RESOLUÇÃO Nº 105-CONSELHO SUPERIOR, de 29 de outubro de 2012.

APROVA A REFORMULAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES – POSIC DO IFRR.

O PRESIDENTE DO CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RORAIMA, no uso de suas atribuições legais e

CONSIDERANDO o Parecer nº 36/2012 do Conselheiro Relator e a decisão do colegiado tomada em sessão plenária realizada em 21 de setembro de 2012,

RESOLVE:

Aprovar a Reformulação da Política de Segurança da Informação e Comunicações – POSIC do Instituto Federal de Roraima, conforme anexo.

Dê-se ciência, publique-se e cumpra-se.

Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia de Roraima, em Boa Vista – RR, 29 de outubro de 2012.

ADEMAR DE ARAÚJO FILHO
Presidente

ANEXO DA RESOLUÇÃO Nº 105-CONSELHO SUPERIOR, de 29 de outubro de 2012.

REFORMULAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES – POSIC DO IFRR

1 OBJETIVO

Fornecer diretrizes, responsabilidades, competências e apoio da alta direção na implementação da gestão de segurança da informação e comunicações no Instituto Federal de Educação, Ciência e Tecnologia de Roraima (IFRR), buscando assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis.

2 FUNDAMENTAÇÃO LEGAL

2.1DECRETO 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.

2.2INSTRUÇÃO NORMATIVA GSI/PR NO 1, DE 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.

2.3LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011, Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

2.4DECRETO Nº 7.724, DE 16 DE MAIO DE 2012, Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.

2.5ABNT NBR ISO/IEC 27001:2006, Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gerência da Segurança da Informação – Requisitos.

2.6ABNT NBR ISO/IEC 27002:2005, Código de Prática para a Gestão de Segurança da Informação.

3 CONCEITOS E DEFINIÇÕES

3.1Comitê Gestor de Tecnologia da Informação (CGTI): instância autônoma que atende ao disposto na Instrução Normativa nº 04/SLTI/MPOG de 19/05/2008 em seu Art. 4º Inciso IV, possui natureza consultiva e deliberativa e é responsável pelo alinhamento e regulação das ações de TIC ao disposto no Plano de Desenvolvimento Institucional (PDI) e no Plano Estratégico de Tecnologia da Informação (PETI).

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

3.3Diretoria de Tecnologia da Informação (DTI): instância administrativa/executiva responsável pelo desenvolvimento, implantação e manutenção dos recursos e serviços de tecnologia da informação e comunicações no âmbito do IFRR e por propor as políticas e programas do Instituto na área de informática e telecomunicações, bem como por sua implementação e gestão.

3.4Coordenação de Tecnologia da Informação (CTI) de um câmpus: instância que tem como atribuição principal o gerenciamento da rede local, bem como dos recursos de TIC do campus a ela conectados, direta ou indiretamente.

3.5Unidade: qualquer instância administrativa do IFRR a exemplo dos câmpus, unidades ligadas aos campi, núcleos de pesquisa e centros com funcionalidades específicas.

3.6Política 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;

3.7Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

3.8Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

3.9Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

3.10 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;

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

3.12 **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

3.13 **Informação**: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

3.14 **Dados processados**: dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;

3.15 **Tratamento da informação**: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

3.16 **Controle**: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. Controle também é usado como sinônimo para proteção ou contramedida.

3.17 **Risco**: combinação da probabilidade de ocorrência de um evento e de suas consequências;

3.18 **Gestão de riscos**: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para mitigar os riscos a que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos. A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos;

3.19 **Análise de riscos**: uso sistemático de informações para identificar fontes e estimar o risco;

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

3.21 **Análise/avaliação de riscos**: processo completo de análise e avaliação de riscos;

3.22 **Tratamento do risco**: processo de seleção e implementação de medidas para modificar um risco;

3.23 **Aceitação do risco**: decisão de aceitar a probabilidade de ocorrência de eventos ou incidentes de segurança e suas consequências;

3.24 **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 pra a segurança da informação [ISO/IEC TR 18044:2004];

3.25 **Incidente de segurança da informação**: um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou

inesperados, que tenham uma grande probabilidade de comprometer as operações de negócio e ameaçar a segurança da informação [ISO/IEC TR 18044:2004];

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

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

3.28 **Ativo**: qualquer bem, tangível ou intangível, que tenha valor para a Instituição. Neles incluem-se:

a) ativos de informação;

b) ativos de software;

c) ativos físicos;

d) serviços;

e) pessoas e suas qualificações, habilidades e experiências;

f) reputação e a imagem da instituição.

3.29 **Ativos de informação**: base de dados e arquivos, contratos e acordos, documentação de sistemas, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e quaisquer informações armazenadas em meio físico ou digital.

3.30 **Ativos de software**: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários.

3.31 **Ativos físicos**: equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos.

3.32 **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:

a) equipamentos de informática e de telecomunicações de qualquer espécie;

b) infraestrutura e materiais de redes lógicas e de telecomunicações de qualquer espécie;

c) laboratórios de informática de qualquer espécie; e

d) 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 IFRR, redes ou outros sistemas de informação.

4 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

A Política de Segurança da Informação e Comunicações do Instituto Federal de Educação, Ciência e Tecnologia de Roraima é uma declaração formal da Instituição 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 IFRR ou quem quer que tenha acesso estas informações, aos recursos de processamento delas ou aos locais onde elas são tratadas e/ou armazenadas.

A POSIC é constituída por um conjunto documentos que definem a estrutura, diretrizes, obrigações e procedimentos referentes à segurança da informação e estabelecem orientações quanto à sua implementação. Seu objetivo é estabelecer políticas para o tratamento, controle e recuperação das informações em razão da ocorrência de eventos ou incidentes de segurança, a proteção dos ativos e a definição dos papéis e responsabilidades de cada uma das partes envolvidas na gestão da segurança da informação. Desta forma, ela deve contar com o apoio ativo da alta administração dentro da organização, por meio de um claro direcionamento, demonstrando seu comprometimento, definindo atribuições de forma explícita e reconhecendo suas responsabilidades pela segurança da informação.

5 PRINCÍPIOS

Além dos princípios de confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio, a POSIC do IFRR é regida também pelos seguintes princípios:

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

b) 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 IFRR são responsáveis pelo tratamento da informação e pelo cumprimento das Normas de Segurança da Informação e Comunicações advindas desta política.

c) Ciência: Todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço devem ter ciência das normas, procedimentos, orientações e outras informações que permitam a execução de suas atribuições sem comprometer a segurança.

d) Ética: Todos os direitos e interesses legítimos de servidores, colaboradores, estagiários, prestadores de serviço e usuários do sistema de Informação do IFRR devem ser respeitados.

e) Legalidade: Além de observar os interesses do IFRR, as ações de Segurança da Informação e Comunicações 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.

f) Proporcionalidade: O nível, a complexidade e os custos das ações de Segurança da Informação e Comunicações no IFRR serão adequados ao entendimento administrativo e ao valor do ativo a proteger.

6 ESTRUTURA DA POSIC

A POSIC do IFRR é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

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

b) Normas de Segurança da Informação e Comunicações: estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas instâncias em que a informação é tratada. A cada Norma será associado um conjunto de Procedimentos destinados a orientar sua implementação. A elaboração das Normas seguirá as orientações contidas em um documento do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República intitulado Atividade de Normatização.

c) Procedimentos de Segurança da Informação e Comunicações: instrumentalizam o disposto nas Normas, permitindo a direta aplicação nas atividades do IFRR, cabendo a cada gestor a responsabilidade de gerá-los. Cada procedimento poderá ainda ser detalhado em instruções. Estes procedimentos e instruções são de uso interno, não sendo obrigatória a sua publicação.

7 ESCOPO

A Política de Segurança da Informação e Comunicações do IFRR abrange os seguintes aspectos:

a) Requisitos de Segurança Lógica;

b) Requisitos de Segurança Física;

c) Requisitos de Segurança em Recursos Humanos; e

d) Requisitos de Segurança dos Recursos Criptográficos.

Os requisitos de segurança abrangidos por esta Política serão regulamentados por meio de normas e procedimentos específicos elaborados pelo Comitê Gestor de Segurança da Informação e Comunicação e avaliados e aprovados pelo Conselho Superior.

8 COMPETÊNCIAS E RESPONSABILIDADES

8.1 Ao Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia de Roraima compete:

a) Apreciar e aprovar a Política de Segurança da Informação e Comunicações e suas Normas Complementares.

8.2 Aos gestores compete:

a) Zelar pelo cumprimento das diretrizes da POSIC;

b) Designar responsáveis pela manutenção de ativos;

c) Elaborar e/ou aprovar procedimentos referentes aos ativos.

8.3A todos usuários compete:

a) Conhecer a POSIC e manter níveis de segurança adequados, seguindo as suas diretrizes e normas complementares.;

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

8.4 Aos setores de Gestão de Pessoas de cada unidade compete:

a) Dar ciência a todos os Servidores do Instituto Federal de Roraima e aos novos contratados sobre a Política de Segurança da Informação e Comunicações do Instituto Federal de Roraima – IFRR, colhendo a assinatura do respectivo termo;

b) Informar à equipe de Tecnologia da Informação da sua unidade sobre mudanças no quadro funcional da Instituição que possam alterar os perfis de acesso dos usuários aos recursos de TI.

8.5 Ao Comitê Gestor de Tecnologia da Informação compete:

a) Estabelecer diretrizes para implementação de Recursos de Tecnologia da Informação e Comunicação no âmbito do IFRR, de modo a padronizar as ações referentes à segurança da informação dos recursos (RTIC).

8.6 Ao Comitê Gestor de Segurança da Informação e Comunicação compete, além das atribuições definidas na Portaria 391 de 27 de março de 2012:

a) Elaborar e revisar periodicamente a Política de Segurança da Informação e Comunicações (POSIC) e normas relacionadas, submetendo-as a aprovação do Conselho Superior;

b) propor, acompanhar e divulgar planos de ação para aplicação da POSIC, incluindo a conscientização de usuários;

c) Propor a implantação de soluções para minimização dos riscos; e

d) Apreciar propostas de normas complementares e políticas de uso dos recursos de informação.

9 DIRETRIZES GERAIS

9.1É política do IFRR prover para a sua comunidade o acesso a fontes de informação locais, nacionais e internacionais, promovendo um ambiente de produção, uso e compartilhamento do conhecimento e de comprometimento com a liberdade acadêmica.

9.2 Zelar pela Segurança da Informação e Comunicações é dever de todos.

9.3O IFRR, como usuário dos serviços providos pela Rede Nacional de Pesquisa (RNP) é, por princípio, signatário de suas Políticas e Normas de Segurança.

9.4 Cabe a toda a comunidade envolvida com a geração, uso e tratamento da informação propor normas de segurança da informação e comunicações, que deverão ser submetidas à apreciação do Comitê Gestor de Segurança da Informação e Comunicação.

9.5O padrão para apresentação de normas de segurança da informação e comunicações será definido em Norma Complementar elaborada pelo CGSICC e deverá ser seguida por todos os responsáveis pela preservação das informações e recursos de comunicação no âmbito do IFRR.

10 DIRETRIZES PARA O TRATAMENTO DE ATIVOS

10.1 Todos os ativos deverão ser inventariados, classificados, documentados e sua documentação mantida atualizada, devendo ser revista mensalmente ou sempre que ocorrerem fatos que justifiquem sua atualização.

10.2 A documentação dos ativos deverá conter informações que permitam sua recuperação após um desastre, incluído o tipo de ativo, formato, localização, informações sobre cópias de segurança e informações sobre a importância do ativo para a instituição.

10.3 Os ativos de um setor deverão ser de responsabilidade do gestor ou alguém por ele designado, que ficará encarregado da manutenção do ativo, incluindo sua documentação, e de notificar qualquer evento que aconteça a ele.

10.4 A designação do responsável deverá constar de termo de responsabilidade assinado pelo gestor, definindo os cuidados e obrigações que o responsável deverá ter com o ativo, e assinado pelo responsável dando ciência de suas atribuições.

10.5 A Instituição adotará as medidas necessárias para que os responsáveis pelos ativos possam geri-los adequadamente.

11 ATIVOS DE INFORMAÇÃO

11.1 O responsável designado para guardar determinado ativo de informação deverá elaborar os procedimentos necessários ao seu tratamento, devendo seguir os requisitos de segurança adotados por esta política além de outras normas em vigor no âmbito da administração pública federal.

11.2 Qualquer ativo 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.

11.3 Os ativos de informação armazenados em serviços ou sistemas mantidos em equipamentos destinados exclusivamente para este fim (servidores de rede), que estejam sob a guarda da Diretoria de Tecnologia da Informação ou das Coordenações de Tecnologia da Informação dos Câmpus são de responsabilidade desta(s) Diretoria/Coordenações, cabendo a elas adotar todas as medidas necessárias para realizar as cópias de segurança destes ativos e proceder sua recuperação em caso de desastres.

11.4 Os ativos de informação armazenados nos equipamentos utilizados pelos usuários (computadores de mesa, notebooks, tablets, smartphones, HDs externos, pendrives, etc.) são de responsabilidade do usuário, cabendo a ele adotar todas as medidas necessárias para realizar as cópias de segurança destes ativos e proceder sua recuperação em caso de desastres.

11.5 A DTI ou as CTIs não se responsabilizam por ativos de informação armazenados fora de sistemas ou serviços mantidos por elas.

11.6 Norma complementar estabelecerá diretrizes para a criação, manutenção e teste das cópias de segurança dos ativos de informação.

12 ATIVOS DE SOFTWARE

12.1 A gestão dos ativos de software homologados pela Diretoria de Tecnologia da Informação ou pelas Coordenações de Tecnologia da Informação dos Câmpus são de responsabilidade

desta(s) Diretoria/Coordenações, cabendo a elas adotar todos os procedimentos necessários à sua implementação, desenvolvimento, instalação, suporte, treinamento, manutenção, remoção, gestão de licenças e realização de cópias de segurança junto a Instituição.

12.2 Os ativos de software não homologados pela DTI ou pelas CTIs dos Câmpus não são de responsabilidade destes, não cabendo à(s) Diretoria/Coordenações a gestão de tais ativos.

13 ATIVOS FÍSICOS

13.1 A gestão dos ativos físicos é de competência de cada gestor nas suas respectivas unidades, mediante assinatura do Termo de Responsabilidade emitido pela Coordenação de Patrimônio de cada Câmpus e Reitoria do Instituto Federal de Roraima – IFRR.

13.2 Não cabe ao responsável pelo ativo físico alterar a localização do ativo ou transferir sua responsabilidade a outros, devendo ser acionado o setor de patrimônio de cada unidade para que tome as medidas cabíveis.

13.3 A utilização de equipamento de armazenagem e processamento de informação com tombamento (Ex.: computadores de mesa, 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, obedecendo os controles estabelecidos pelo setor de patrimônio das unidades.

13.4 A retirada de um ativo físico de sua localização, quando não estiverem dentro da situação prevista no item 13.3, poderá ser efetuada apenas para realização de manutenções, devendo o ativo retornar para o seu local de origem após o termino do serviço. O setor de patrimônio deverá ser comunicado da saída e do retorno do ativo.

13.5 Antes da retirada de um ativo, o responsável deverá cuidar para que as informações críticas contidas nele não seja acessada por pessoas não autorizadas, devendo estas informações serem guardadas em local seguro até o retorno do ativo.

14 SERVIÇOS

14.1 Os serviços oferecidos pela Instituição também constituem ativos passíveis de inventário e documentação, devendo cada gestor designar um responsável pela execução destas tarefas.

14.2 A documentação dos serviços deverá incluir requisitos e procedimentos detalhados para sua execução, devendo constar ainda de orientações para a execução do serviço ou sua restauração em

caso de desastres. Esta documentação deverá ser revista semestralmente ou sempre que ocorrerem fatos que justifiquem sua revisão.

15 DIRETRIZES PARA GESTÃO DE RISCO E TRATAMENTO DE INCIDENTES

15.1 A gestão de riscos deverá constar planos de gerenciamento de riscos e da ação de resposta a incidentes, a serem aprovados pelo Comitê Gestor de Segurança da Informação e Comunicação. Os seguintes pontos principais devem ser identificados:

a) O que deve ser protegido;

b) Análise de riscos (contra quem ou contra o quê deve ser protegido);

c) Avaliação de riscos (análise da relação custo/benefício).

15.2 O Comitê Gestor de Segurança da Informação e Comunicação elaborará normas e procedimentos para implantação e gerenciamento de riscos de Informação.

15.3 O IFRR 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.

16 GESTÃO DE CONTINUIDADE

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

16.2 O PCN do IFRR será definido pelo Comitê Gestor de Segurança da Informação e Comunicação com base na análise de riscos e terá a aprovação do Conselho Superior.

17 AUDITORIA E CONFORMIDADE

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

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

17.3 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 CTIs 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 IFRR dependendo da gravidade.

a) São consideradas atividades de gravidade:

- baixa: aquela que comprometa apenas a máquina do usuário;
- média: que comprometa o desempenho da rede;
- alta: aquela que comprometa a segurança e disponibilidade dos serviços.

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

18 CONTROLE DE ACESSO

18.1 Todos os usuários do IFRR têm o direito ao uso dos recursos (RTIC) do IFRR 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 câmpus.

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

18.3 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 IFRR, devendo ser bloqueados em períodos em que o servidor estiver em inatividade ou cancelados quando da exoneração definitiva do servidor.

18.4 Os procedimentos para cadastro de usuários para acesso aos serviços de rede do IFRR serão definidos pela DTI através da elaboração de procedimentos, que deverão ser seguidos em todas as unidades do IFRR.

18.5 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 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.

18.6 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.

18.7 As diretrizes para a entrada de pessoas na instituição será definida em norma complementar elaborada pelo CGSICC.

18.8 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.

19 CORREIO ELETRÔNICO

19.1 O serviço de correio eletrônico disponibilizado pelo IFRR constitui recurso do Instituto disponibilizado na rede de Comunicação de dados para aumentar a agilidade, segurança e economia da Comunicação oficial e informal. O correio eletrônico constitui bem do IFRR e, portanto, é passível de auditoria.

19.2 O CGSICC elaborará normas que disciplinarão o uso do correio eletrônico no âmbito do IFRR.

20 PUBLICAÇÃO E ACESSO À INTERNET

20.1 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.

20.2 Além do portal do IFRR, com informações que dizem respeito à comunidade interna e externa do Instituto, cada unidade do IFRR terá um portal próprio para publicação de notícias que dizem respeito à unidade.

20.3 A utilização dos portais de notícias será disciplinada por normas complementares.

21 PENALIDADES

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

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

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

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

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

e) 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.

f) LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011, Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências.

22 DISPOSIÇÕES GERAIS

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

22.2 Estando em vigência esta política, fica invalidada a Política de Segurança da Estrutura de Informática do Centro Federal de Educação Tecnológica de Roraima (CEFET-RR), cabendo ao CGSIC normatizar os itens que nela são tratados, que não foram abrangidos por esta política.

23 ATUALIZAÇÃO

23.1 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.

24 VIGÊNCIA

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

24.2 Nos seis primeiros meses de vigência da política deverão serão desenvolvidas ações conforme item 8.6, letra b) para que os usuários tomem conhecimento da política e possam se adequar a ela.

Boa vista-RR, 29 de outubro de 2012

ADEMAR DE ARAÚJO FILHO
Reitor do IFRR