ORIGEM

Instituto Federal da Bahia – Comitê de Tecnologia da Informação

CAMPO DE APLICAÇÃO

Esta Política de Segurança da Informação se aplica no âmbito do IFBA.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

AURINA SANTANA

Reitora

Instituto Federal de Educação, Ciência e Tecnologia da Bahia

1. ESCOPO

1.1. Apresentação

O IFBA tem como missão "Promover a formação do cidadão histórico-crítico, oferecendo ensino, pesquisa e extensão com qualidade socialmente referenciada, objetivando o desenvolvimento sustentável do país". Nos dias atuais o avanço das tecnologias tem mudado o perfil da sociedade que se tornou cada vez mais conectada com o mundo digital e com as formas de agir, gerir e produzir conhecimento e informação nesta nova realidade.

Em um cenário moderno e ao mesmo tempo prezando pela qualidade de seus serviços educacionais, a Instituição não pode deixar de acompanhar tal evolução e por isso, vem investindo em recursos tecnológicos.

Com o aumento do emprego desses recursos, crescem igualmente as ameaças e os riscos que envolvem tais tecnologias. Assim, considerando a Instrução Normativa GSI/PR nº1, de 13 de junho de 2008 que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, Direta e Indireta, o IFBA considera necessário criar e formalizar uma Política de Segurança da Informação e Comunicações, visando a atingir os objetivos descritos neste documento.

1.2. Objetivos

A Política de Segurança da Informação e Comunicações (PSIC) tem como objetivo declarar o comprometimento formal da Instituição com vistas a prover diretrizes estratégicas, atribuir responsabilidades, delimitar competências e conceber estruturas de apoio para implementar a Gestão de Segurança da Informação e Comunicações (GSIC) no IFBA, devendo ser cumprida por todos que exerçam atividades no âmbito da Instituição, sejam servidores docentes e técnico-administrativos, discentes, estagiários, terceirizados, bolsistas, colaboradores, consultores externos ou quem quer que tenha acesso aos ativos, ativos de informação e dados do IFBA.

Essa Política tem também o objetivo de estabelecer diretrizes que nortearão as normas, procedimentos, mecanismos, competências, responsabilidades, direcionamentos e valores a serem adotados para a Gestão de Segurança da Informação e Comunicações no âmbito

do IFBA, adequados ao manuseio, tratamento, controle e proteção dos ativos, ativos de informação e dados.

1.3. Abrangência e Aplicação

As diretrizes da PSIC do IFBA aplicam-se a todos os usuários dos ativos, ativos de informação e dados do IFBA.

Os acordos de cooperação, contratos, convênios e outros instrumentos do mesmo gênero celebrados com o IFBA devem observar o conteúdo desta PSIC.

2. CONCEITOS E DEFINIÇÕES

Estabelece as definições e conceitos dos seguintes termos para efeito dessa PSIC:

Ativo: qualquer bem, tangível ou intangível, que tenha valor para a Instituição;

Ativo de informação: qualquer informação que tenha valor para a Instituição [ISO/IEC 13335-1:2004];

Incidente: evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação;

Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a Instituição [ISO/IEC 13335-1:2004];

Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação [ISO/IEC TR 18044:2004];

Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento;

Dados: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;

Controles de Segurança: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário [ISO/IEC 13335-1:2004];

Integridade: incolumidade de dados ou informações na origem, no trânsito ou no destino [ISO/IEC 13335-1:2004]; consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não-violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital.

Autenticidade: propriedade que garante que um indivíduo ou recurso é quem ele anuncia ser [ISO/IEC 13335-1:2004]; consiste na garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações, permitindo, inclusive, a identificação do emissor e do equipamento utilizado, quando for o caso;

Confidencialidade: propriedade de que a informação não esteja disponível ou divulgada a pessoas, entidades ou processos não autorizados [ISO/IEC 13335-1:2004];

Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

3. REFERÊNCIAS LEGAIS E NORMATIVAS

Essa política está fundamentada nas seguintes legislações e normas específicas:

Documento	Data	Conteúdo
Decreto nº 3.505	13 de junho de 2000	Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
Decreto nº 4.553	27 de dezembro de 2002	Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;
Decreto nº 5.482	30 de junho de 2005	Dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da Rede Mundial de Computadores - Internet;
Portaria Interministerial nº 140	16 de março de 2006	Disciplina a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores - internet e dá outras providências;
Acórdão do Tribunal de Contas da União nº 461/2004	28 de abril de 2004	Dispõe sobre a análise regular de arquivos logs com utilização, sempre que possível, de softwares utilitários específicos, para monitoramento do uso dos sistemas;
Instrução Normativa GSI nº 1	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;

Norma Complementar nº 03/IN01/DSIC/GSI/PR	03 de julho de 2009	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 - APF;
Norma Complementar nº 04/IN01/DSIC/GSI/PR	17 de agosto de 2009	Estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta - APF;
Norma Complementar nº 05/IN01/DSIC/GSI/PR	17 de agosto de 2009	Disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;
Norma Complementar nº 06/IN01/DSIC/GSI/PR	23 de novembro de 2009	Disciplina as Diretrizes para Gestão de Continuidade de Negócios nos aspectos relacionados à Segurança da Informação e Comunicações - GCN nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;
Norma Complementar nº 07/IN01/DSIC/GSI/PR	07 de maio de 2010	Disciplina as diretrizes para implementação de Controles de Acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;
Norma Complementar nº	24 de agosto de	Disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado

08/IN01/DSIC/GSI/PR	2010	pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;
Norma ABNT NBR ISO/IEC 27001	2006	Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos;
Norma ABNT NBR ISO/IEC 27002	2005	Técnicas de segurança - Código de práticas para a segurança da informação;
Norma ABNT NBR ISO/IEC 27005	2008	Técnicas de segurança - Gestão de riscos de segurança da informação
Norma ISO/IEC 13335:1	2004	Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management

4. PRINCÍPIOS

Esta Política de Segurança da Informação e Comunicações e os documentos elaborados a partir dela devem obedecer além dos princípios constitucionais, administrativos e legislativos vigentes que regem a Administração Pública Federal, também aos princípios da Segurança da Informação:

1. Confidencialidade: somente pessoas devidamente autorizadas e credenciadas devem ter acesso à informação não pública.
2. Integridade: somente operações de alteração, supressão e adição autorizadas pelo IFBA devem ser realizadas nas informações.
3. Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado.
4. Autenticidade: princípio de segurança que assegura ser do autor a responsabilidade pela criação ou divulgação de uma dada informação;
5. Não-Repúdio: garantia de que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação;

5. ESTRUTURA NORMATIVA DA PSIC

A PSIC está estruturada hierarquicamente com três níveis descritos a seguir:

- Política de Segurança da Informação e Comunicação – PSIC (Política): constituída neste documento, define a estrutura, estabelece as diretrizes e define as responsabilidades referentes à segurança da informação. A política abrange todo o Instituto;
- Normas de Segurança da Informação e Comunicação (Normas): estabelecem obrigações e definem procedimentos a serem seguidos de acordo com as diretrizes da Política;
- Procedimentos de Segurança da Informação (Procedimentos): definem as regras operacionais conforme o disposto nas Normas e na Política de Segurança, permitindo sua utilização nas atividades do Instituto.

A Política de Segurança da Informação, representada por este documento abrange todo o Instituto. As normas e os procedimentos são elaborados por cada Campus de forma a atender suas especificidades, sempre de acordo com as diretrizes aqui definidas.

6. DIRETRIZES GERAIS

Esta política tem a finalidade de definir as diretrizes para a Segurança da Informação, visando à preservação da integridade, confidencialidade e disponibilidade dos ativos, ativos de informação e dados do IFBA.

O IFBA é usuário dos serviços providos pela Rede Nacional de Ensino e Pesquisa (RNP), de acordo com o Programa Interministerial dos ministérios da Educação e da Ciência, Tecnologia e Inovação estando, portanto, por princípio, alinhado as suas Políticas e Normas de Segurança.

A PSIC deve ser conhecida e obedecida por todos que utilizam os ativos, ativos de informação e dados de propriedade ou controlados pelo IFBA, sendo de responsabilidade de cada um o seu cumprimento, considerando que zelar pela segurança da informação é dever de todos.

6.1. Tratamento da Informação

Toda informação criada, adquirida ou custodiada pela Instituição é considerada um bem e deverá ser protegida por normas específicas de tratamento da informação, portanto, o IFBA deverá criar, gerir e avaliar critérios de tratamento e classificação da informação observando a legislação em vigor.

A classificação deve ser respeitada durante todo o ciclo de vida da informação.

6.2. Gestão de Incidentes de Segurança da Informação

Os incidentes de segurança devem ser identificados, monitorados, comunicados e devidamente tratados.

6.3. Gestão de Riscos de Segurança da Informação

O IFBA deverá estabelecer um processo contínuo de Gestão de Riscos de Segurança da Informação considerando que os ativos devem ser monitorados e analisados periodicamente, de forma a possibilitar a seleção e a priorização dos ativos a serem

protegidos, bem como a definição e a implementação de controles para a identificação e o tratamento de possíveis falhas de segurança, minimizando dessa forma os fatores de risco.

6.4. Gestão de Continuidade

O IFBA deverá estabelecer um processo de Gestão de Continuidade de Negócio, observados a proteção e a disponibilidade dos seus ativos de informação.

6.5. Auditoria e Conformidade

O IFBA deverá criar e manter registros e procedimentos, que possibilitem o rastreamento, acompanhamento, controle e verificação de acessos aos sistemas de informação, conforme norma específica. Os serviços disponibilizados pelo IFBA, através dos diversos sistemas de informação, aos servidores técnico-administrativos e docentes, discentes, estagiários, bolsistas, terceiros ou visitantes constituem ativo do Instituto, sendo disponibilizado na rede conforme as normas específicas, com utilização para fins acadêmicos, científicos ou administrativos, estando assim, passível de auditoria, conforme previsto no item 9.1.4 do acórdão do Tribunal de Contas da União Nº 461 de 28 de abril de 2004.

6.6. Controles de Acesso

Os ativos do IFBA devem ser protegidos contra acesso não autorizado, danos, perdas, furtos e interferências, portanto o IFBA deverá instituir normas que estabeleçam procedimentos, processos e mecanismos que garantam o controle de acesso aos ativos, ativos de informação, dados, instalações e sistemas de informação.

6.7. Uso de correio eletrônico

O serviço de correio eletrônico disponibilizado pelo IFBA aos servidores técnico-administrativos e docentes, discentes, estagiários, terceiros ou visitantes constitui ativo do Instituto sendo disponibilizado na rede, conforme as normas específicas, para comunicação com fins acadêmicos, científicos ou administrativos sendo o mesmo, portanto, passível de auditoria.

6.8. Acesso ao serviço de Internet.

Toda a comunidade do IFBA tem o direito de acesso à internet, conforme as normas específicas, com utilização para fins acadêmicos, científicos ou administrativos, portanto, o mesmo é passível de auditoria.

7. PENALIDADES

A violação dos preceitos existentes nesta Política e nos documentos elaborados a partir dela poderá implicar na aplicação de sanções administrativas, cíveis e penais previstas na legislação em vigor.

8. COMPETÊNCIAS E RESPONSABILIDADES

É responsabilidade de todos que têm acesso aos ativos do IFBA conhecer e zelar pelo cumprimento da Política de Segurança da Informação e Comunicações, bem como, reportar, de imediato, ao Gestor de Segurança da Informação do IFBA, qualquer ocorrência de segurança ou, até mesmo, suspeitas iminentes.

9. ATUALIZAÇÃO

Esta Política bem como os documentos gerados a partir dela, deverá ser revisada ou atualizada sempre que se fizer necessário ou a cada 12 meses a partir da data de publicação.

10. VIGÊNCIA

Esta Política entra em vigor a partir da data da sua publicação.

11. DIVULGAÇÃO

Esta Política deve ser amplamente divulgada pelo Comitê Gestor de Segurança da Informação utilizando-se dos meios disponíveis.