MINISTÉRIO DA EDUCAÇÃO
Instituto Federal de Educação, Ciência e Tecnologia de Brasília

RESOLUÇÃO N.º 034-2011/CSIFB

Aprova a Política de Segurança da Informação e Comunicações (POSIC) no âmbito do IFB

O Presidente do Conselho Superior do INSTITUTO FEDERAL DE BRASÍLIA, nomeado pela Portaria Nº 649, de 23 de maio de 2011, publicada no Diário Oficial da União em 24 de maio de 2011, em observância ao disposto no §1º do art. 10 da Lei nº 11.892, de 29 de dezembro de 2008, e em conformidade com o disposto no inciso IX, art. 9º, do Estatuto do IFB;

CONSIDERANDO o que consta na Norma Complementar nº 03/IN01/DSIC/GSIPR;

CONSIDERANDO o que consta no Processo nº. 23098.001837/2011-09, de 30 de novembro de 2011;

CONSIDERANDO decisão da 10ª Reunião Ordinária do Conselho Superior do IFB, realizada no dia 13 de dezembro de 2011;

No uso de suas atribuições legais, R E S O L V E:

Art. 1° APROVAR a Política de Segurança da Informação e Comunicações (POSIC) no âmbito do IFB, devendo ser criados ambientes reais e virtuais em conformidade com os objetivos e finalidades do IFB, a legislação pertinente, seu estatuto, plano de desenvolvimento institucional e projeto político pedagógico, na forma do anexo desta Resolução.

Parágrafo único. As informações geradas ou acessadas por atividades de ensino, pesquisa ou extensão serão controladas apenas com relação à identificação do usuário ou proprietário das mesmas, protegendo o direito à propriedade intelectual e a liberdade acadêmica, e ainda atendendo ao disposto no art.10 da Lei nº 9.296/96.

Brasília – DF, 22 de dezembro de 2011.

WILSON CONCIANI
Presidente do Conselho Superior do IFB

POLÍTICA DE SEGURAÇA DA INFORMAÇÃO E COMUNICAÇÃO (POSIC) DO INSTITUTO FEDERAL DE BRASÍLIA

CAPÍTULO I
DO ESCOPO

Art. 2° A POSIC objetiva instituir diretrizes estratégicas, responsabilidades e competências, visando assegurar a integridade, confidencialidade, disponibilidade e autenticidade das informações custodiadas e de propriedade do IFB, de modo a preservar os seus ativos e sua imagem institucional.

Art. 3° A POSIC trata do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito do IFB, em todo o seu ciclo de vida - criação, manuseio, divulgação, armazenamento, transporte e descarte -, visando a continuidade de seus processos críticos, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

Art. 4° Esta POSIC se aplica a todas as unidades da estrutura organizacional do IFB.

CAPÍTULO II
CONCEITOS E DEFINIÇÕES

Art. 5° Para fins desta Resolução, entende-se por:

I - Política de Segurança da Informação e Comunicações: documento aprovado pela autoridade responsável do pelo IFB, com o objetivo de definir diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

II - dispositivo ou recurso de tecnologia da informação e comunicações (TIC): todo e qualquer material que permita a armazenagem e/ou veiculação de informações ou dados, por qualquer processo, seja ele óptico, gráfico, magnético ou eletrônico;

III - gestor da informação: servidor público do IFB responsável pela administração das informações geridas nos processos de trabalho sob sua responsabilidade;

IV - incidente: evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

V - agente público: aquele que, por força de lei, contrato ou qualquer ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira, ao IFB;

VI - dado: representação de uma determinada situação ou evento em determinado espaço e tempo, sob uma forma apropriada ao armazenamento, processamento ou transmissão, não fornecendo julgamento nem interpretações para a tomada de decisões;

VII - informação: dados e fatos dotados de relevância e propósito que foram organizados e comunicados de forma coerente e com significado e a partir dos quais se podem tirar conclusões e interpretações; e

VIII - documento: toda a base de conhecimento, fixada materialmente, susceptível de ser utilizada para consulta, estudo ou prova.

CAPÍTULO III
REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 6° Este documento baseia-se nos seguintes requisitos legais e normativos:

I - Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

II - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

III - Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

IV - Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

V - Decreto nº 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores – Internet;

VI – Lei nº 9.610, de 19 de fevereiro de 1998, altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.

VII - Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

VIII - Norma Complementar no 03/IN01/DSIC/GSI/PR, de 03 de julho de 2009, que estabelece as diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta;

IX - Norma ABNT NBR ISO/IEC 27001:2006 – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos;

X - Norma ABNT NBR ISO/IEC 27002:2005 – Técnicas de segurança - Código de práticas para a segurança da informação;

CAPÍTULO IV
DAS DIRETRIZES GERAIS

Seção I
Do Tratamento da Informação

Art. 7° Toda informação criada, adquirida ou custodiada pelo agente público, no exercício de suas atividades, é considerada um bem e deve ser protegida de acordo com as

regulamentações de segurança existentes com o objetivo de minimizar riscos às atividades e serviços prestados pelo IFB, preservando sua imagem.

Art. 8° As informações produzidas ou custodiadas pelo IFB devem ser descartadas conforme o seu nível de classificação.

Seção II
Da Classificação da Informação

Art. 9° As informações custodiadas ou de propriedade do IFB devem ser classificadas levando-se em consideração seu valor, criticidade, sensibilidade e requisitos legais e receber o nível de proteção condizente com sua classificação, conforme normas e legislação específica em vigor.

Art. 10 O gestor da informação é responsável por atribuir o nível de classificação das informações sob sua responsabilidade.

Art. 11 A classificação deve ser respeitada durante todo o ciclo de vida da informação, ou seja, criação, manutenção, armazenamento, transporte e descarte.

Seção III
Da Sensibilização, Conscientização e Capacitação

Art. 12 O IFB desenvolverá processo permanente de divulgação, sensibilização, conscientização e capacitação dos agentes públicos sobre os cuidados e deveres relacionados à segurança da informação e comunicações.

Seção IV
Da Gestão de Riscos

Art. 13 O IFB deve adotar processo contínuo de gestão de riscos, o qual será aplicado na implantação e operação da gestão de segurança da informação e comunicações.

Seção V
Da Gestão de Continuidade

Art. 14 O IFB deve manter processo de gestão de continuidade das atividades e processos críticos, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil.

Art. 15 As ações de continuidade do IFB devem ser adotadas por todos os titulares de unidade administrativa, de forma a proteger a reputação e a imagem institucional.

Art. 16 As informações de propriedade ou custodiadas pelo IFB, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança de forma a garantir a continuidade das atividades do órgão. As informações armazenadas em outros meios devem possuir mecanismos de proteção que preservem sua integridade, conforme o nível de classificação atribuído.

Seção VI
Do Uso de Recursos Computacionais e Comunicações

Art. 17 O uso de recursos computacionais e de comunicações do IFB pelos agentes públicos deve ser direcionado exclusivamente para realização das atividades profissionais desempenhadas para o órgão no limite dos princípios da ética, razoabilidade e legalidade.

Art. 18 Não é permitida a utilização de programas que violem direitos autorais, conforme legislação em vigor.

Seção VII
Dos Controles de Acesso

Art. 19 O IFB deve sistematizar a concessão de acesso como forma de evitar a quebra de segurança da informação e comunicações.

Art. 20 O acesso às informações custodiadas ou de propriedade do IFB pelos agentes públicos deve ser restrito ao necessário para desempenho de suas funções.

Art. 21 O acesso físico às instalações do IFB deverá ser regulamentado com o objetivo de garantir a segurança dos agentes públicos e a proteção dos seus ativos.

CAPÍTULO V
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 22 É dever do agente público do IFB conhecer e zelar pelo cumprimento da POSIC.

Art. 23 Os agentes públicos são responsáveis pela segurança dos ativos e processos que estejam sob sua custódia e por todos os atos executados com suas identificações, tais como crachá, *login*, senha eletrônica, certificado digital e endereço de correio eletrônico.

Parágrafo único. A identificação do usuário deve ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o seu reconhecimento.

CAPÍTULO VI
DAS NORMAS ESPECÍFICAS DE SEGURANÇA

Art. 24 Os aspectos de segurança física, lógica e de pessoal, serão tratados em documentos independentes, a fim de complementar com maior especificidade e detalhamento as normas e recomendações de segurança no trato das informações.

Parágrafo único. Todos os procedimentos relacionados à Segurança da Informação, definidos em instruções específicas, devem estar de acordo com esta Política, e uma vez divulgados, passam a ser parte integrante da mesma.

CAPÍTULO VII
DA ESTRUTURA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 25 Fica instituído, no âmbito do IFB o Comitê de Segurança da Informação e Comunicações, com as seguintes competências:

I- assessorar na implementação das ações de segurança da informação e comunicações no Instittuto;

II- constituir grupos de trabalho para tratar temas e propor soluções específicas sobre segurança da informação e comunicações; e

III- propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com a legislação existente sobre o tema.

Parágrafo único. O Comitê de Segurança da Informação e Comunicações será constituído por meio de portaria do reitor.

Art. 26 Fica instituído, no âmbito do IFB o Gestor de Segurança da Informação e Comunicações, com as seguintes competências:

I - promover cultura de segurança da informação e comunicações;

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III - propor recursos necessários às ações de segurança da informação e comunicações;

IV - coordenar a equipe de tratamento e resposta a incidentes em redes computacionais;

V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VI - manter contato direto com o Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações; e

VII - propor normas relativas à segurança da informação e comunicações.

Parágrafo único. O gestor de segurança da informação e comunicações será designado em expediente próprio.

Parágrafo único. O gestor de segurança da informação e comunicações deverá reportar-se sempre ao Comitê de Segurança da Informação e Comunicações.

Art. 27 Fica instituída, no âmbito do IFB, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), conforme a Norma Complementar Nº 5, de 14 de agosto de 2009.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Art. 28 O descumprimento ou violação de um ou mais itens desta Política de Segurança da Informação e Comunicações poderá resultar na aplicação de sanções administrativas, penais, ou civis.

Art. 29 A POSIC e todos os instrumentos normativos gerados a partir dela devem ser revisados sempre que se fizer necessário, não devendo exceder o período máximo de 3 (três) anos.

Art. 30. Os casos omissos serão resolvidos pelo Comitê Gestor de Tecnologia da Informação e Comunicação (CGITC).

Art. 31 Esta Resolução entra em vigor na presente data.