PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações

ATUAÇÃO E ADEQUAÇÕES PARA PROFISSIONAIS DA ÁREA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NOS ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA LEGAL E NORMATIVA

Decreto nº 3.505, de 13 de junho de 2000.
Instrução Normativa GSI Nº 01 de 13 de junho de 2008 e suas respectivas Normas Complementares publicadas no DOU pelo DSIC/GSIPR.

CAMPO DE APLICAÇÃO

Esta Norma Complementar se aplica no âmbito da Administração Pública Federal, direta e indireta.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

RAPHAEL MANDARINO JUNIOR
Diretor do Departamento de Segurança da Informação e Comunicações

1 OBJETIVO

Estabelecer diretrizes nos contextos de atuação e adequações para profissionais da área de Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF).

2 CONSIDERAÇÕES INICIAIS

As diretrizes nos contextos de atuação e adequações para profissionais da área de SIC na APF declaram o comprometimento da alta direção organizacional com vistas a prover diretrizes estratégicas, responsabilidades, competências e o apoio para implementar a Gestão de SIC nos órgãos, bem como a ampliação do conhecimento de seus profissionais, a troca de experiências, a capacitação e consequente evolução da SIC nos órgãos e entidades da APF.
Os anexos desta norma devem ser tomados como recomendações para seu conteúdo, eles não são limitadores para os temas.

3 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Conforme disposto no inciso II do art. 3º da Instrução Normativa nº 01, de 13 de Junho de 2008, do Gabinete de Segurança Institucional, compete ao Departamento de Segurança da Informação e Comunicações - DSIC, estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de SIC pelos órgãos e entidades da APF.

4 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

Certificações profissionais: processo negociado pelas representações dos setores sociais, pelo qual se identifica, avalia e valida formalmente os conhecimentos, saberes, competências, habilidades e aptidões profissionais desenvolvidos em programas educacionais ou na experiência de trabalho, com o objetivo de promover o acesso, permanência e progressão no mundo do trabalho e o prosseguimento ou conclusão de estudos.

Ativos de informação: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

5 ATUAÇÃO DOS PROFISSIONAIS DA ÁREA DE SIC

Aos profissionais das áreas de SIC recomenda-se:

5.1 Engajar-se na busca pelo conhecimento e promover ações no sentido de consolidar a cultura de SIC.

5.2 Contribuir de forma ativa e constante no processo de melhoria da SIC nos órgãos e entidades da APF em que atuam.

5.3 Buscar o melhor aproveitamento dos recursos e serviços disponíveis.

5.4 Dedicar-se nos processos de formação em nível de capacitação, educação e conscientização, buscando atuar como disseminador das melhores práticas em SIC.

5.5 Buscar a segurança dos ativos de informação.

5.6 Participar e contribuir na busca e compartilhamento do conhecimento, bem como na troca de experiências com outras entidades do governo, participando de grupos de trabalho, listas de discussões e eventos que tratem o tema SIC.

5.7 Buscar o conhecimento multidisciplinar, entendendo que a SIC abrange os contextos estratégico, tático e operacional dos órgãos e entidades da APF em que atuam.

5.8 Agir em conformidade com a legislação vigente, as normas internas e melhores práticas em SIC.

5.9 Empenhar-se para obter certificações profissionais, seguindo preferencialmente as recomendações propostas no ANEXO A.

6 ADEQUAÇÕES PARA A ATUAÇÃO DOS PROFISSIONAIS DA ÁREA DE SIC

Aos órgãos e entidades da APF, no que tange a SIC recomenda-se:

6.1 Estabelecer ciclo de palestras, seminários, reuniões e outros eventos que contribuam para o constante processo de compartilhamento e absorção do conhecimento nos domínios da SIC.

6.2 Promover a troca de conhecimento e experiências no contexto e domínios de SIC por meio de grupos de trabalho formalmente instituídos, seguindo preferencialmente os temas propostos no ANEXO B.

6.3 Designar, sempre que solicitado, profissionais da área de SIC para integrar os grupos de trabalho citados no item 6.2.

6.4 Designar profissionais da área de SIC para participarem da elaboração do planejamento estratégico e da programação orçamentária do órgão ou entidade a qual mantenham vínculo.

6.5 Estabelecer no planejamento estratégico e tático ações que contemplem os aspectos de formação educacional, retenção e compartilhamento do conhecimento em SIC.

6.6 Prover a capacitação dos profissionais de SIC, em âmbito interno e externo, preferencialmente alinhada às certificações profissionais e aos temas recomendados nos ANEXOS A e B.

6.7 Estabelecer políticas de incentivo ao estudo e à pesquisa, bem como a produção e aquisição de obras literárias e normas técnicas de SIC e áreas correlatas.

7 VIGÊNCIA

Esta Norma entra em vigor na data de sua publicação.

8 ANEXOS

A - CERTIFICAÇÕES RECOMENDADAS PARA PROFISSIONAIS DE SIC

B - LINHAS E TEMAS DE SIC PARA FORMAÇÃO/CAPACITAÇÃO E ATIVIDADES RELACIONADAS AO COMPARTILHAMENTO/TROCA DE CONHECIMENTO

ANEXO A

CERTIFICAÇÕES RECOMENDADAS PARA PROFISSIONAIS DE SIC

FOCO	CERTIFICAÇÃO	ENTIDADE
Gestão da Segurança da Informação	CISM - Certified Information Security Manager	ISACA
	CISSP - Certified Information Systems Security Professional	*ISC*²
	CISSP (ISSAP) - Information Systems Security Architecture Professional	*ISC*²
	CISSP (ISSEP) - Information Systems Security Engineering Professional	*ISC*²
	CISSP (ISSMP) - Information Systems Security Management Professional	*ISC*²
	ISFS - Information Security Foundation based on ISO/IEC 27002	EXIN
	ISMAS - Information Security Management Advanced based on ISO/IEC 27002	EXIN
	ISMES - Information Security Management Expert based on ISO/IEC 27002	EXIN
	MCSO - Modulo Certified Security Officer	Módulo
Segurança de Redes	CompTIA Security+	Comptia
	ECSA - Ec-Council Security Analyst	Ec-Council
	GAWN - GIAC Assessing Wireless Networks	SANS
	GCIA - GIAC Certified Intrusion Analyst	SANS
	GPEN - GIAC Penetration Tester	SANS
	SSCP - Systems Security Certified Practitioner	ISC²
Segurança de Redes/Gestão da Segurança da Informação	CASP - CompTIA Advanced Security Practitioner	Comptia

FOCO	CERTIFICAÇÃO	ENTIDADE
Segurança de Redes/Segurança no Desenvolvimento de Software	CEH - Certified Ethical Hacker	Ec-Council
	GWAPT - GIAC Certified Web Application Penetration Tester	SANS
	LPT - Licensed Penetration Tester	Ec-Council
Tratamento de Incidentes de Segurança Computacional	GCIH - GIAC Certified Incident Handler	SANS
Forense Computacional	CHFI - Certified Hacking Forensic Investigator	Ec-Council
	GCFA - GIAC Certified Forensic Analyst	SANS
	GCFE - GIAC Certified Forensic Examiner	SANS
	GREM - GIAC Certified Reverse Engineering Malware	SANS
Segurança no Desenvolvimento de Software	CSSLP - Certified Secure Software Lifecycle Professional	*ISC*²
Gestão de Continuidade de Negócios	ABCP - Associate Business Continuity Professional	DRI International
	AMBCI - Associate Member Business Continuity Institute	BCI
	CBCI - Certified Business Continuity Institute	BCI
	CBCP - Certified Business Continuity Professional	DRI International
	CFCP - Certified Functional Continuity Professional	DRI International
	MBCP - Master Business Continuity Professional	DRI International
	SBCI - Specialist Business Continuity Institute	BCI

FOCO	CERTIFICAÇÃO	ENTIDADE
Auditoria/Conformidade	Auditor Lider ISO 27001	RAB ou IRCA
	CISA - Certified Information Systems Auditor	ISACA
Gestão/Auditoria/Conformidade	Cobit - Control Objectives for Information and related Technology	ISACA
	CRISC - Risk and Information Systems Control	ISACA
	ITIL - Information Technology Infrastructure Library	OGC

SIGLAS (ENTIDADE):

BCI - Business Continuity Institute
Comptia - Computing Technology Industry Association
DRI International - Disaster Recovery Institute International
Ec-Council - Electronic Commerce Consultants
EXIN - Examinations Institute
GIAC - Global Information Assurance Certification
IRCA - International Register of Certificated Auditors
ISACA - Information Systems Audit and Control Association
*ISC*² - International Information Systems Security Certification Consortium, Inc.
OGC - Office of Government Commerce
RAB - Registrar Accreditation Board
SANS - SysAdmin Audit Networking and Security

ANEXO B

LINHAS E TEMAS DE SIC PARA FORMAÇÃO/CAPACITAÇÃO E ATIVIDADES RELACIONADAS AO COMPARTILHAMENTO/TROCA DE CONHECIMENTO

LINHA/TEMA	CONTEÚDO RECOMENDADO
Gestão da Segurança da Informação e Comunicações	Gestão de Segurança da Informação e Comunicações
	Governança e Riscos
	Leis, Regulação e Conformidade
	Segurança em Redes
	Controle de Acesso Físico e Lógico
	Gestão de Continuidade de Negócios
	Criptografia e Infraestrutura de Chaves Públicas (ICP)
	Desenvolvimento Seguro
	Gerencia de Projetos
	Gestão de Processos
	Prospecção de oportunidades, tecnologias e inovação em SIC
Segurança de Redes	Firewall
	IDS/IPS
	Arquiteturas e Escopo de Segurança
	Segmentação
	Tunelamento de Tráfego e VPN
	Segurança de Perímetro
	Segurança de Aplicações e Serviços
	Segurança Redes Wireless e Serviços Móveis
	Segurança dos Dispositivos de Rede
Tratamento de Incidentes de Segurança Computacional	Aspectos Normativos: criação de CSIRTS, CSIRTS de Governo; CSIRTS na Rede Mundial de Computadores
	Processos de Monitoramento e Detecção de Intrusão
	Processos de Análise e Resposta a Incidentes
	Processos de Divulgação e Comunicação com Entidades Externas

LINHA/TEMA	CONTEÚDO RECOMENDADO
Forense Computacional	Aspectos Normativos
	Técnicas de Cópia e Preservação de Evidências
	Técnicas de Análise Forense
Segurança no Desenvolvimento de Software	Vulnerabilidades de Software
	Testes de Vulnerabilidade
	Arquitetura de Software Seguro
	Codificação de Software Seguro
	Firewall de Aplicações Web
Gestão de Continuidade de Negócios	Gestão de Continuidade de Negócios e Recuperação de Desastres
	Estratégias de Gestão de Continuidade de Negócios
	Implementação, Manutenção e Testes
	Cultura da Gestão de Continuidade de Negócios
Gestão de Riscos	Planejamento de Gestão de Riscos
	Metodologias de Gestão de Riscos
	Identificação de Riscos
	Análise/Avaliação de Riscos
	Tratamento de Riscos
Auditoria/Conformidade	Planejamento
	Análise dos Riscos
	Execução
	Relatório Final
Certificação Digital	Conceitos e Recursos
	Convenções, Políticas e Formatos
	Aplicações em uso
Computação em Nuvem	Conceitos Básicos
	Modelos de Computação em Nuvem
	Riscos da Computação em Nuvem
	Proteção dos Dados
	Responsabilidades dos Usuários
	Responsabilidades do Provedor de Serviço

LINHA/TEMA	CONTEÚDO RECOMENDADO
Mobilidade	Conceito e Evolução
	Riscos de Segurança associados com os Dispositivos Móveis
	Segurança para Dispositivos Móveis
	Gerenciamento de Dispositivos Móveis
	Responsabilidades dos Usuários
Redes Sociais	Conceito e Evolução
	Riscos de Segurança associados com o uso das Redes Sociais
	Privacidade, Exposição e Comportamento do Usuário
	Principais Controles de Segurança