INSTITUTO FEDERAL DE
EDUCAÇÃO CIÊNCIA E TECNOLOGIA
Baiano

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

DEZEMBRO/2011

Rua do Rouxinol, N°115 / Salvador – Bahia –CEP: 41 .720-052
Telefone: (71) 3186-0001. Email: cgti@listas.ifbaiano.edu.br
Site: http://www.ifbaiano.edu.br

SUMÁRIO

1 FINALIDADE

A Política de Segurança da Informação e Comunicação do IF Baiano é uma declaração formal do IF Baiano acerca do seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço que exerçam atividades no âmbito do IF Baiano ou quem quer que tenha acesso a dados ou informações no ambiente do IF Baiano. O seu propósito é estabelecer diretrizes, normas, procedimentos, e responsabilidades adequadas para o manuseio, tratamento, controle e proteção das informações pertinentes ao IF Baiano.

2 DECLARAÇÃO DE COMPROMETIMENTO DA DIRETORIA

O Magnífico Reitor do IF Baiano declara-se comprometida em proteger todos os ativos de informação do IF Baiano.

3 PRINCÍPIOS

Esta política abrange onze aspectos básicos da Segurança da Informação e Comunicação, destacados a seguir:

I. Confidencialidade: somente pessoas devidamente autorizadas pela organização devem ter acesso à informação;

II. Integridade: somente operações de alteração, supressão e adição autorizadas pela organização devem ser realizadas nas informações;

III. Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado;

IV. Autenticidade: princípio de segurança que assegura ser do autor a responsabilidade pela criação ou divulgação de uma dada informação;

V. Criticidade: princípio de segurança que define a importância da informação para a continuidade da atividade-fim da Instituição;

VI. Não-Repúdio: garantia que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação;

VII. Responsabilidade: as responsabilidades iniciais e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas. Todos os servidores do IF Baiano são responsáveis pelo tratamento da informação e pelo cumprimento das normas de Segurança da Informação e Comunicação;

VIII. Conhecimento: todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço devem ter ciência de normas, procedimentos, orientações e outras informações que permitam a execução de suas atribuições sem comprometer a segurança;

IX. Ética: todos os direitos e interesses legítimos de servidores, colaboradores, estagiários, prestadores de serviço e usuários do sistema de Informação ORGANIZAÇÃO devem ser respeitados;

X. Legalidade: além de observar os interesses do IF Baiano, as ações de Segurança da Informação e Comunicação levarão em consideração leis, normas, políticas organizacionais, administrativas, técnicas e operacionais, padrões, procedimentos aplicáveis e contratos com terceiros, dando atenção à propriedade da informação e direitos de uso;

XI. Proporcionalidade: o nível, a complexidade e os custos das ações de Segurança da Informação e Comunicação na ORGANIZAÇÃO serão adequados ao entendimento administrativo e ao valor do ativo a proteger;

4 TERMOS E DEFINIÇÕES

Para os efeitos desta Política, entende-se por:

I. Política de Segurança de Informação e Comunicação: conjunto de normas destinadas à proteção dessa informação e à disciplina do seu manuseio;

II. Contingência: indisponibilidade ou perda de integridade da informação que os dispositivos de segurança não tenham conseguido evitar;

III. Gestor: setor do IF Baiano responsável pela definição de critérios de acesso, classificação, tempo de vida e normas específicas do uso da informação;

IV. Usuário interno: qualquer pessoa física ou unidade interna que faça uso de informações e que esteja vinculada administrativamente ao IF Baiano;

V. Usuário externo: qualquer pessoa física ou jurídica que faça uso de informações e que não esteja vinculada administrativamente ao IF Baiano;

VI. Comunicação oficial: tráfego de documentos, informações ou formulários emitidos por caixas postais eletrônicas do IF Baiano, de atividades especiais ou de projetos específicos;

VII. Comunicação informal: tráfego de documentos, informações ou formulários que não estejam incluídos no conceito de que trata o ponto anterior, emitidos via caixas postais eletrônicas individuais de autoridade, servidor, estagiário ou fornecedor de bens e/ou serviços;

VIII. Plano de continuidade: conjunto de procedimentos que devem ser adotados quando a Instituição deparar-se com problemas que comprometam o andamento normal dos processos e a consequente prestação dos serviços;

IX. Plano de Segurança da Informação e Comunicação: conjunto de princípios que norteiam a Gestão de Segurança de Informação e Comunicação e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos;

X. Princípios da Segurança da Informação e Comunicação: são princípios que regem a Segurança da Informação e Comunicação, em acordo com o artigo 3° do Decreto n° 3.505, de 13 de junho de 2000, quais sejam: confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio;

XI. Termo de responsabilidade: acordo de confidencialidade e não divulgação de informações que atribui responsabilidades ao Colaborador e Administrador de Serviço quanto ao sigilo e a correta utilização dos ativos de propriedade ou custodiados pelo IF Baiano;

XII. Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da Segurança da Informação e da Comunicação;

XIII. Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XIV. Continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável e previamente definido;

XV. Plano de gerenciamento de incidentes: plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente e cubra as pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

XVI. Plano de recuperação de negócios: documentação cujo conteúdo abrange os procedimentos e informações necessárias para que a organização operacionalize o retorno das atividades críticas à normalidade;

XVII. Gestão da continuidade de negócios: processo contínuo de gestão e governança suportado pela alta direção com recursos apropriados para garantir que as ações necessárias de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento dos produtos;

XVIII. Análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco;

XIX. Avaliação de riscos: processo onde se compara o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

XX. Gestão de riscos de Segurança da Informação e Comunicação: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

XXI. Identificação de riscos: processo para localizar, listar e caracterizar elementos do risco;

XXII. Tratamento dos riscos: processo e implementação de ações de Segurança da Informação e Comunicação para evitar, reduzir, reter ou transferir um risco;

XXIII. Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de Segurança da Informação e Comunicação;

XXIV. Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

5 ESCOPO

O escopo do Plano de Segurança da Informação e Comunicação do IF Baiano refere-se:

I. Aos aspectos estratégicos, estruturais e organizacionais, preparando a base para elaboração dos demais documentos normativos que as incorporarão;

II. Aos requisitos de segurança humana;

III. Aos requisitos de segurança física;

IV. Aos requisitos de segurança lógica;

V. Á sustentação dos procedimentos, dos processos de trabalho e dos ativos que influirão diretamente nos produtos e serviços oriundos da Informação e Comunicação do IF Baiano.

6 ESTRUTURA NORMATIVA DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÂO

A estrutura normativa da Segurança da Informação e Comunicação do IF Baiano é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

I. Política de Segurança da Informação e Comunicação (Política): constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à Segurança da Informação e Comunicação;

II. Normas de Segurança da Informação e Comunicação (Normas): estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada;

III. Procedimentos de Segurança da Informação e Comunicação (Procedimentos): instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades do IF Baiano.

7 DIRETRIZES GERAIS

Servidores, colaboradores, consultores externos, estagiários e prestadores de serviço no IF Baiano devem observar que:

I. Acesso, Proteção e Guarda da Informação: o acesso à informação deve ser regulamentado por normas específicas de tratamento da informação. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo IF Baiano é considerada seu patrimônio e deve ser protegida;

II. Deverão ser estabelecidas normas para as operações de armazenamento, divulgação, reprodução, transporte, recuperação e destruição da informação serão definidos de acordo com a classificação desta, sem prejuízo de outros cuidados que serão especificados pelo gestor;

III. Gestão de Risco: é estabelecido um processo de Gestão de Risco, contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicação, produzindo subsídios para a Gestão de Continuidade dos Negócios. Os riscos devem ser monitorados e analisados periodicamente, a fim de verificar mudanças nos critérios de avaliação e aceitação dos riscos, no ambiente, nos ativos de informação e em fatores de risco, como ameaça, vulnerabilidade, probabilidade e impacto;

IV. Plano de Continuidade: é constituído de um conjunto de medidas, regras e procedimentos definidos, que serão adotados para assegurar que as funções ou atividades críticas da Instituição possam ser mantidas ou recuperadas após falha ou interrupção na operação normal dos sistemas direta ou indiretamente envolvidos com a gestão das informações;

V. Auditoria e Conformidade: deverá ser levantado regulamente os aspectos legais de segurança aos quais as atividades do IF Baiano estão submetidas, de forma a evitar ações penais decorrentes da não observância de tais aspectos por desconhecimento ou omissão;

VI. Segurança Física: controles que monitorem o acesso físico a equipamentos, documentos, suprimentos e locais físicos do IF Baiano e que garantam a proteção dos recursos de forma que apenas as pessoas autorizadas tenham acesso, restringindo a entrada e saída de visitantes, pessoal interno, equipamentos e mídias, estabelecendo perímetros de segurança;

VII. Uso de e-mail: o serviço de correio eletrônico disponibilizado pela Organização constitui recurso do IF Baiano disponibilizado na rede de comunicação de dados para aumentar a agilidade, segurança e economia da comunicação oficial e informal. O correio eletrônico deve ser utilizado exclusivamente no interesse do serviço, passível de auditoria por solicitação de Comissão de Processo Administrativo Disciplinar;

VIII. Capacitação e Aperfeiçoamento: os servidores deverão ser continuamente capacitados para o desenvolvimento de competências em Segurança da Informação e Comunicação;

IX. Acesso a Internet: todos os servidores têm o direito de acesso à internet, com utilização exclusiva para fins complementares às atividades do setor, para o enriquecimento intelectual de seus servidores ou como ferramenta para busca por informações que venham contribuir para o desenvolvimento de seus trabalhos;

X. Patrimônio Intelectual: as informações, os sistemas e os métodos criados pelos servidores do IF Baiano, no exercício de suas funções, são patrimônios intelectuais da Instituição, não cabendo a seus criadores qualquer forma de direito autoral;

XI. Termo de Responsabilidade e Sigilo: é o documento oficial que compromete colaboradores, terceirizados e prestadores de serviço com a política de segurança do IF Baiano.

8 COMPETÊNCIAS E RESPONSABILIDADES

A implementação, o controle e a gestão da política de Segurança da Informação e Comunicação são de responsabilidade da seguinte infraestrutura de gerenciamento:

I. Autoridade máxima; é o Magnífico Reitor, responsável pela aprovação da Política de Segurança da Informação e Comunicação;

II. “Grupo de Trabalho de Segurança da Informação e Comunicação”, responsável por:

a. Promover cultura de Segurança da Informação e Comunicação;
b. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
c. Propor recursos necessários às ações de Segurança da Informação e Comunicação;
d. Requerer e acompanhar atividades da a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, setor ligado à Diretoria de Gestão de tecnologia da Informação;
e. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na Segurança da Informação e Comunicação;

f. Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à Segurança da Informação e Comunicação;
g. Promover intercambio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privas sobre as atividades de segurança da informação (art.3º, VI do Decreto 3..505 de 2000);
h. Propor Normas adicionais e procedimentos relativos à segurança da informação e comunicação no âmbito do IF Baiano.

9 DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

A Política e as Normas de Segurança da Informação e Comunicação devem ser divulgadas a todos os colaboradores do IF Baiano, e dispostas de maneira que o seu conteúdo possa ser consultado a qualquer momento.

I. As áreas atingidas por esta política são imediatamente responsáveis pela elaboração e proposição de normas, procedimentos e atividades necessárias ao cumprimento desta política;
II. As áreas deverão submeter suas propostas de normas ao “Comitê de Segurança da Informação e Comunicação” para análise, discussão e aprovação no âmbito do Comitê;
III. Após aprovação, estas normas e procedimentos serão divulgadas aos interessados pela área responsável por sua manutenção.

10 REVISÕES E ATUALIZAÇÃO

Esta POSIC será revista e alterada sempre que as atribuições e normas do IF Baiano justificar as alterações, sendo ainda obrigatória a revisão anual.

11 VIOLAÇÕES, PENALIDADES E SANÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Nos casos em que houver o descumprimento ou violação de um ou mais itens da Política ou das Normas, procedimentos ou atividades pertinentes à Segurança da Informação e Comunicação, serão tratadas conforme legislação e regulamentos internos aplicáveis.

12 VIGÊNCIA E VALIDADE

A presente política passa a vigorar a partir da data de sua publicação.

Publique-se e Cumpra-se

SEBASTIÃO EDSON MOURA
Reitor

REFERÊNCIAS LEGAIS E NORMATIVAS

As referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicações do IF Baiano são:

- ABNT NBR ISO 17799: 2005 - Código de Práticas para a Gestão da Segurança da Informação.

- ABNT NBR ISO Guia 73: 2002 - Gestão de Riscos / Vocabulário.

- ISO/IEC TR 13335-3: 1998 - fornece técnicas para a gestão de segurança na área de tecnologia da informação. Baseada na norma ISO/IEC 13335-1 e TR ISO/IEC 13335-2. As orientações são projetadas para auxiliar o incremento da segurança na TI.

- ISO/IEC GUIDE 51: 1999 - fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos.

- Constituição Federal de 1988.

- Lei nº 9.983, de 14 de julho de 2000 - Altera o Decreto Lei nº 2848/40 – Código Penal - tipificação de crimes por computador contra a Previdência Social e a Administração Pública.

- Decreto 1.171, de 24 de junho de 1994 - Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, e outras providências.

- Código Processo Penal - Lei 3.689, de 03 de outubro de 41, atualizado até as alterações introduzidas pelas Leis nº 11.900, de 08.01.09.

- Código de Processo Civil - Lei 5.869, de 11 de janeiro de 1973.

- Lei nº 7.232 de 29 de Outubro de 1984 - Política Nacional de Informática, e dá outras providências.

- Lei nº 8.027 de 12 de abril de 1990 - Normas de conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas, e dá outras providências.

- Lei nº 8.112 de 11 de dezembro de 1990 - Regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

- Lei nº 8.429 de 2 de junho de 1992 - sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional e dá outras providências.

- Decreto nº 6.029 de 1 de fevereiro de 2007 - Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências.

- Lei nº 8.159 de 8 de janeiro de 1991 - política nacional de arquivos públicos e privados e dá outras providências.

- Decreto nº 1.048 de 21 de janeiro de 1994 - Sistema de Administração dos Recursos de Informação e Informática, da Administração Pública Federal, e dá outras providências.

- 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.

- 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.

- Lei nº 9.983, de 14 de julho de 2000: Altera o Decreto Lei nº 2848/40 – Código Penal, sobre tipificação de crimes por computador contra a Previdência Social e a Administração Pública.

• Decreto 1.171, de 24 de junho de 1994 que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, e outras providências.

• Normas e Resoluções do Gabinete de Segurança Institucional da Presidência da Republica.

- Instrução Normativa GSI Nº 01 de 13 de Junho de 2008.
- Norma Complementar nº 02/IN01/DSIC/GSIPR, de 14 Out 2008.
- Norma Complementar nº 03/IN01/DSIC/GSIPR, de 03 Jul 2009.
- Norma Complementar nº 04/IN01/DSIC/GSIPR, de 17 Ago 2009.
- Norma Complementar nº 05/IN01/DSIC/GSIPR, de 17 Ago 2009.
- Norma Complementar nº 06/IN01/DSIC/GSIPR , de 23 Nov 2009.

• Acórdão 1603/2008 do Plenário do Tribunal de Contas da União – TCU.