<<Folha de Aprovação da PSI pelo Comitê Gestor em TI>>

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Dispõe sobre a criação da Política de Segurança da Informação e Comunicação do Instituto Federal da Paraíba

CAPÍTULO I
DA FINALIDADE

Art. 1º. A Política de Segurança da Informação e Comunicação, também representada pela sigla POSIC/IFPB, é uma declaração formal da Instituição sobre o seu compromisso com a proteção das informações onde contém as diretrizes para a segurança do manuseio, tratamento, controle e proteção das informação e comunicação no âmbito deste Instituto.

CAPÍTULO II
DO OBJETIVO

Art. 2º. Fornecer diretrizes, responsabilidades, competências e apoio da alta direção na implementação da gestão de segurança da informação e comunicações do Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB), buscando assegurar a disponibilidade, integridade e confidencialidade das informações.

CAPÍTULO III
DA DECLARAÇÃO DE COMPROMETIMENTO DA REITORIA

Art. 3º. A alta direção do IFPB, configurado na figura do Reitor e Diretores Gerais dos Campi, declara-se comprometida em proteger todos os seus ativos de informação além de apoiar e divulgar esta Política de Segurança da Informação.

CAPÍTULO IV
DO ESCOPO

Art. 4º. O escopo desta política serão todos os sistemas de informação e serviços de comunicação de domínio e/ou uso do IFPB, como sistemas administrativos, acadêmicos, e-mail institucional como também sites hospedados no domínio deste Instituto.

Os quesitos desta Política de Segurança da Informação serão aplicados de maneira mandatória na Reitoria, Campi e demais unidades, para todo aquele que de forma direta ou indireta fizer se relacionar com o IFPB.

CAPÍTULO V
DOS TERMOS E DEFINIÇÕES

Art. 5º. Para os efeitos desta política são estabelecidos os seguintes conceitos e definições:

§1. *Comitê Gestor de Tecnologia da Informação (CGTI)*: comitê responsável por apreciar e aprovar o Plano Diretor de Tecnologia da Informação (PDTI) e a Política de Segurança da Informação e Comunicações (POSIC) e demais normas e procedimentos a esta última relacionadas; analisar e aprovar os investimentos na área de Tecnologia da Informação e monitorar o estágio dos projetos e o nível dos serviços, recomendando ações para solução dos problemas de recursos e interesses da área;

§2. *Comitê Gestor de Segurança da Informação e Comunicação*: comitê responsável de assessorar a implementação das ações de segurança da informação e comunicações no âmbito da Instituição;

§3. *Diretoria Geral de Tecnologia da Informação (DGTI)*: órgão sistêmico executivo , que planeja, dirige, avalia e executa as políticas de tecnologia da

informação e comunicação (TIC) em todo o Instituto, em articulação com as Pró-Reitorias e as Direções Gerais dos Campi;

§4. *Equipe de Tratamento e Resposta de Incidentes (ETRI)*: equipe responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança;

§5. *Gestor de Segurança da Informação e Comunicação*: responsável pelas ações de segurança da informação e comunicações no âmbito da Instituição;

§6. *Política de Segurança da Informação e Comunicação (POSIC)*: documento aprovado pela autoridade responsável da Instituição, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação;

§7. Ativo de informação: qualquer informação que tenha valor para a Instituição, nos termos da Norma ISO/IEC no 13335-1:2004;

§8. Recurso de Tecnologia da Informação (RTIC): os equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados nas Unidades de Ensino, tais como:

I - equipamentos de informática e de telecomunicações de qualquer espécie;

II - infraestrutura e materiais de redes lógicas e de telecomunicações de qualquer espécie;

III - laboratórios de informática de qualquer espécie; e

IV - recursos de informação eletrônicos, tais como: serviços de rede, sistemas de informação, programas de computador, arquivos de configuração que são armazenados, executados e/ou transmitidos por meio da infraestrutura computacional do IFPB, redes ou outros sistemas de informação.

§9. Área responsável pela Tecnologia da Informaçã (T.I.): Denomina-se área responsável pela T.I., qualquer setor, coordenação, núcleo, centro de tecnologia ou outra divisão organizacional onde haja profissionais de T.I. responsáveis pela administração local.

§10. *Usuário*: qualquer pessoa física ou jurídica com vínculo oficial com o IFPB ou em condição autorizada que utiliza, de alguma forma, algum recurso de tecnologia da informação e comunicação (RTIC) do IFPB. Os usuários

poderão ser cadastrados ou não no domínio do IFPB e serão classificados, para fins de acesso aos recursos (RTIC), de acordo com os seguintes perfis:

I - Servidores: qualquer servidor, ativo ou aposentado, com vínculo ao IFPB;
II - alunos;
III - outros:
    a. responsável por entidade externa que utiliza o domínio do IFPB (procuradoria, grupos de pesquisa, e outros afins);
    b. entidade representativa de alunos;
    c. aluno bolsista;
    d. estagiário externo;
    e. servidores terceirizados;
    f. visitante;
    g. pensionista.

CAPÍTULO VI
DAS FUNDAMENTAÇÕES LEGAIS E NORMATIVAS

Art. 6º. As referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicação do IFPB são as seguintes:

§1. 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;

§2. Decreto 7.845, de 14 de novembro de 2012, que procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

§3. Instrução Normativa 01 de 13 de junho de 2008 (IN GSI/PR 01/2008) , disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

§4. Norma Complementar 03/IN01/DSIC/GSIPR de 30 de junho de 2009, discorre sobre diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

§5. Instrução Normativa IN SLTI/MP 04/2014 de 11 de setembro de 2010 que dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do SISP do Poder Executivo Federal.

CAPÍTULO VII
DOS PRINCÍPIOS

Art. 7º. A Segurança da Informação e Comunicações do IFPB orienta-se pelos seguintes princípios:

§1. *Disponibilidade*: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade. [IN01/DSIC/GSIPR];

§2. *Confidencialidade*: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado. [IN01/DSIC/GSIPR];

§3. *Integridade*: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental. [IN01/DSIC/GSIPR];

§4. *Não-repúdio*: garantia de que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação;

§5. *Autenticidade*: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade [IN01/DSIC/GSIPR, 2008, p. 2];

§6. *Legalidade*: garantia de que todas as ações de Segurança da Informação e Comunicação deverão obedecer aos princípios constitucionais, administrativos e à legislação vigente.

CAPÍTULO VIII
DAS DIRETRIZES GERAIS

Art. 8º. As seguintes diretrizes gerais deverão ser observadas por todos os envolvidos no IFPB:

§1. *Tratamento da Informação*: Deverão ser realizados procedimentos de tratamento, armazenamento, identificação e classificação das informações da instituição de tal forma a garantir a integridade, facilidade de localização e

evitar o uso dessas informações por pessoas não autorizadas. Deverão ser realizadas cópias de segurança das informações tomando como base a norma de gerenciamento de cópias de segurança da informação do IFPB;

§2. *Gestão de Riscos:* Será apresentado planos de gerenciamento de riscos e da ação de resposta a incidentes, a serem aprovados pelo Comitê Gestor de Tecnologia da Informação e executados pela DGTI e seus núcleos de tecnologia locais. Normas e Procedimentos para implantação e gerenciamento de riscos de Informação serão definidos em documento específico elaborado pelo Comitê Gestor de Segurança da Informação. Além disto, este comitê deverá realizar, periodicamente, treinamentos específicos de conscientização para todos os servidores em noções de segurança da informação visando à implantação e gerenciamento de todos os componentes do Sistema de Gestão de Segurança da Informação (SGSI) e a agilidade da notificação de qualquer evento relacionado a segurança da informação que venha a ocorrer.

§3. *Tratamento de Incidentes:* Deverá ser mantida uma equipe de para tratamento de e resposta a incidentes de tecnologia da informação onde será responsável por receber, filtrar, classificar e responder as solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa, bem como a identificação de tendências.

§4. *Gestão de Continuidade*: O Plano de Continuidade de Negócio (PCN) tem como objetivo manter em funcionamento os serviços e processos críticos ao IFPB na possibilidade da ocorrência de desastres naturais, falhas de equipamentos, furto, roubo, falhas humanas e qualquer outro tipo de eventualidade que venha a ocorrer. O PCN será definido pelo Comitê Gestor de Segurança da Informação com base na análise de riscos e terá a aprovação do Comitê Gestor de Tecnologia da Informação.

§5. *Auditoria e Conformidade*: Todo e qualquer usuário estará sujeito à auditoria em sua utilização dos recursos (RTIC). Os procedimentos de auditoria e de monitoramento de uso dos recursos (RTIC) serão realizados periodicamente pela DTI ou área responsável pela T.I., com o objetivo de observar o cumprimento das políticas pelos usuários e com vistas à gestão de desempenho e segurança. Havendo evidência de atividade que possa comprometer o desempenho e/ou a segurança dos recursos ou que infrinja a POSIC ou normas complementares, será permitido à DTI ou área responsável pela T.I., auditar e monitorar atividades de usuários, inspecionar arquivos e registros de acesso, podendo restringir o acesso à fonte causadora do problema, remover dados, desativar servidores e implementar filtros, devendo o fato ser imediatamente comunicado à chefia imediata do

usuário, à direção geral do campus e/ou a Reitoria do IFPB dependendo da gravidade. Deverá ser mantido um canal de comunicação pela Ouvidoria do IFPB para receber denuncias de infração a qualquer parte desta política de segurança. Deverão ser levantados regularmente os aspectos legais de segurança aos quais as atividades da Instituição estão submetidas, de forma a evitar responsabilizações decorrentes da não observância de tais aspectos por desconhecimento ou omissão.

§6. *Controle de Acesso e utilização dos recursos*: Todos os usuários do IFPB têm o direito ao uso dos recursos de tecnologia da informação e comunicação (RTIC) de acordo com as diretrizes de seu perfil, definidas por meio de requisitos técnicos ou por determinação específica da Reitoria ou dos órgãos da administração superior dos campi. Ainda, deverão ser observado alguns ítens:

I - O acesso aos serviços de rede do IFPB que necessitem de autenticação só será permitido a usuários cadastrados.

II - O acesso aos recursos (RTIC) será feito por controles físicos ou lógicos, com objetivo de proteger equipamentos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada.

III - Quando da utilização de nome de usuário e senha, estes serão definidos no momento de ingresso no IFPB. Todos os usuários deverão por meio de um termo de responsabilidade específico assumir o compromisso de:

a) declarar o conhecimento e aceitação dos termos desta política de segurança e de suas políticas e normas complementares, não podendo a qualquer tempo alegar desconhecimento ou ignorância;

b) declarar estar ciente que os acessos realizados à Internet, assim como conteúdo das mensagens de correio eletrônico institucional são passíveis de auditoria; e

c) manter a confidencialidade de sua senha, alterando-a sempre que existir qualquer indício de possível comprometimento, em intervalos regulares de tempo ou com base no número de acessos, a critério da área responsável pela T.I..

§7. *Correio Eletrônico*: O correio eletrônico é um serviço oferecido pelo IFPB como um recurso profissional para apoiar os usuários cadastrados no cumprimento dos objetivos institucionais e são passíveis de auditoria. Deverá ser garantido o sigilo, confidencialidade, o não-repúdio, a autenticidade, a disponibilidade geral do serviço e, os usuários que o utilizarem, deverão assegurar que o endereçamento da mensagem esteja correto. Seu uso é exclusivo para fins Institucionais.

§8. *Correio Eletrônico*: O correio eletrônico é um serviço oferecido pelo IFPB como um recurso profissional para apoiar os usuários cadastrados no cumprimento dos objetivos institucionais e são passíveis de auditoria. Deverá ser garantido o sigilo, confidencialidade, o não-repúdio, a autenticidade, a disponibilidade geral do serviço e, os usuários que o utilizarem, deverão assegurar que o endereçamento da mensagem esteja correto. Seu uso é exclusivo para fins Institucionais.

§9. *Publicação e Acesso à Internet*: Todos os usuários têm o direito de acesso à internet, conforme as permissões de acesso estipuladas nas normas de segurança da instituição. Esse acesso deverá ser feito exclusivamente para fins diretos e complementares às atividades da instituição, para o enriquecimento intelectual de seus servidores ou como ferramenta para busca por informações que venham contribuir para o desenvolvimento de suas atividades laborais. Toda informação publicada no portal do IFPB será de responsabilidade do usuário que realizou a publicação.

§10. *Patrimonio Intelectual*: Informações, sistemas, sites, metodologias e outros assuntos afins, criados pelos servidores, alunos e colaboradores da Instituição, no exercício de suas funções, são patrimônios intelectuais da Instituição, não cabendo a seus criadores qualquer forma de direito autoral, ressalvado o disposto na lei 10.973/ 2004.

§11. *Capacitação e Aperfeiçoamento*: Os servidores deverão ser continuamente capacitados para o desenvolvimento de competências em Segurança da Informação e Comunicação.

CAPÍTULO IX
DAS PENALIDADES

Art. 9º. Em caso de descumprimento desta política de segurança e comunicações serão aplicadas as sanções e penalidades previstas na legislação em vigor, em especial o que consta:

§1. Lei nº 8112/1990, que dispõe sobre o regime jurídico dos servidores civis da União, das autarquias e das fundações públicas federais;

§2. Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto nº 1.171/1994;

§3. Código Penal, através do Decreto-Lei nº 2848/1940;

§4. Lei 8159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências;

§5. Decreto nº 7.845 que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Art. 10º. Um termo de responsabilidade para uso de RTIC deverá ser assinado para todo e qualquer usuário em potencial do IFPB. Este termo poderá assumir a forma eletrônica através dos sistemas internos ou nos meios de autenticação.

CAPÍTULO X
DA ESTRUTURA NORMATIVA DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 11º. A estrutura normativa da Segurança da Informação e Comunicação será composta por um conjunto de documentos distribuídos em três níveis hierárquicos diferentes, descritos a seguir:

§1. *Política de Segurança da Informação e Comunicação (POSIC)*: constituída por este documento, define as diretrizes básicas, globais, referentes à Segurança da Informação, e será detalhada em conjunto de Normas específicas;

§2. *Normas da Segurança da Informação (Normas)*: estabelecem as obrigações, no plano tático, as escolhas tecnológicas e os controles que deverão ser implantados para alcançar o cenário definido estrategicamente nas diretrizes da política.

§3. *Procedimentos de Segurança da Informação (Procedimentos)*: Serão elaboradas pelo Comitê Gestor Segurança da Informação e Comunicação e definem o que foi estabelecido nas normas e na política permitindo sua direta aplicação nas atividades do IFPB.

CAPÍTULO X
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 12º. Estrutura para gestão de SIC: Para a gestão de Tecnologia da Informação e Comunicação será estrutura da seguinte forma:

§1. *Conselho Superior*: Ao Conselho Superior compete aprovar esta política, normas e procedimentos;

§2. *Comitê Gestor de Tecnologia da Informação*: Ao Comitê Gestor de Tecnologia da Informação compete apreciar e recomendar a política, normas e procedimentos à apreciação do Conselho Superior;

§3. *Comitê de Segurança da Informação e Comunicação*: compete a este comitê:

I - Promover a cultura de Segurança da Informação e Comunicação;
II - Coordenar a elaboração e/ou revisão da Política de Segurança da Informação e Comunicação (POSIC), normas e procedimentos relacionados;
III - Acompanhar as investigações e avaliações dos dados decorrentes de quebras de segurança;
IV - Propor recursos necessários às ações de segurança da informação e comunicação;
V - Instituir a Equipe de Tratamento e Respostas a Incidentes de Segurança da Informação;
VI - Acompanhar estudo de novas tecnologias, no que diz respeito a possíveis impactos sobre Segurança da Informação;
VII - Promover intercâmbio científico-tecnológico entre órgãos e as entidades da Administração Pública Federal e as Instituições Públicas e Privadas sobre as atividades de Segurança da Informação e Comunicação (Art 3º. do Decreto 3.505 de 2000); e

VIII - Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional; e

IX - Auditar e monitorar atividades dos usuários, inspecionar arquivos e registros de acesso, podendo restringir o acesso à fonte causadora do problema, desativar servidores e implementar filtros, devendo o fato ser imediatamente comunicado à chefia imediata do usuário.

CAPÍTULO XI
DA ATUALIZAÇÃO

Art. 13º. Todos os instrumentos normativos gerados a partir da POSIC/IFPB, incluindo a própria POSIC/IFPB, devem ser revisados sempre que se fizer necessário. Será apresentado um relatório anual com um estudo das necessidades de mudança para esta Política.

CAPÍTULO XI
DAS DISPOSIÇÕES FINAIS

Art. 14º. Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Segurança da Informação e Comunicações do IFPB, devem ser direcionados ao Comitê Gestor de Segurança da Informação, com a interveniência do Comitê Gestor de Tecnologia da Informação.