprimento de suas funções. Como parte integrante desse arcabouço de proteção, historicamente, tem sido utilizado mecanismo de controle de acesso a esses sistemas com base em senhas, o que tem se mostrado, principalmente nos tempos atuais, uma forma de controle ultrapassada e ineficiente, possibilitando acesso por pessoas não autorizadas com objetivos no mais das vezes inescrupulosos, trazendo prejuízos tanto para o Estado quanto para o cidadão. A Administração Pública deve avançar cada vez mais não apenas técnica e culturalmente, com o objetivo de alcançar melhor e mais eficazmente os objetivos finais a que se propõe, mas também nas formas acessórias de bem servir ao cidadão, zelando criteriosamente pelas suas informações sob sua guarda, bem assim primar pelo cumprimento dos requisitos legais de proteção à informação a qual está submetida. Visando atender a essa necessidade de aprimoramento do controle de acesso pelos servidores públicos aos recursos computacionais da Administração Pública, esta pesquisa descreve uma proposta de controle de acesso utilizando certificado digital armazenado em cartão inteligente, cujo acionamento se efetiva com a utilização de senha.

Palavras-chave: *Acesso, Criptografia, Certificado, Digital, Biometria, Senha.*

CAPÍTULO 15

SEGURANÇA EM TELECOMUNICAÇÕES E REDES DE COMPUTADORES

O intenso aumento da conectividade entre sistemas computacionais por meio das redes de computadores e sistemas de telecomunicações ofereceu, simultaneamente, uma grande oportunidade e várias ameaças para a segurança computacional e para a segurança da informação e segurança das comunicações.

No CEGSIC 2007-2008, foram desenvolvidas três monografias que abordam temas relacionados à segurança de redes de computadores e sistemas de telecomunicações. A monografia de Everardo de Lucena Tavares (TAVARES, 2008) foi desenvolvida sob um tema que combina Comunicações Operacionais Multimídia e Comunicações Móveis em rede mesh 802.11s. A monografia de Marcos Ambrogi Leite (LEITE, 2008) abordou práticas nos serviços de telefonia da Administração Pública Federal. A monografia de Lindeberg Pessoa Leite (LEITE, 2009) abordou a implantação do IPv6 no Brasil.

A monografia de Everardo Tavares foi defendida no dia 1 de dezembro de 2008, perante uma banca composta por Jacir Luiz Bordim (orientador), João José Costa Gondim e Jorge Henrique Cabral Fernandes. A monografia de Marcos Ambrogi Leite foi defendida no dia 1 de dezembro de 2008, perante uma banca composta por Jacir Luiz Bordim (orientador), João José Costa

Gondim e Jorge Henrique Cabral Fernandes. A monografia de Lindeberg Leite foi defendida no dia 20 de julho de 2009, perante uma banca composta por João José Costa Gondim (orientador), Jorge Henrique Cabral Fernandes e Priscila Solis Barreto.

15.1 **SISTEMA DE COMUNICAÇÕES OPERACIONAIS MULTIMÍDIA, COMUNICAÇÕES MÓVEIS (REDE MESH) 802.11S**, por Everardo de Lucena Tavares

Este trabalho descreve as tecnologias empregadas na implantação de uma infraestrutura de rede sem fio WLAN (Wireless Local Area Network) - WMAN (Wireless Metropolitan Area Network), no Haiti, em um Teatro de Operações de Combate, utilizando o Padrão 802.11s (Mesh). Uma WLAN-WMAN é uma rede sem fio, implementada como extensão ou alternativa para redes convencionais. Além de redes locais, esta tecnologia pode ser utilizada para redes de acesso à Internet, que nestes casos são denominadas redes WiFi (Wireless Fidelity) / WiMAX (Worldwide Interoperability for Microwave Access). Estas redes utilizam sinais de RF ou infravermelho para a transmissão de dados, minimizando a necessidade de cabos de conexão dos usuários à rede. Desta forma, uma WLAN-WMAN combina comunicação de dados com mobilidade dos usuários dentro da área de cobertura da rede. As tecnologias de redes sem fio mais conhecidas atualmente são as IEEE 802.11b/g/s, as quais foram propostas como elementos agregados, para comporem o sistema do trabalho em análise. O padrão 802.11 utiliza frequências das bandas ISM (Instrumentation, Scientific & Medical), as quais compreendem três segmentos do espectro (902 a 928 MHz, 2.400 a 2.483,5 MHz e 5.725 a 5.850 MHz) reservados para uso, sem a necessidade de licença, sendo, portanto, de uso livre. Qualquer pessoa pode utilizar esta fatia de frequência, como um provedor para um grande bairro, por exemplo. As WLAN-WMAN adotam uma técnica chamada OFDM (Orthogonal Frequency-Division Multiplexing).

Palavras-chave: *Redes sem Fio, Wi-Fi, WiMAX, Mesh.*

15.2 **BOAS PRÁTICAS E SUA APLICAÇÃO NOS SERVIÇOS DE TELEFONIA DA ADMINISTRAÇÃO PÚBLICA FEDERAL**, por Marcos Ambrogi Leite

A pesquisa foi desenvolvida com foco nas atuais práticas na gestão de Serviços de Telefonia Fixa Comutada (STFC) prestados ao Ministério da Saúde, com o intuito de propor melhorias que possam ser implementadas, de imediato, em conformidade com a Norma Brasileira ABNT NBR ISO/IEC 27002:2006 - Código de Prática para a Gestão da Segurança da Informação.

Palavras-chave: *Gestão, Segurança, Informação, Comunicações, Telefonia.*

15.3 **UM ESTUDO DE IMPLANTAÇÃO DE IPV6 NA ADMINISTRAÇÃO PÚBLICA FEDERAL**, por Lindeberg Pessoa Leite

Este trabalho tem o objetivo de subsidiar os gestores da Administração Pública Federal (APF) na elaboração de um plano de implantação de IPv6. Os assuntos pertinentes foram levantados por meio de uma pesquisa explanatória constituída por uma análise bibliográfica e documental. A análise bibliográfica está baseada em livros sobre o assunto, bem como artigos e documentos publicados na internet. Na análise documental, foi analisada a experiência do POP-RS na implantação de IPv6, uma vez que o mesmo guarda características com os órgãos da APF. Essa pesquisa se inicia com informações técnicas sobre o assunto, para fundamentar o desenvolvimento e conclusão do trabalho. No desenvolvimento, são analisados os impactos organizacionais com relação aos equipamentos, custos, pessoal e serviços. Por fim, com a análise documental conclui-se qual a melhor estratégia de implantação de IPv6 na APF e quais medidas emergenciais devem ser praticadas.

Palavras-chave: *IPV6, Implantação, Estratégias, Medidas Emergenciais, Administração Pública Federal.*

CAPÍTULO 16

GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Uma organização não detém nem jamais deterá controle pleno sobre os eventos do seu ambiente, sejam o interno ou o externo. Portanto, sujeita-se aos riscos. Decorre da exposição ao risco a necessidade de ações que consistem em:

- observar os eventos passados e as condições da situação presente;
- estimar as chances de eventos potenciais no futuro (riscos) que influenciem a organização de forma negativa (riscos de segurança) ou positiva; e
- adotar decisões e controles para neutralizar os riscos negativos, garantindo o alcance de condições desejáveis no futuro.

Dá-se o nome de gestão da segurança a este conjunto de ações, quando realizadas de forma intencional, planejada, organizada, monitorada e controlada.

No CEGSIC 2007-2008, foram desenvolvidas 4 monografias que adotaram a perspectiva de gestão para a melhoria da segurança. A monografia de Silvana Crispim Loureiro (LOUREIRO, 2008) apresenta uma revisão bibliográfica dos conceitos relacionados ao estabelecimento de um SGSI, tomando por base a situação da Advocacia Geral da União. A monografia de Antônio Carlos Pereira de Britto (BRITTO, 2008) relatou o uso de uma metodologia de implementação de SGSI baseada no modelo PMBOK, desenvolvida pelo autor no ano de 2006. A monografia de Juscelino Kilian

(KILIAN, 2009) propôs um modelo para avaliação da maturidade dos processos de Gestão da Segurança da Informação e Comunicações para órgãos da APF, visando a concessão de prêmios aos melhores gestores e praticantes da segurança. A monografia de Mônica Costa Tkaczyk Martins (MARTINS, 2009) descreveu os passos iniciais para estabelecimento de um SGSI na Advocacia-Geral da União, por meio de uma declaração preliminar de escopo de um SGSI.

A monografia de Silvana Crispim Loureiro foi defendida no dia 1 de dezembro de 2008, perante uma banca composta por Jacir Luiz Bordim (orientador), João José Costa Gondim e Jorge Henrique Cabral Fernandes. A monografia de Antonio Britto foi defendida no dia 15 de dezembro de 2008, perante uma banca composta por composta por Jorge Henrique Cabral Fernandes (orientador), João José Costa Gondim e Gilberto de Oliveira Netto. A monografia de Mônica Costa Tkaczyk Martins foi defendida no dia 23 de junho de 2009, perante uma banca composta por Jorge Henrique Cabral Fernandes (orientador), Edgard Costa Oliveira e Jacir Luiz Bordim. A monografia de Juscelino Kilian (KILIAN, 2009) foi defendida no dia 25 de junho de 2009, perante uma banca composta por Magda Fernanda Medeiros Fernandes (orientadora), Jorge Henrique Cabral Fernandes e Gilberto de Oliveira Netto.

16.1 **SEGURANÇA DA INFORMAÇÃO: PRESERVAÇÃO DAS INFORMAÇÕES ESTRATÉGICAS COM FOCO EM SUA SEGURANÇA**, por Silvana Crispim Loureiro

O estudo tem como objetivo realizar uma revisão bibliográfica acerca da Segurança da Informação, especialmente tratando da preservação das informações estratégicas e contribuir para ressaltar sua importância para a Advocacia-Geral da União (AGU). Na primeira parte do trabalho é apresentada uma pesquisa bibliográfica para nivelamento dos conceitos relacionados à informação, normas e melhores práticas existentes e aspectos legais, ressaltando o valor da informação como recurso estratégico para organização. O foco do estudo será a Advocacia-Geral da União, que, como outras organizações da Administração Pública Federal (APF), necessita de informações seguras e confiáveis para tomada de decisão. Novos modelos para tratar de segurança têm sido propostos, mas são sempre voltados para parte tecnológica, esquecendo que a mudança de cultura, programas de conscientização e o apoio da alta direção são fatores primordiais para alcançar o sucesso. Na conclusão, apresenta sugestões de medidas a serem tomadas para aprimorar a Segurança da Informação na Advocacia-Geral da União, podendo até servir para utilização em outras organizações que ainda não iniciaram estudos para atender o Decreto N. 3.595, que institui a Política de Segurança nos órgão e entidades APF.

Palavras-chave: *ABNT NBR ISO/IEC 27002, ABNT NBR ISO/IEC 27001, Segurança da Informação, Ativos, Classificação da Informação.*

16.2 **PMBOK E GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO**, por Antônio Carlos Pereira de Britto

A Gestão da Segurança da Informação e Comunicação (GSIC) é hoje um dos pilares do Modelo de Governança de Tecnologia da Informação (TI), e responsável por assegurar a disponibilidade, integridade, autenticidade e confidencialidade das informações da Sociedade e do Estado. Um Modelo de Gestão de Segurança da Informação e Comunicação (MGSIC) deve ser utilizado na Administração Pública Federal (APF) para satisfazer os critérios técnicos de segurança da informação e as obrigações legais, e principalmente como forma de atender aos requisitos para a preservação do valor intrínseco da informação em uso na APF. Esta monografia propõe a abordagem do Gerenciamento de Projetos baseada nas orientações do Guia Project Management Body of Knowledge (PMBOK), criado pelo Project Management Institute (PMI), como forma de viabilizar a implementação do MGSIC na APF. O modelo considerado para a implementação foi o proposto pelo Grupo de Trabalho Metodologia 2005 (GT-2005), instituído pelo DSIC/GSI, do qual o autor participou quando da coordenação dos trabalhos do GT pelo CEPESC nos anos de 2005 e 2006. O modelo do GT-2005 é aderente ao conjunto de Normas 27000, sendo que o GT-2005 usou uma abordagem holística e sistêmica que leva a visão da Governança de TI para a fundamentação do MGSIC. Esta monografia relaciona dois modelos: o PMBOK para o Gerenciamento de Projetos e o Modelo de Gestão da Segurança da Informação e Comunicação do GT-2005, propondo uma abordagem orientada ao projeto na implantação do MGSIC na APF.

Palavras-chave: *Gestão da Segurança da Informação e Comunicação, Governança de TI, Modelo de Referência, Modelo de Gestão, APF, DSIC/GSI, Grupo de Trabalho Metodologia 2005, Gerenciamento de Projetos, Ciclo PDCA, PMBOK, ISO/IEC 27001.*

16.3 **ANÁLISE E SOLUÇÃO PRELIMINAR PARA PROBLEMAS DE SEGURANÇA DA INFORMAÇÃO NA ADVOCACIA-GERAL DA UNIÃO**, por Mônica Costa Tkaczyk Martins

A produção e manutenção das notas técnicas, pareceres e demais trabalhos jurídicos produzidos pelos profissionais da área jurídica são informações imprescindíveis para a AGU e tornaram-se tão essenciais que qualquer problema que afete a segurança destas informações causa inúmeros transtornos e atrasos nos serviços prestados pela AGU. Tendo em vista este cenário, torna-se fundamental tomar as providências necessárias para evitar

problemas e/ou minimizar os efeitos de possíveis falhas de segurança nos ambientes tecnológicos e físicos da AGU. Como proposta para minimizar e solucionar estes problemas, a implantação de um Sistema de Gestão de Segurança da Informação, oriundo de modelos de qualidade como as normas da família NBR ISO/IEC 27000, apresenta grande chance de ser adotada e melhorar a situação de segurança da AGU, no trato de suas informações e comunicações. Esta monografia descreve os resultados de um estudo preliminar para implantação de um sistema de gestão de segurança da informação na AGU, onde se faz uma breve análise da organização e as restrições que afetam a implantação deste SGSI, propondo ao final o escopo onde deverá ser implantado o SGSI.

Palavras-chave: *Sistema de Gestão de Segurança da Informação, ISO 27001, ISO 27005, Administração Pública Federal, Advocacia-Geral da União.*

16.4 **PRÊMIO DE QUALIDADE EM GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NA ADMINISTRAÇÃO PÚBLICA FEDERAL**, por Juscelino Kilian

A sociedade da informação trouxe mudanças nas organizações em relação ao uso das informações, as quais têm sido reconhecidas como um ativo de importância crescente. As informações estão cada vez mais disponíveis a todos os segmentos de atividades de governo, com um papel importante no suporte à tomada de decisões em níveis operacionais e estratégicos. O trabalho tem por objetivo propor o Prêmio de Qualidade em Gestão da Segurança da Informação e Comunicações na Administração Pública Federal, que será um instrumento valioso de avaliação da maturidade dos processos de Gestão da Segurança da Informação e Comunicações para órgãos da Administração Pública Federal (APF). Para tanto foi realizada uma revisão de literatura procurando relacionar assuntos relativos à Segurança da Informação, incluídos modelos existentes e formas de avaliação de processos contexto de órgãos públicos, visando identificar a aderência em relação à Instrução Normativa No. 1 do Gabinete de Segurança Institucional da Presidência da República (IN GSIPR Nr 1).

Palavras-chave: *Níveis de Maturidade de Processo, Gestão de Segurança da Informação, Administração Pública Federal.*

CAPÍTULO 17

SEGURANÇA EM COMPRAS E CONTRATOS DE TI

As compras e contratos do governo brasileiro são regidas pela Lei 8.666, de 21 de junho de 1993. A aquisição e implementação de sistemas de tecnologia da informação encontram-se em fase de regulação na esfera Federal, especialmente pela Instrução Normativa 04 da SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO DO MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO (2008), a qual "dispõe sobre o processo de contratação de serviços de Tecnologia da Informação pela Administração Pública Federal direta, autárquica e fundacional." Em adição à realidade complexa envolvida no processo das compras públicas em TI, destaca-se o desafio do domínio gerencial e tecnológico sobre os serviços e produtos que implementam controles de segurança da informação, qualquer que seja a natureza dos mesmos. Os controles de segurança apresentam complexas formas de funcionamento, e o grau de domínio necessário sobre esses, por parte das organizações pública contratantes e adquirentes, demanda um processo bastante elaborado, onde surge necessidade de tratar, ainda durante a aquisição, aspectos como monitoramento, aprimoramento e continuidade do serviço ou produto. A especificação, contratação, aquisição, implementação, operação, monitoramento e aprimoramento de controles de segurança constituem-se um dos grandes desafios à gestão da segurança da informação e comunicações.

Se ainda acrescenta-se a este cenário as possíveis demandas atuais e futuras pela criação de uma indústria de produtos e serviços de segurança

computacional e da informação, que permita o necessário grau de autonomia à segurança da nação, cria-se um cenário promissor para estudos sobre Segurança em Compras e Contratos.

Uma pesquisa do CEGSIC 2007-2008 abordou o tema compras públicas relacionadas a segurança, e foi desenvolvido por Gerson Ben-Hur Mayer (MAYER, 2008), descrevendo Procedimentos de Segurança da Informação e Comunicações em Contratos de Tecnologia da Informação no Exército Brasileiro.

A monografia de Gerson Ben-Hur Mayer foi defendida no dia 17 de dezembro de 2008, perante uma banca composta por José Ricardo Camelo (orientador), Jorge Henrique Cabral Fernandes e João José Costa Gondim.

17.1 **PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES EM CONTRATOS DE TECNOLOGIA DA INFORMAÇÃO NO EXÉRCITO BRASILEIRO**, por Gerson Ben-Hur Mayer

Este trabalho pretende apresentar uma proposta de procedimentos a serem observados em segurança da informação e comunicações por ocasião da formulação de contratos de Tecnologia da Informação (TI). Genericamente, tais procedimentos já vêm sendo adotados nas Organizações Públicas e Privadas, sendo, no entanto, em muitas delas, um processo feito quase instintivamente ou baseado na experiência pessoal dos envolvidos na formulação do contrato. Para este trabalho, o universo considerado foi o Centro de Desenvolvimento de Sistemas (CDS) do Exército Brasileiro, instituição voltada para a formulação e acompanhamento técnico de Contratos de Tecnologia da Informação.

Palavras-chave: *Contratos, Tecnologia da Informação, Procedimentos, Exército Brasileiro.*

CAPÍTULO 18

GOVERNANÇA, CONTROLE, AUDITORIA, CONFORMIDADE E CERTIFICAÇÃO

Os temas Governança, Controle, Auditoria, Conformidade e Certificação são interrelacionados. É por meio da conformidade aos controles, atestada especialmente através de relatos de auditoria, que a alta administração pode reduzir a incerteza sobre o alinhamento de interesses entre as áreas de gestão e de operação. De outra forma, é por meio da conformidade aos controles, atestada através de um certificado de conformidade, que o cliente de uma organização pode reduzir a incerteza acerca dos procedimentos e processos realizados por um fornecedor atual ou potencial.

No CEGSIC 2007-2008, foram desenvolvidas 8 monografias relacionadas aos temas Governança, Controle, Auditoria, Conformidade e (ou) Certificação. Kleber Ferreira Rangel (RANGEL, 2008) realizou um levantamento de requisitos e controles de segurança para o Portal de Inteligência Operacional do Estado Maior de Defesa. Henrique Aparecido da Rocha (ROCHA, 2008a) propôs um cenário para aplicação da norma NBR ISO/IEC 27002:2005 em auditorias governamentais do sistema de controle interno implementado pela CGU. Newton Daltro Santos (SANTOS, 2008) discorreu sobre o paradigma da auditoria baseada em cenários de risco. Rogério Xavier Rocha (ROCHA, 2008c) elaborou uma proposta de procedimento simplificado de auditoria de gestão em segurança da informação em órgãos do Poder Executivo Federal. Rubem Ribeiro Veloso (VELOSO, 2008) fez uma avaliação de conformidade na Marinha do Brasil

(MB) a modelos de gestão da segurança da informação. A monografia de Alessandro Sá Barbosa (BARBOSA, 2009) realizou uma Avaliação Preliminar de Controles de Segurança usados em algumas organizações militares do Exército Brasileiro. A monografia de Idilson Alexandre Palhares Cassilhas (CASSILHAS, 2008) está relatada no Capítulo 19. A monografia de Roberto Ribeiro Bastos (BASTOS, 2009) está relatada no Capítulo 8.

A monografia de Kleber Ferreira Rangel foi defendida no dia 10 de dezembro de 2008, perante banca composta por Jorge Henrique Cabral Fernandes (orientador), Tatiana Vieira Malta e João José Costa Gondim. A monografia de Henrique da Rocha foi defendida no dia 10 de dezembro de 2008, perante banca composta por Edgard Costa Oliveira (orientador), José Carlos Ralha e Jorge Henrique Cabral Fernandes. A monografia de Newton Daltro foi defendida no dia 10 de dezembro de 2008, perante banca composta por Edgard Costa Oliveira (orientador), José Carlos Ralha e Jorge Henrique Cabral Fernandes. A monografia de Rubem Ribeiro Veloso foi defendida no dia 15 de dezembro de 2008, perante banca composta por José Ricardo Camelo (orientador), Jorge Henrique Cabral Fernandes e João José Costa Gondim. A monografia de Rogério Rocha foi defendida no dia 17 de dezembro de 2008, perante banca composta por Jorge Henrique Cabral Fernandes (orientador), João José Costa Gondim e José Ricardo Camelo. A monografia de Alessandro Sá Barbosa foi defendida no dia 27 de julho de 2009, perante banca composta por José Ricardo Camelo (orientador), Jorge Henrique Cabral Fernandes e Jacir Luiz Bordim.

18.1 **LEVANTAMENTO DE REQUISITOS E CONTROLES DE SEGURANÇA PARA O PORTAL DE INTELIGÊNCIA OPERACIONAL DO ESTADO MAIOR DE DEFESA**, por Kleber Ferreira Rangel

O trabalho descreve um conjunto de requisitos e controles de segurança que foram levantados para o Portal de Inteligência Operacional do Estado-Maior de Defesa do Ministério da Defesa. O enfoque é desenvolvido sob o ponto de vista dos diversos conceitos, métodos e técnicas usualmente abordados na área de gestão da segurança da informação e comunicações. O resultado apresenta-se útil no complemento a uma visão de segurança, com base nos princípios de Contra-Inteligência, normalmente utilizada por esse Estado-Maior de Defesa com o propósito de aumentar a segurança de seus sistemas.

Palavras-chave: *Requisitos, Controles de Segurança, Segurança da Informação, Inteligência Operacional.*

18.2 **PROPOSTA DE CENÁRIO PARA APLICAÇÃO DA NORMA NBR ISO/IEC 27002 EM AUDITORIAS GOVERNAMENTAIS DO SISTEMA DE CONTROLE INTERNO**, por Henrique Aparecido da Rocha

As iniciativas em segurança da informação têm se destacado nos últimos anos em virtude de fatores que incluem o poder conquistado pela informação nos processos de negócio atuais, a grande exposição dessas informações propiciada pelo desenvolvimento tecnológico e o consequente aumento dos registros de incidentes de segurança. Entretanto, a Administração Pública Federal (APF) ainda não absorveu totalmente essa cultura de segurança e não protege adequadamente as suas informações de valor. De outro lado, o sistema de controle interno tem a incumbência de assessorar os gestores públicos na implementação dos controles internos responsáveis por garantir que sejam alcançados os objetivos das instituições. Nesse contexto, a segurança da informação pode ajudar. O foco desta monografia é especificar meios de disseminar a cultura de segurança da informação entre os órgãos da APF e apoiá-los a implementar os controles adequados para esse fim. A solução proposta consiste na incorporação de procedimentos de verificação, baseados em normas de segurança da informação amplamente utilizadas, no processo de auditoria do sistema de controle interno. A ideia é utilizar a estrutura já existente de auditorias periódicas como suporte também para conscientizar e orientar os órgãos da importância da segurança da informação para suas missões. As principais contribuições desta monografia são: (1) descrever o processo de auditoria empregado pelo sistema de controle interno do governo federal; (2) descrever a norma NBR ISO/IEC 270002 que apresenta código de prática para a gestão da segurança da informação; e (3) propor cenário de aplicação da norma NBR ISO/IEC 270002 no processo de auditoria do Sistema de Controle Interno do Governo Federal.

Palavras-chave: *Controle Interno, Cultura de Segurança, Procedimentos de Auditoria.*

18.3 **AUDITORIA BASEADA EM CENÁRIOS DE RISCO: UM PARADIGMA MODERNO INTEGRADO À GESTÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NO ÂMBITO DA ADMINISTRAÇÃO PÚBLICA FEDERAL**, por Newton Daltro Santos

Os recursos organizacionais definidos como pessoa, informação, sistema, equipamento, serviço e reputação representam hoje os principais ativos tangíveis e intangíveis de qualquer corporação, pública ou privada, sendo de importância estratégica a administração sólida e eficaz dos riscos associados a esses ativos corporativos, como requisito indispensável ao sucesso no gerenciamento da segurança da informação aplicado ao negócio

organizacional e, consequentemente, na adequada governança corporativa. Nesse contexto, o comprometimento da equipe de auditores internos da organização com tal desafio, mediante uma mudança de enfoque em relação à auditoria tradicional centrada em controles, agregaria maior valor à sistemática gerencial adotada pela corporação para lidar com os riscos que ameaçam os ativos que sustentam os negócios. Este trabalho acadêmico visou dissertar a respeito de um novo paradigma no campo da auditoria, conhecido como risk-based auditing, no intento de investigar se essa moderna abordagem contribuiria no aperfeiçoamento de processos voltados ao gerenciamento de riscos e, por conseguinte, na melhoria contínua de sistemas de gestão especializados na segurança de sistemas de informação e comunicações no âmbito da administração pública federal. Para tanto, o trabalho de pesquisa evidencia com clareza as diferenciações mais evidentes entre o paradigma tradicional e o enfoque moderno da auditoria, descreve alguns benefícios e desafios que caracterizam a utilização de uma sistemática de auditoria baseada em riscos, com foco no gerenciamento seguro de ativos organizacionais, além de propor algumas competências necessárias aos gestores públicos que atuam ou venham a atuar na auditoria interna, quando da utilização desse novo paradigma no âmbito governamental.

Palavras-chave: *Auditoria, Auditoria Baseada em Risco.*

18.4 **AVALIAÇÃO DE CONFORMIDADE A MODELOS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO NA MARINHA DO BRASIL (MB)**, por Rubem Ribeiro Veloso

A pesquisa visa a atender à necessidade de aprimoramento da Gestão da Segurança da Informação na Marinha do Brasil e também verificar se os instrumentos normativos internos sobre Segurança da Informação estão em conformidade com a norma ABNT NBR ISO/IEC 17999 (Tecnologia da Informação - Técnicas de Segurança - Código de Prática para a Gestão da Segurança da Informação). O levantamento dos assuntos relevantes foi realizado por meio de uma pesquisa exploratória constituída por uma análise bibliográfica e a análise documental. A análise documental está baseada nos documentos formalmente publicados no âmbito da Marinha do Brasil. Os dados obtidos na pesquisa documental são tratados de forma qualitativa. São abordados temas da gestão da segurança da informação e apresenta-se como a Marinha do Brasil trata a Gestão da Segurança da Informação, sua infraestrutura de intranet e internet. É feita uma avaliação de conformidade dos controles: "Política de Segurança da Informação", "Organizando a Segurança da Informação" e "Gestão de Riscos". Ao final, conclui-se que a Marinha do Brasil possui documentação formalmente instituída e estruturada de forma a se adequar e manter atualizada frente às constantes inovações de

TI e preparada para se contrapor às possíveis ameaças no campo da segurança da Informação.

Palavras-chave: *Conformidade, Segurança da Informação, Marinha do Brasil.*

18.5 **PROPOSTA DE PROCEDIMENTO SIMPLIFICADO DE AUDITORIA DE GESTÃO EM SEGURANÇA DA INFORMAÇÃO EM ÓRGÃOS DO PODER EXECUTIVO FEDERAL**, por Rogério Xavier Rocha

A pesquisa tem por objetivo principal propor um procedimento de auditoria de gestão de segurança da informação em órgãos da Administração Pública Federal, baseado em controles de normas consagradas em segurança da informação, tais como a NBR ISO/IEC 17799:2005. A partir de levantamentos sobre os principais riscos e vulnerabilidades encontradas que impactam uma gestão efetiva da segurança da informação em órgãos da administração pública federal, buscar-se-á, por meio do procedimento proposto, incentivar uma implementação gradativa e sedimentada de diversos controles por meio das ações de controle do sistema de controle interno do poder executivo federal, que por força constitucional, tem por missão auxiliar a gestão pública na consecução de seus objetivos.

Palavras-chave: *Auditoria, Segurança da Informação. Procedimentos de Auditoria.*

18.6 **AVALIAÇÃO PRELIMINAR DOS CONTROLES DE SEGURANÇA USADOS NO EXÉRCITO BRASILEIRO**, por Alessandro Sá Barbosa

A informação, cada vez mais, tem sido considerada um importante ativo para muitas empresas e organizações da iniciativa privada e, também, da administração pública em todos os níveis. Portanto, protegê-la de acessos não autorizados, que ocasionem alteração em quaisquer de suas características básicas, tem se tornado um constante desafio para gestores e profissionais que atuam na área da Tecnologia da Informação e, mais especificamente, da Segurança da Informação e das Comunicações. A adoção da Norma ABNT NBR ISO/IEC 27002:2005 e a implementação dos controles de segurança sugeridos no documento mencionado têm se constituído em importantes aliados na luta contra o aumento da ocorrência de incidentes de segurança. Após realização de uma criteriosa análise de riscos, que permite dimensionar adequadamente o tipo de controle de segurança a ser adquirido pelas instituições, a adoção de tais dispositivos de segurança é aprovada com a finalidade de mitigar as vulnerabilidades encontradas. Com vistas a obter novos controles de segurança e a aprimorar o nível de maturidade dos controles adotados em algumas Organizações

Militares do Exército Brasileiro, a pesquisa verificou em que níveis de maturidade estão os controles de segurança atualmente adotados e se os mesmos estão em conformidade com os sugeridos pela Norma de Segurança. Para tanto, a pesquisa utilizou um instrumento que permitiu coletar os dados necessários, junto aos responsáveis pela Segurança da Informação de cada Organização Militar selecionada, que possibilitou, após a análise, verificar os níveis de maturidade e, posteriormente, a proposição de ações que visem a melhoria desses níveis de maturidade e, quando necessária, a adoção de novos controles de segurança, mais adequados e condizentes com a realidade de cada Organização. O trabalho teve, também, o intuito de nortear as ações do Órgão de Direção Setorial, responsável, atualmente, por prescrever as diretrizes de segurança da informação para a Força Terrestre.

Palavras-chave: *Informação, Controles de Segurança, Segurança da Informação, Exército Brasileiro, Maturidade.*

CAPÍTULO 19

GESTÃO DA CONTINUIDADE

Segundo a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2008), continuidade de negócios é uma capacidade estratégica e tática de uma organização de se planejar e responder a incidentes de grandes proporções, desastres ou interrupções de negócios significativas, para conseguir continuar suas operações em um nível aceitável previamente definido.

Na Administração Pública Federal já dispomos de uma norma que regula a gestão da continuidade no serviço público, que é a NC 06 do DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR (2009d), de 11 de novembro de 2009.

No CEGSIC 2007-2008, foram desenvolvidas 3 monografias relacionadas ao temas da gestão da continuidade. A monografia de Idilson Alexandre Palhares Cassilhas (CASSILHAS, 2008) realizou uma Análise da Atividade de Testes do Plano da Continuidade de Negócio em um setor da Marinha do Brasil, avaliando sua Conformidade com a Norma ABNT NBR ISO/IEC 17799:2005. A monografia de Antônio Magno Figueiredo de Oliveira (OLIVEIRA, 2008) envolveu pesquisa qualitativa e quantitativa acerca do Nível de Compreensão da Gestão da Continuidade dos Negócios junto a gestores de segurança de organizações públicas. Vitor Friedenhain (FRIEDENHAIN, 2008) fez um levantamento de Métodos e Processos para a Implantação da Gestão da Continuidade de Negócios que poderiam ser aplicáveis a órgãos da Administração Pública Federal.

A defesa da monografia de Idilson Alexandre Palhares Cassilhas ocorreu no dia 01 de dezembro de 2008, e foi avaliada pela banca composta por Jacir

Luiz Bordim (orientador), João José Costa Gondim e Jorge Henrique Cabral Fernandes. A monografia de Vitor Friedenhain foi defendida no dia 10 de dezembro de 2008, perante banca composta por Jorge Henrique Cabral Fernandes (orientador), Tatiana Vieira Malta e João Roberto V. Guimarães. A monografia de Antônio de Oliveira foi defendida no dia 15 de dezembro de 2008, perante banca composta por Jorge Henrique Cabral Fernandes (orientador), João José Costa Gondim e Magda Fernanda Medeiros Fernandes.

19.1 **UMA ANÁLISE DA ATIVIDADE DE TESTES DO PLANO DE CONTINUIDADE DE NEGÓCIO E SUA CONFORMIDADE COM A NORMA ABNT NBR ISO/IEC 17799:2005**, por Idilson Alexandre Palhares Cassilhas

Um Plano de Continuidade de Negócio (PCN) é uma descrição detalhada das ações que devem ser tomadas em resposta a uma interrupção súbita e inesperada de um dado serviço, permitindo que a organização continue trabalhando mesmo com uma redução aceitável do desempenho de seus processos. A rede integrada de comunicações de uma instituição como a Marinha do Brasil, que possui diversas organizações militares interligadas e espalhadas por todo o território nacional, para ser considerada um sistema bem sucedido e que mantém a continuidade de seus negócios durante uma falha ou qualquer acontecimento brusco e imprevisto, deve possuir capacidade de oferecer os serviços essenciais requeridos por seus usuários, preservando as suas principais conexões e componentes durante o tempo que for necessário para o reestabelecimento da situação normal de operação. Tal capacidade é conseguida através de preparação, planejamento, investimento e, principalmente, por meio da implementação de um Plano de Continuidade de Negócio (PCN), precedido de uma análise detalhada sobre cada um dos ativos que fazem parte dessa grande infraestrutura e dos seus respectivos riscos. Esta pesquisa visa averiguar se a atividade de testes de continuidade de negócio aplicada ao serviço fixo de comunicações da Marinha do Brasil é eficaz e se está em conformidade com as melhores técnicas e práticas para a Gestão da Segurança da Informação e Comunicações, previstas na Norma ABNT NBR ISO/IEC 17799:2005.

Palavras-chave: *Marinha do Brasil, Continuidade, PCN, Conformidade, Comunicaçoes.*

19.2 **UM ESTUDO SOBRE MÉTODOS E PROCESSOS PARA A IMPLANTAÇÃO DA GESTÃO DE CONTINUIDADE DE NEGÓCIOS APLICÁVEIS A ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA FEDERAL BRASILEIRA**, por Vitor Friedenhain

O trabalho apresenta um estudo sobre métodos e processos para a implantação da Gestão de Continuidade de Negócios (GCN) aplicáveis a

órgãos da Administração Pública Federal (APF). A implantação da GCN é importante dada a essencialidade dos serviços prestados por essas instituições, os quais estão sujeitos a uma ampla gama de riscos que podem levar à sua interrupção. Inicialmente, destaca-se que os gestores da APF devem ser convencidos da importância da GCN, para que estes dêem respaldo ao seu desenvolvimento, alocando recursos para o programa. Mostra-se, também, que é necessário um diagnóstico da situação atual de maturidade em GCN das organizações. A partir do diagnóstico, é possível traçar um objetivo que as instituições pretendam atingir, e verificar quais variáveis devem ser desenvolvidas para que o mesmo seja alcançado. Com base no diagnóstico, destaca-se que deve ser desenvolvida a política de GCN com variáveis como o conceito de GCN, escopo do programa, normas e regulamentos que a influenciaram, entre outros. Tendo sido estabelecida a infraestrutura para a implantação do programa de GCN, mostra-se a necessidade de uma análise de impacto nos negócios e avaliação de riscos para determinar quais são relevantes para as atividades consideradas críticas. Estas definições servem de embasamento para a definição de estratégias preventivas de tratamento dos riscos e estabelecimento de parâmetros (meta de tempo de recuperação e nível mínimo de serviços, por exemplo) que são base para a formulação dos planos de continuidade de negócios. Finalizando, após a formulação dos planos, estes devem ser divulgados através de programas de conscientização e treinamento, assim como testados e atualizados, completando o ciclo de etapas de implantação da GCN na APF.

Palavras-chave: *Gestão de Continuidade de Negócios, GCN, Administração Pública Federal.*

19.3 **NÍVEL DE COMPREENSÃO DA GESTÃO DE CONTINUIDADE DOS NEGÓCIOS**, por Antônio Magno Figueiredo de Oliveira

O trabalho busca identificar a compreensão dos conceitos de Gestão de Continuidade de Negócios pelos Gestores Públicos no âmbito da Administração Pública Federal (APF). Para isso propõe modelo de instrumento a fim de realizar pesquisa qualitativa para coleta de dados com gestores que atuem na APF. O pesquisador propõe análise subjetiva, diretamente relacionada com a avaliação da correlação que o entrevistado demonstra fazer, a partir do conteúdo de sua resposta, com: o tema da pergunta; os conceitos de GCN aos quais ele se reporta para embasar a sua

resposta; e o entendimento sobre a organização e as suas especificidades e o quanto os procedimentos adotados pela organização estão em conformidade com conceitos de GCN. Propõe uma análise dos dados para classificar o nível de compreensão dos conceitos, usando como referência de avaliação a Taxonomia de Bloom, dividindo o nível de compreensão em três categorias: baixo, médio e alto. Apresenta uma revisão de literatura abordando os principais conceitos relacionados à Gestão de Continuidade de Negócios. Como resultado apresenta a consolidação dos dados levantados na pesquisa a fim de subsidiar a realização de futuros trabalhos acerca do tema na APF.

Palavras-chave: *Gestão de Continuidade de Negócios (GCN), Internalização, Gestão de Risco, Análise de Impacto de Negócios, GCN, Aprovação, Implantação, Teste e Manutenção do Plano, Incidentes, Desastres, Riscos, Ameaças, Vulnerabilidades, Mitigar.*

CAPÍTULO 20

SEGURANÇA E DEFESA CIBERNÉTICAS

Pesquisa do CENTRO DE ESTUDOS SOBRE AS TECNOLOGIAS DA INFORMAÇÃO E DA COMUNICAÇÃO - CETIC.br (2008) sobre uso das TICs no Brasil, realizada no ano de 2008, revela que:

- Cerca de 1/4 da população brasileira estava usando a Internet;
- a quase totalidade das organizações privadas e públicas faz acesso à Internet;
- cerca de 1/5 das organizações brasileiras ofertam serviços (na Internet) através de Extranet.

De uma forma ou de outra, organizações do país conectam seus sistemas de informação e comunicação à Internet, a fim de permitir o compartilhamento e o acesso a informações e serviços providos pela Internet. Há nítida percepção, não só aqui no Brasil mas especialmente nos EUA, que é cada vez maior a diferença entre o aumento da exposição dos SICs públicos às redes mundiais e o tempo de resposta da administração pública no sentido de preservar a segurança destes SICs. Apresenta-se desta forma, com extrema relevância, as pesquisas sobre a segurança nas redes abertas, associadas ao conceito de Segurança Cibernética.

No CEGSIC 2007-2008, foram desenvolvidas 2 monografias relacionadas aos temas Defesa e Segurança Cibernéticas na Administração Pública Federal. A monografia de Marcelo Paiva Fontenele (FONTENELE, 2008) contém análises e propostas para articulação de organizações do Estado Brasileiro no Contexto da Defesa Cibernética. A monografia de Raphael Mandarino Junior (MANDARINO JÚNIOR, 2009) realiza um amplo estudo e proposta de classificação para alvos e atores do crime cibernético, propõe um modelo de atuação em segurança e defesa cibernética no Brasil baseado na construção de comunidades de prática e formula uma definição para Infraestrutura Crítica de Informação.

A monografia de Marcelo Fontenele foi defendida no dia 15 de dezembro de 2008, perante banca composta por João José Costa Gondim (orientador), Macarino Bento Garcia de Freitas e Jorge Henrique Cabral Fernandes. A monografia de Raphael Mandarino Junior foi defendida no dia 24 de junho de 2009, perante banca composta por Jorge Henrique Cabral Fernandes (orientador), João José Costa Gondim e Claúdia Lyrio Canongia.

20.1 **ANÁLISE E PROPOSTA DE ARTICULAÇÃO DE ESFORÇOS NO CONTEXTO DA DEFESA CIBERNÉTICA DA ADMINISTRAÇÃO PÚBLICA FEDERAL**, por Marcelo Paiva Fontenele

Visando atender à necessidade de desenvolver a Defesa Cibernética no âmbito da Administração Pública Federal, este trabalho analisa e propõe uma articulação de esforços para sua implementação por meio da definição do escopo dos órgãos envolvidos e de requisitos para suas ligações e comunicações.

Palavras-chave*: Segurança da Informação e Comunicações, Guerra da Informação, Guerra Cibernética, Defesa Cibernética, Crime Digital, Administração Pública Federal, Criptografia, Infraestrutura Crítica, Inteligência, Segurança e Defesa Cibernética.*

20.2 **UM ESTUDO SOBRE A SEGURANÇA E A DEFESA DO ESPAÇO CIBERNÉTICO BRASILEIRO**, por Raphael Mandarino Junior

Com o advento da Internet, parte da humanidade se viu inserida, quase que sem perceber, na chamada Sociedade da Informação. As modificações

introduzidas nos valores sociais, profissionais, políticos ou econômicos até então presentes foram absorvidas sem maiores questionamentos. Várias informações geradas e armazenadas em diferentes lugares do planeta passaram a trafegar livremente, ultrapassando fronteiras e continentes fazendo com que o acesso a elas e aos conhecimentos ocorresse de forma inimaginável até pouco tempo. Por um certo período acreditou-se, romanticamente, que a Internet permitiria o romper de barreiras econômicas, culturais e até quem sabe religiosas entre os povos, constituindo-se no ideal filosófico de democracia da antiga Grécia. Mas a realidade acabou por demonstrar que esses tempos românticos eram uma utopia. A nova fronteira constituída, o Espaço Cibernético, à semelhança de qualquer novo espaço ainda não perfeitamente demarcado, como o antigo "velho oeste", atraiu também pessoas mal intencionadas, que buscam vantagens e ganhos ilícitos, explorando a falta de regras e sendo acobertadas pela distância e pelo aparente anonimato. Assim, a questão da proteção das informações ganhou destaque. Como a informação é um bem incorpóreo, intangível, os seus ativos, os meios de armazenagem, de transmissão, de processamento, os sistemas, interconexões e as pessoas que os usam; passaram a ser o foco da atenção da Segurança Informação. A um subconjunto desses ativos de informação, aqueles que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade, denominamos Infraestrutura Crítica de Informação, crítica para a existência do Espaço Cibernético. Apesar da impossibilidade de definição clara dos limites das suas fronteiras, o Espaço Cibernético se constitui em verdadeiro Estado-Nação, que, embora virtual, se confunde com Estado Real, pois reúne as três características de formação de um Estado: o povo - caracterizado pela Sociedade da Informação que o habita; o território - que é o próprio espaço cibernético; e a soberania - a capacidade de controlar e de ter poder sobre este espaço. Como cabe ao Estado o monopólio do uso legítimo da força e da produção legislativa, cabe-lhe também a proteção desse Estado-Nação virtual, e de suas Infraestruturas Críticas. Propomos nesta monografia, ações que em seu conjunto se constituem em uma Estratégia de Segurança Cibernética, entendida como a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas.

Palavras-chave: *Segurança Cibernética, DSIC/GSIPR, Sociedade da Informação.*

CAPÍTULO 21

EPÍLOGO

Decorridos praticamente um ano desde a formatura da primeira turma de especialistas do CEGSIC, CEGSIC 2007-2008, cujos resumos de trabalhos foram aqui apresentados, se pode dizer com certa confiança que o CEGSIC 20072008 apresentou valiosas contribuições diretas e indiretas para a formulação de uma Metodologia Brasileira de Gestão da Segurança da Informação e Comunicações. Áreas temáticas foram mapeadas, relações de troca de informação entre servidores públicos da esfera federal foram fortalecidas, estudos organizacionais foram realizados, revelando fragilidades que passaram a ser melhor compreendidas e sanadas.

Do ponto de vista da instituição universitária brasileira, se apresentam grandes oportunidades de contribuição para o fortalecimento do Estado brasileiro.

Falando em nome de todos os que contribuíram para a produção do conhecimento aqui apenas parcialmente registrado, esperamos que este livro possa lançar sementes de reflexão, discussão, investigação, proposta e implementação de soluções para a melhoria da gestão pública sobre o ponto de vista da segurança.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBERTS, C.; DOROFEE, A. Managing Information Security Risks: The OCTAVE Approach. [S.l.]: Addison Wesley, 2002. 512 p.

ALVES, R. do Carmo das N. Um Modelo de Análise do Comportamento de Segurança de Servidores da Administração Pública Federal Brasileira. [S.l.], 6 2009. Monografia de Conclusão de Curso (Especialização) – Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

ANDERSON, R. security Engineering: a guide to building dependable distributed systems. USA: John Wiley and Sons, 2001. 612 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação: ABNT NBR ISO/IEC 27002:2005. 2a. ed. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos: ABNT NBR ISO/IEC 27001:2006. 1a. ed. Rio de Janeiro, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Gestão de continuidade de negócios: Parte 1 - Código de Prática: ABNT NBR 15999-1:2007. Errata 1, de 01.02.2008. Rio de Janeiro, 2008.

BARBOSA, A. de S. Avaliação Preliminar dos Tipos de Controles de Segurança da Informação e Comunicação usados nas Organizações Militares do Exército Brasileiro. [S.l.], 7 2009. 72 p. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

BARRETO, P. A. S. M. Controles de Acesso Lógico. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Fevereiro 2008. 24 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

BASTOS, R. R. Análise da Política de Segurança da Informação da Marinha quanto aos Controles Voltados para o Risco do Componente Humano em Ambientes e Sistemas Críticos. [S.l.], 7 2009. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

BERGER, P. de A. Segurança Física de Tecnologia da Informação - Parte 1. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Fevereiro 2008. 31 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

BORDIM, J. L. Controles de Segurança da Informação. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Fevereiro 2008. 19 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

BORDIM, J. L. Redes de Computadores. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Abril 2008. 17 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

BORDIM, J. L. Gestão de Riscos de Segurança da Informação Parte II: Notas de Aula. Brasília, Abril 2009. 31 p.

BRASIL. Decreto No. 3.505, de 13 de junho de 2000 : Institui a política de segurança da informação nos órgãos e entidades da administração pública federal. Brasília, 2000. Disponível em: <http:www:planalto:gov:br/ccivil 03/decreto/D3505:htm>. Acesso em: Agosto de 2009.

BRAZ, F. A. Segurança de Aplicações. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Maio 2008. 32 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

BRITTO, A. C. P. de. Estudo do Gerenciamento de Projeto Baseado no PMBOK para a Implantação da Gestão da Segurança da Informação e Comunicação na Administração Pública Federal. [S.l.], 12 2008. 125 p. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

CAMPOS, L. S. L. de Q. Uma Proposta de Conceito para "Comunicações" no Termo Segurança da Informação e Comunicações. [S.l.], 12 2008. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

CANONGIA, C. Inteligência Competitiva: Informação Estratégica e Decisão. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Janeiro 2008. 25 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a

Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

CARNIELLI, W. A. Pensamento Crítico. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Março 2008. 10 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA. Diretrizes de Segurança Parte III: Política de segurança da ICP - Brasil. 2001. 26 p. Disponível em: <http:www:planalto:gov:BR/ccivil 03/consultapublica/PDF/PoliticadeSeguranca:pdf>. Acesso em: Jul 2009.

CASSILHAS, I. A. P. Uma Análise da Atividade de Testes do Plano de Continuidade de Negócio e sua Conformidade com a Norma ISO 17799:2005. [S.l.], 12 2008. 84 p. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

CENTRO DE ESTUDOS SOBRE AS TECNOLOGIAS DA INFORMAÇÃO E DA COMUNICAÇÃO - CETIC.br. Pesquisa sobre o uso das Tecnologias da Informação e da Comunicação no Brasil 2008:: TIC Domicílios e TIC Empresas 2008. Brasil, 2008. Disponível em: <http://www.cetic.br/tic/2008/index.htm>. Acesso em: Outubro de 2010.

CENTRO DE ESTUDOS SOBRE AS TECNOLOGIAS DA INFORMAÇÃO E DA COMUNICAÇÃO - CETIC.br. PESQUISA SOBRE USO DAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO NO BRASIL 2009. Brasil, 2009. Disponível em: <http://www.cetic.br/tic/2009/index.htm>. Acesso em: Outubro de 2010.

COMITTEE ON NATIONAL SECURITY SYSTEMS. National Information Assurance (IA) Glossary: CNSS Instruction No. 4009. 2010. Disponível em: <http://www.cnss.gov>. Acesso em: Novembro de 2010.

CONVERY, S. Network Security Architectures. USA: Cisco, 2004. 794 p. COSTA, D. R. da. Fatores Críticos de Sucesso para Elaboração de Políticas de Segurança da Informação e Comunicações no Âmbito da Administração

Pública Federal. [S.l.], 12 2008. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

COSTA, E. O. Gestão de Riscos. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Janeiro 2008. 15 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

COSTA, G. C. Gestão de Crises no Âmbito da Administração Pública Federal e sua Relação com a Responsabilidade Civil Objetiva em Demandas Judiciais Decorrentes. [S.l.], 12 2008. 108 p. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

CRUZ, E. F. da. A Criptografia e seu Papel na Segurança da Informação e das Comunicações (SIC): Retrospectiva, Atualidade e Perspectiva. [S.l.], 7 2009. Monografia de Conclusão de Curso (Especialização) – Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

DA SILVA, S. R. F. Proposta de Modelo de Controle de Acesso Lógico por Servidores Públicos aos Recursos Computacionais da Administração Pública. [S.l.], 12 2008. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR. Norma Complementar 02/IN01/DSIC/GSIPR, de 13 de outubro de 2009 : Metodologia de gestão de segurança da informação e comunicações. Brasília,

outubro 2008. Disponível em: <http://dsic.planalto.gov.br>. Acesso em: Outubro de 2010.

DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR. Norma Complementar 03/IN01/DSIC/GSIPR, de 30 de junho de 2009 : Diretrizes para elaboração de política de segurança da informação e comunicações nos Órgãos e entidades da administração pública federal. Brasília, junho 2009. Publicada no DOU No. 115, de 18 Jun 2008 - Seção 1. Disponível em: <http://dsic.planalto.gov.br>. Acesso em: Novembro de 2010.

DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR. Norma Complementar 04/IN01/DSIC/GSIPR, de 14 de agosto de 2009 : Gestão de riscos de segurança da informação e comunicações - grsic. Brasília, agosto 2009. Disponível em: <http://dsic.planalto.gov.br>. Acesso em: Novembro de 2010.

DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR. Norma Complementar 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009 : Criação de equipes de tratamento e resposta a incidentes em redes computacionais - etir. Brasília, agosto 2009. Disponível em: <http://dsic.planalto.gov.br>. Acesso em: Novembro de 2010.

DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR. Norma Complementar 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009 : Gestão de continuidade de negócios em segurança da informação e comunicações. Brasília, novembro 2009. Disponível em: <http://dsic.planalto.gov.br>. Acesso em: Novembro de 2010.

DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR. Norma Complementar 07/IN01/DSIC/GSIPR, de 06 de maio de 2010 : Diretrizes para implementação de controles de acesso relativos á segurança da informação e comunicações. Brasília, maio 2010. Disponível em: <http://dsic.planalto.gov.br>. Acesso em: Novembro de 2010.

DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR. Norma Complementar 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010 : Gestão de etir: Diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da administração pública federal. Brasília, agosto 2010. Disponível em: <http://dsic.planalto.gov.br>. Acesso em: Novembro de 2010.

DESCARTES, R. DISCURSO DO MÉTODO: para bem conduzir a própria razão e procurar a verdade nas ciências. São Paulo: Difel Difusão Européia do Livro, 1962. Disponível em: <http://www.consciencia.org/o-discurso-do-metodo-rene-descartes>. Acesso em: Novembro de 2010.

DOCKHORN, G. O. V. Quando a Ordem é Segurança e o Progresso Desenvolvimento: O Estado Civil Militar Brasileiro 1964-1974. Dissertação (Mestrado) | História, 1999. Disponível em: <http://books.google.com.br/books?id=iPS1kOtBLesC>. Acesso em: Maio de 2009.

FERNANDES, J. H. C. Auditoria e Certiçação de Segurança da Informação. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Março 2008. 26 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

FERNANDES, J. H. C. Estratégias e doutrinas para a Gestão da Segurança da Informação e Comunicações. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Julho 2008. 32 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

FERNANDES, J. H. C. Gestão de Crise. [S.l.], Junho 2008. 22 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

FERNANDES, J. H. C. Sistemas Complexos. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Janeiro 2008. 65 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

FERNANDES, J. H. C. CEGSIC 2007-2008 - Relatório I - O Estado da Arte das Metodologias, Doutrinas e Estratégias em Gestão da Segurança de Informação e Comunicações. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Maio 2009. 38 p.

FERNANDES, M. F. M. Sociedade da Informação: breve introdução sociológica. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Dezembro 2007. 28 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

FONTENELE, M. P. Análise e Proposta de Articulação de Esforços no Contexto da Defesa Cibernética da Administração Pública Federal. [S.l.], 12 2008. 66 p. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

FRIEDENHAIN, V. Um estudo sobre métodos e processos para a implantação da gestão de continuidade de negócios aplicáveis a órgãos da administração pública federal brasileira. [S.l.], 12 2008. 56 p. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA. Instrução Normativa GSI 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. Brasília, junho 2008. Publicada no DOU No. 115, de 18 Jun 2008 – Seção 1. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic>. Acesso em: Agosto de 2009.

GONDIM, J. J. C. Ataques, Intrusões e Investigação Forense em Sistemas de Computação: Parte 1 - Vulnerabilidades e Ataques. [S.l.], Maio 2008. 38 p.

GONDIM, J. J. C. Ataques, Intrusões e Investigação Forense em Sistemas de Computação: Parte 2 - Introdução á Auditoria de Sistemas. [S.l.], Maio 2008. 36 p.

HANSMAN, S.; HUNT, R. A taxonomy of network and computer attacks. Computers & Security, v. 24, n. 1, p. 31{43, February 2005. Disponível em: <http://linkinghub.elsevier.com/retrieve/pii/S0167404804001804>. Acesso em: agosto de 2008.

HARGER, V. P. Segurança Física de Tecnologia da Informação – Parte 2: Interpretação do Capítulo 9 da Norma NBR ISO/IEC 17799. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Fevereiro 2008. 19 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

HARRIS, S. CISSP Exam guide. 3. ed. USA: Osborne McGraw Hill, 2005. 1001 p.

HOGLUND, G.; MCGRAW, G. Exploiting Software: How to Break Code. [S.l.]: Addison-Wesley, 2004.

HOLBROOK, M. B. Adventures in complexity: An essay on dynamic open complex adaptive systems, buttery eécts, self-organizing order, coevolution, the ecological perspective, fitness landscapes, market spaces, emergent beauty at the edge of chaos, and all that jazz. Academy of Marketing Science Review (online), v. 6, 2006. Disponível em: <http://www.amsreview.org/articles/holbrook06-2003.pdf>. Acesso em: 15/09/2008.

HOWARD, M.; LIPNER, S. The Security Development Lifecycle: SDL: a process for developing demonstrably more secure software. USA: Microsoft, 2006.

ISO/IEC. ISO/IEC FDIS 27005 - Information technology – Security Techniques - Information security risk management. [S.l.], 2007.

IT GOVERNANCE INSTITUTE. COBIT 4.1. 4.1. ed. USA, 2007. Disponível em: <http://www.itgi.org>. Acesso em: Janeiro de 2009.

KILIAN, J. Prêmio de Qualidade em Gestão da Segurança da Informação e Comunicações na Administração Pública Federal. [S.l.], 6 2009. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

LEACH, J. Improving user security behaviour. Computers & Security, Elsevier Ltd, v. 22, n. 8, 2003.

LEITE, L. P. Um Estudo de Implantação de IPv6 na Administração Pública Federal. [S.l.], 7 2009. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

LEITE, M. A. Boas Práticas e sua Aplicação nos Serviços de Telefonia da Administração Pública Federal. [S.l.], 12 2008. 127 p. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

LITCHFIELD, D. et al. The Database Hacker's Handbook: Defending Database Servers. USA: Wiley, 2005. 500 p.

LOUREIRO, S. C. Segurança da Informação: Preservação das Informações Estratégicas com Foco em sua Segurança. [S.l.], 12 2008. 66 p. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

MALTA, T. V. Direito na Sociedade da Informação. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Dezembro 2007. 50 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da

Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

MANDARINO JÚNIOR, R. Um Estudo sobre a Segurança e a Defesa do Espaço Cibernético Brasileiro. [S.l.], 6 2009. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

MARTINS, M. C. T. Análise e Solução Preliminar para Problemas de Segurança da Informação na Advocacia-Geral da União. [S.l.], 6 2009. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

MAYER, G. B.-H. Procedimentos de Segurança da Informação e Comunicações em Contratos de Tecnologia da Informação no Exército Brasileiro. [S.l.], 12 2008. 61 p. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

MINISTÉRIO DO PLANEJAMENTO, ORçAMENTO E GESTÂO. Construindo uma agenda de gestão pública. 2009. Disponível em: <http://www.gespublica.gov.br/>. Acesso em: Setembro de 2009.

MITROFF, I.; PAUCHANT, T.; SHRIVASTAVA, P. The structure of man-made organizational crises: Conceptual and empirical issues in the development of a general theory of crisis management. In: SMITH, D.; ELLIOT, D. (Ed.). Key Readings in Crisis Management. USA: Routeledge, 2006. cap. 4.

MONTEIRO, I. L. C. de O. Proposta de um Guia para Elaboração de Políticas de Segurança da Informação e Comunicações em _ Órgãos da Administração Pública Federal (APF). [S.l.], 6 2009. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

NASCIMENTO, A. C. do. Criptograá e infra-estrutura de chaves públicas. Campus Universitário Darcy Ribeiro. Instituto Central de

Ciências, Abril 2008. 65 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR - NIC.br. Dimensões e Características da Web Brasileira: um estudo do gov.br. Brasil, 2010. Disponível em: <http://www.cgi.br/publicacoes/pesquisas/govbr/>. Acesso em: Outubro de 2010.

NETTO, G. O.; ALLEMAND, M.; FREIRE, P. F. Notas de Aula sobre Gestão Operacional da Segurança da Informação. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Novembro 2007. 47 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

NETTO, G. O. et al. Notas de Aula sobre Políticas, Procedimentos e Normas da Segurança da Informação. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Maio 2008. 30 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

OHTOSHI, P. H. Análise Comparativa de Metodologias de Gestão e de Análise de Riscos sob a _ Otica da Norma NBR-ISO/IEC 27005. [S.l.], 12 2008. Monografia de Conclusão de Curso (Especialização) – Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

OLIVEIRA, A. M. F. de. Nível De Compreensão Dos Gestores Da Administração Pública Federal Acerca De Conceitos De Gestão De Continuidade Dos Negócios. [S.l.], 12 2008. 109 p. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

PALMEIRA JÚNIOR, G. D. Gestão de Crises na Administração Pública Federal: Um Estudo sobre a Tipologia de Mitroff. [S.l.], 12 2008. 75 p. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

PELTIER, T. R. Information security policies and procedures: a practitionert's reference. Boca Raton: Auerbach Publications, 1998.

PELTIER, T. R. Information security risk analysis. Boca Raton: Auerbach Publications, 2001.

PIMENTA, R. M. Proposta de modelo de melhoria de qualidade baseado em processos para tratamento de incidentes computacionais na administração pública federal. [S.l.], 12 2008. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

RALHA, C. G. Gestão por Processos e Projetos. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Abril 2008. 15 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

RANGEL, K. F. Levantamento de Requisitos e Controles de Segurança para o Portal de Inteligência Operacional do Estado Maior de Defesa. [S.l.], 12 2008. 67 p. Monografia de Conclusão de Curso (Especialização) – Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

REZENDE, P. A. D. de. Modelos de Conánça para Segurança em Informática. Campus Universitário Darcy Ribeiro. Instituto Central de Ciências, Maio 2009. 47 p. Notas de Aula desenvolvidas no âmbito do Programa de Pesquisas e Formação de Especialistas para a Elaboração da Doutrina Nacional de Gestão da Segurança da Informação e Comunicações.

ROCHA, H. A. da. Proposta de Cenário para Aplicação da Norma NBR ISO/IEC 27002 em Auditorias Governamentais do Sistema de Controle Interno. [S.l.], 12 2008. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

ROCHA, P. C. C. Segurança da Informação - Uma Questão Não Apenas Tecnológica. [S.l.], 12 2008. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

ROCHA, R. X. Proposta de procedimento simplificado de auditoria de gestão em segurança da informação em órgãos do Poder Executivo Federal. [S.l.], 12 2008. Monografia de Conclusão de Curso (Especialização) – Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

SANTOS, N. D. Auditoria Baseada Em Cenários De Risco: Um Paradigma Moderno Integrado á Gestão de Segurança da Informação e Comunicações no Âmbito da Administração Pública Federal. [S.l.], 12 2008. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

SCHNEIER, B. Applied Cryptography: protocols, algorithms, and source code in C. 2nd. ed. USA: John Wiley and Sons, 1996.

SCHNEIER, B. Segurança.com: segredos e mentiras sobre a proteção na vida digital. Rio de Janeiro - RJ: Campus, 2001.

SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO DO MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO. INSTRUÇÃO NORMATIVA No. 4, DE 19 DE MAIO DE 2008 : Dispõe sobre o processo de contratação de serviços de tecnologia da informação pela administração pública federal direta, autárquica e fundacional. Brasília, maio 2008. Disponível em: <http://www.servidor.gov.br/noticias/noticias08/arqdown/080519 IN 4.pdf>. Acesso em: Agosto de 2009.

SILVA, P. J. S. Análise/Avaliação de Riscos de Segurança da Informação para a Administração Pública Federal: um enfoque de alto nível baseado na ISO/IEC 27005. [S.l.], 6 2009. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

SIMIÃO, R. S. Segurança da Informação e Comunicações: conceito aplicável em organizações governamentais. [S.l.], 6 2009. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

SMITH, D.; ELLIOT, D. (Ed.). Key Readings in Crisis Management. USA: Routeledge, 2006. 430 p.

STALLINGS, W. Criptograá e Segurança em Redes: Princípios e práticas. São Paulo: Pearson Education Brasil, 2008.

STONEBURNER, G.; GOGUEN, A.; FERINGA, A. NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems. [S.l.], July 2002. 55 p. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>. Acesso em: julho de 2009.

SYSTEMS AND NETWORK ATTACK CENTER - SNAC. The 60 Minute Network Security Guide: First steps towards a secure network environment. USA, 2006. 48 p. Disponível em: <http://www.nsa.gov/ia/ _les/support/I33011R-2006.pdf>. Acesso em: março de 2009.

TAKAHASHI (Org.), T. Livro Verde da Sociedade da Informação no Brasil. Brasília - DF: Ministério de Ciência e Tecnologia, 2000. 195 p. ISBN 85-88063-01-8. Disponível em: <http://www.mct.gov.br/index.php/content/view/18878.html>. Acesso em: Outubro de 2010.

TAVARES, E. de L. Sistema de Comunicações Operacionais Multimídia, Comunicações Móveis (REDE MESH 802.11s). [S.l.], 12 2008. 126 p. Monografia de Conclusão de Curso (Especialização) - Departamento de

Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

THE INTERNATIONAL BANK FOR RECONSTRUCTION AND DEVELOPMENT and THE WORLD BANK. A Decade of Measuring the Quality of Governance. Washington - DC - USA, 2006. Disponível em: <http://go.worldbank.org/KUDGZ5E6P0>.

TRIBUNAL DE CONTAS DA UNIÃO. Acórdão 1.603/2008-TCU-Plenário: Levantamento acerca da Governança de Tecnologia da Informação na Administração Pública Federal: Sumários Executivos. Brasília, 2008. 48 p. Disponível em: <www.tcu.gov.br/_scalizacaoti>. Acesso em: agosto de 2009.

VELOSO, R. R. Avaliação de Conformidade a Modelos de Gestão de Segurança da Informação na Marinha do Brasil (MB). [S.l.], 12 2008. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

VIEIRA, J. E. Proposta de uma Solução de Certiçação Digital para o Exército Brasileiro. [S.l.], 12 2008. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

WENGER, E.; MCDERMOTT, R.; SNYDER, W. M. Cultivating Communities of Practice: A guide to managing knowledge. USA: Harward Business School Press, 2002.

NOTAS SOBRE ESTA EDIÇÃO

Visite http://cegsic.unb.br para atualizações, errata e outras informações.

Este livro foi impresso na Gráfica da Agência Brasileira de Inteligência, e produzido para atendimento à Portaria 17/2007, do Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil.