POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ
POSIC

Julho/2012

ORIGEM

Diretoria de Tecnologia da Informação

REFERÊNCIAS

ABNT NBR ISO/IEC 27002:2005 - Tecnologia da Informação - Técnicas de Segurança - Código de Prática para a Gestão de Segurança da Informação.

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.

Constituição da República Federativa do Brasil de 1988.

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

Instrução Normativa GSI Nº 01, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta e demais normas complementares.

Instrução Normativa DSIC-GSIPR nº 02, de 13 de outubro 2008, que disciplina a Metodologia de Gestão de Segurança da Informação e Comunicações.

Instrução Normativa DSIC-GSIPR nº 03, de 30 Junho 2009, que disciplina a Diretrizes para Elaboração De Política De Segurança Da Informação E Comunicações Nos Órgãos E Entidades Da Administração Pública Federal.

Instrução Normativa DSIC-GSIPR nº05 , de 14 agosto 2009, que disciplina a Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR.

Instrução Normativa DSIC-GSIPR nº 06, de 11 novembro 2009, que disciplina a Gestão de Continuidade de Negócios em segurança da Informação e Comunicações.

Resolução CUNI Nº 054, de 5 de julho de 2011, que dispõe sobre a Política de Segurança da Informação e Comunicações da Universidade Federal de Lavras.

Resolução Nº 18, de 31 de maio de 2010, que normatiza o uso dos recursos de tecnologia da informação e comunicação do IFRO .

Política de Segurança da Informação – IFPE - Campus Caruaru, de 31 de março de 2011.

Política de Segurança da Informação – IFPB .

CAMPO DE APLICAÇÃO

Esta Política de Segurança da Informação se aplica no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Amapá (IFAP).

APROVAÇÃO

Anderson Brasiliense de Oliveira Brito

Presidente do Comitê Gestor de Tecnologia da Informação

1. OBJETIVO

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 do Amapá (IFAP), buscando assegurar a disponibilidade, integridade e confidencialidade das informações.

2. FUNDAMENTO LEGAL DA POLÍTICA DE SEGURANÇA

Conforme o 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.

3. CONCEITOS E DEFINIÇÕES

3.1 Comitê Gestor de Tecnologia da Informação (CGTI): comitê responsável por apreciar e aprovar o Plano Estratégico de Tecnologia da Informação (PETI), o Plano Diretor de Tecnologia da Informação (PDTI) e a Política de Segurança da Informação e Comunicações (POSIC) e demais normas 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 area;

3.2 Comitê Gestor de Segurança da Informação (CGSI): comitê responsável por elaborar e revisar periodicamente a Política de Segurança da Informação e Comunicações (POSIC) e normas relacionadas, submetendo à aprovação do Comitê Gestor de Tecnologia da Informação, entre outras competências;

3.3 Diretoria de Tecnologia da Informação (DTI): órgão executivo da Reitoria, 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;

3.4 **Unidade de Ensino (UE)**: os campi, campi avançados, pólos, pólos de apoio presencial à Educação a Distância (EaD) e outras estruturas administrativas com atividades pedagógicas que demandem o uso das tecnologias da informação e comunicação;

3.5 Recursos de Tecnologia da Informação e Comunicação (RTIC): os equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados nas Unidades de Ensino, tais como:

3.5.1. equipamentos de informática e de telecomunicações de qualquer espécie;

3.5.2. infraestrutura e materiais de redes lógicas e de telecomunicações de qualquer espécie;

3.5.3. laboratórios de informática de qualquer espécie; e

3.5.4. 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 IFAP, redes ou outros sistemas de informação.

3.6 **Sistemas de informação**: os sistemas de controle, organização e planejamento acadêmicos e administrativos, bem como seus conteúdos hospedados e/ou armazenados em máquinas servidoras de responsabilidade da DTI ou NTI/CTI ou em máquinas locais com cópias de segurança em máquinas servidoras de responsabilidade da DTI ou dos núcleos de tecnologia locais. São partes integrantes do sistema de informação os componentes clientes instalados nas máquinas locais;

3.7 **Serviços de rede**: todos os serviços oferecidos aos usuários por meio da infraestrutura de rede interna e externa, tais como: correio eletrônico, *websites* (páginas individuais e institucionais de conteúdos para a Internet), aplicações *web* (sistemas corporativos acessados via rede), repositórios de arquivos em rede, servidores de bancos de dados individuais e corporativos,

sistemas de autenticação de usuários de rede, serviços de segurança e monitoração, entre outros; bem como seus conteúdos (mensagens de correio eletrônico, dados corporativos, documentos, arquivos de configuração) que são hospedados e armazenados em máquinas servidoras de responsabilidade da DTI ou dos núcleos de tecnologia locais;

3.8 **Usuário**: qualquer pessoa física ou jurídica com vínculo oficial com o IFAP ou em condição autorizada que utiliza, de alguma forma, algum recurso de tecnologia da informação e comunicação (RTIC) do IFAP. Os usuários poderão ser cadastrados ou não no domínio do IFAP e serão classificados, para fins de acesso aos recursos (RTIC), de acordo com os seguintes perfis:

3.8.1. servidores: qualquer servidor, ativo ou aposentado, com vínculo ao IFAP;

3.8.2. alunos;

3.8.3. outros:

3.8.3.1. responsável por entidade externa que utiliza o domínio do IFAP (procuradoria, grupos de pesquisa, e outros afins);

3.8.3.2. entidade representativa de alunos;

3.8.3.3. aluno bolsista;

3.8.3.4. estagiário externo;

3.8.3.5. servidores terceirizados;

3.8.3.6. visitante;

3.8.3.7. pensionista.

3.9 **Núcleo de Tecnologia da Informação (NTI) ou Coordenação de Tecnologia da Informação (CTI)**: setor formalmente instituído em uma Unidade de Ensino do IFAP que ficará responsável pela manutenção local dos recursos (RTIC) e preservação da aplicação das políticas, diretrizes e regulamentações na área de informática e telecomunicações. Os setores locais participarão com a DTI no desenvolvimento e administração de sistemas de informação e serviços de rede para o campus ao qual estão vinculados ou para todo o IFAP;

3.10 **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];

3.11 **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];

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

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

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

3.15 **Segurança da informação**: conjunto de políticas, normas e procedimentos que objetivam o controle de acesso, a preservação da autenticidade, confiabilidade, confidencialidade, disponibilidade, privacidade, integridade dos dados e responsabilidade das informações e dos recursos de TIC;

3.16 **Política de Segurança da Informação e Comunicações (POSIC)**: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações. [IN01/DSIC/GSIPR]

3.17 **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais –**

ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

4. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

A Política de Segurança da Informação e Comunicações do Instituto Federal de Educação, Ciência e Tecnologia do Amapá consiste na normatização e no disciplinamento de mecanismos que promovam a integridade da estrutura de rede e demais recursos de TIC nos quais trafegam informações e dados comuns ou restritos, neles incluídos os equipamentos que armazenam tais informações.

4.1 A Política de Segurança da Informação:

4.1.1. é constituída por um conjunto de diretrizes e normas que estabelecem os princípios de proteção, controle e monitoramento das informações processadas, armazenadas ou custodiadas pelo IFAP.

4.1.2. é aplicável a todos os bens e serviços e a todo o pessoal que se utiliza dos recursos de Tecnologia da Informação e Comunicação (TIC), no âmbito do IFAP.

4.2 A Política de Segurança abrange os seguintes aspectos:

4.2.1. Requisitos de Segurança Lógica;

4.2.2. Requisitos de Segurança Física;

4.2.3. Requisitos de Segurança em Recursos Humanos; e

4.2.4. Requisitos de Segurança dos Recursos Criptográficos.

4.3 Os requisitos de segurança, dos itens citados em 4.2 serão regulamentados por meio de normas e procedimentos específicos elaborados pelo Comitê Gestor de Segurança da Informação e avaliados e aprovados pelo Comitê Gestor de Tecnologia da Informação.

5. COMPETÊNCIAS, RESPONSABILIDADES E ESTRUTURA DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

5.1 Ao Comitê Gestor de Tecnologia da Informação compete:

5.1.1. apreciar e aprovar a Política de Segurança da Informação e Comunicações.

5.2 Aos demais gestores compete: Zelar pelo cumprimento das diretrizes da POSIC.

5.3 A todos usuários compete:

5.3.1. conhecer a POSIC e manter níveis de segurança adequados, seguindo as suas diretrizes e normas complementares.

5.3.2. adotar comportamento seguro, assumindo atitude pró-ativa e engajada no que diz respeito à proteção das informações do Instituto.

5.4 Ao Departamento de Recursos Humanos compete: Obter a assinatura do Termo de Responsabilidade e informar à equipe de Tecnologia da Informação sobre mudanças no quadro funcional da Instituição.

5.5 A todos os departamentos: Responsabilidade pela garantia da segurança da informação no âmbito do IFAP, ressalvadas as situações em que:

5.5.1. a informação for retirada do âmbito da rede do IFAP por usuários autorizados;

5.5.2. o usuário autorizado fornecer sua senha de acesso a qualquer outra pessoa;

5.5.3. o acesso à informação for limitado ou indisponibilizado por serviços e estruturas externas ao IFAP ou de responsabilidade de outros órgãos ou empresas;

5.5.4. quando propositadamente ou inadvertidamente o usuário fizer uso inadequado dos

recursos (RTIC), seja por inabilidade, conhecimento insuficiente ou intenção de causar dano à instituição ou a outrem.

5.6 Ao Comitê Gestor de Segurança da Informação compete:

5.6.1. elaborar e revisar periodicamente a Política de Segurança da Informação e Comunicações (POSIC) e normas relacionadas, submetendo a aprovação do Comitê Gestor de Tecnologia da Informação;

5.6.2. propor, acompanhar e divulgar os planos de ação para aplicação da PSI, incluindo a conscientização de usuários;

5.6.3. propor a implantação de soluções para minimização dos riscos; e

5.6.4. elaborar propostas de normas complementares e políticas de uso dos recursos de informação.

5.7 Ao Presidente do Comitê Gestor de Segurança da Informação, no âmbito de suas atribuições, incumbe:

5.7.1. promover cultura e segurança da informação e comunicações;

5.7.2. acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

5.7.3. propor recursos necessários às ações de segurança da informação e comunicações;

5.7.4. coordenar o Comitê Gestor de Segurança da Informação e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR);

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

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

5.7.7. propor normas relativas à segurança da informação e comunicações.

6. DIRETRIZES

6.1 TRATAMENTO DA INFORMAÇÃO

6.1.1. 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.

6.1.2. O descarte de informações sensíveis deverá ser realizado através de trituração, incineração ou remoção dos dados de forma segurança.

6.1.3. Deverão ser realizadas cópias de segurança das informações tomando como base a norma de gerenciamento de cópias de segurança da informação do IFAP.

6.1.3.1. As cópias de segurança das informações citadas em 6.1.3 deverão ser testadas, verificadas e armazenadas, local e remotamente, de tal forma a evitar a perda da informação por alguma eventualidade.

6.2 GESTÃO DE RISCOS E TRATAMENTO DE INCIDENTES

6.2.1. Entende-se como gerenciamento de riscos o processo que visa à proteção dos serviços do IFAP, por meio da eliminação, redução ou transferência dos riscos, conforme seja economicamente (e estrategicamente) mais viável. Os seguintes pontos principais devem ser identificados:

6.2.1.1. o que deve ser protegido;

6.2.1.2. análise de riscos (contra quem ou contra o quê deve ser protegido);

6.2.1.3. avaliação de riscos (análise da relação custo/benefício).

6.2.2. A DTI apresentará 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 DTI e seus núcleos de tecnologia locais.

6.2.3. As normas e procedimentos para implantação e gerenciamento de riscos de Informação serão definidos em documento específico elaborado pelo Comitê Gestor de Segurança da Informação.

6.2.4. O IFAP deverá realizar 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.

6.3 GESTÃO DE CONTINUIDADE

6.3.1. Será orientado pelo Programa de Gestão da Continuidade de Negócios sendo este um processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio análises críticas, testes, treinamentos e manutenção. Em sua composição constarão o Plano de Gerenciamento de Incidentes - PGI, Plano de Continuidade de Negócios - PCN e o Plano de Recuperação de Negócios – PRN.

6.3.2. O Plano de Gerenciamento de Incidentes (PGI) é o plano de ação ser usado quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

6.3.3. O Plano de Continuidade de Negócio (PCN) tem como objetivo manter em funcionamento os serviços e processos críticos do IFAP na possibilidade da ocorrência de desastres naturais, falhas de equipamentos, furto, roubo, falhas humanas e qualquer outro tipo de eventualidade que venha a ocorrer.

6.3.4. Plano de Recuperação de Negócios (PRN) é a documentação dos procedimentos e informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas a normalidade;

6.3.5. O PGI, PCN e PRN do IFAP serão 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.

6.4 AUDITORIA E CONFORMIDADE

6.4.1. Todos os usuários estão sujeitos à auditoria em sua utilização dos recursos (RTIC).

6.4.2. Os procedimentos de auditoria e de monitoramento de uso dos recursos (RTIC) serão realizados periodicamente pela DTI ou NTI/CTI, com o objetivo de observar o cumprimento das políticas pelos usuários e com vistas à gestão de desempenho e segurança.

6.4.3. Havendo evidência de atividade que possa comprometer o desempenho e/ou a segurança dos recursos ou que infrinja a POSIC e normas complementares, será permitido à DTI ou NTI/CTI 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 IFAP dependendo da

gravidade. Sendo considerada gravidade baixa a atividade que comprometa apenas a máquina do usuário, gravidade média a atividade que comprometa o desempenho da rede e gravidade alta aquela que comprometa a segurança e disponibilidade dos serviços.

6.4.4. Será mantido pela Ouvidoria do IFAP canal de comunicação para receber denúncias de infração a qualquer parte desta política de segurança.

6.5 CONTROLE DE ACESSO E UTILIZAÇÃO DOS RECURSOS

6.5.1. Todos os usuários do IFAP têm o direito ao uso dos recursos (RTIC) do IFAP 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.

6.5.2. O acesso aos serviços de rede do IFAP que necessitam autenticação só será permitido a usuários cadastrados.

6.5.3. 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. Quando da utilização de nome de usuário e senha, estes serão definidos no momento de ingresso no IFAP.

6.5.4. Todos os usuários deverão por meio de um termo de responsabilidade específico assumir o compromisso de:

6.5.4.1. 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;

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

6.5.4.3. manter a confidencialidade de sua senha, alterando a mesma sempre que existir qualquer indício de possível comprometimento, em intervalos regulares de tempo ou com base no número de acessos, a critério da DTI.

6.5.5. Todos os usuários e qualquer outra pessoa que entre na instituição deverão possuir algum tipo de identificação visível e ter seu acesso registrado, onde possa ser visualizada a data e hora de sua entrada e saída.

6.5.6. Qualquer tipo de informação referente a conteúdos que dizem respeito à instituição deverão ser guardados em lugar seguro como, por exemplo, cofres, armários e mobílias que possuam algum tipo de fechadura quando não estiverem em uso.

6.5.7. Qualquer tipo de equipamento de armazenagem e processamento de informação com tombamento (Ex.: estações de trabalho, notebooks, celulares) só poderão ser utilizados fora das dependências do instituto ou do departamento de sua responsabilidade com autorização prévia e protegido de forma adequada contra furto, roubo ou perda da informação.

6.5.8. É de total responsabilidade do usuário a proteção das informações institucionais que estejam sob sua responsabilidade, utilizadas no âmbito do instituto ou fora de suas dependências.

6.5.9. O gerenciamento de informações, documentos e materiais sigilosos do IFAP deverão estar em conformidade com a Lei nº 8.159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências e com o Decreto nº 4.553/2002, 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.

6.6 CORREIO ELETRÔNICO

6.6.1. Os serviços de correio eletrônico hospedados em máquinas servidoras do IFAP

são oferecidos como um recurso profissional para apoiar os usuários cadastrados do IFAP no cumprimento dos objetivos institucionais e são passíveis de auditoria.

6.6.2. Os serviços de correio eletrônico citados em 6.6, deverão garantir o sigilo, a 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.

6.7 PUBLICAÇÃO E ACESSO À INTERNET

6.7.1. Todos os servidores 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 seus trabalhos.

6.7.2. Toda informação publicada no portal do IFAP será de responsabilidade do usuário que realizou a publicação.

7. PENALIDADES

A quem descumprir esta política de segurança, as normas e procedimentos estabelecidos pelo IFAP serão aplicadas as sanções e penalidades previstas na legislação em vigor, em especial o que consta:

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

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

7.3 no Código Penal, através do Decreto-Lei nº 2848/1940;

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

7.5 no Decreto nº 4553/2002, 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.

8. DISPOSIÇÕES GERAIS

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

9. ATUALIZAÇÃO

Todos os instrumentos normativos gerados a partir da POSIC, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 01 (um) ano.