MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RORAIMA
REITORIA
Conselho Superior
Rua Fernão Dias Paes Leme, 11, Calungá, Boa Vista - RR, CEP 69303220 , gabinete.reitoria@ifrr.edu.br
www.ifrr.edu.br

Resolução CONSUP/IFRR N° 790, de 6 de maio de 2024.

Dispõe sobre o Política de Segurança da Informação e Comunicação do Instituto Federal de Roraima.

A Presidente do Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia de Roraima, no uso de suas atribuições legais, tendo em vista a autonomia institucional conferida pelo Art. 1º da Lei nº 11.892, de 29 de dezembro de 2008, considerando 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, a Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, bem como , a Instrução Normativa nº 3, de 28 de maio de 2021 do Gabinete de Segurança Institucional da Presidência da República e a Portaria SGD/MGI Nº 852, de 28 de março de 2023, considerando o constante no processo 23231.000130.2024-18 e a decisão do colegiado tomada na 91ª sessão plenária, realizada em 1º de abril de 2024.

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Resolução dispõe sobre a Política de Segurança de Informação e Comunicações (POSIC), e foi elaborada pelo Comitê Gestor de Segurança da Informação e Comunicação (CGSIC) no âmbito Instituto Federal de Educação, Ciência e Tecnologia de Roraima (IFRR) instituído pela Resolução 685/2022 - CONSUP/IFRR, de 20 de julho de 2022, com vigência no biênio de 2024 a 2025.

Art. 2º A presente Resolução visa promover a segurança da informação, fomentando o envolvimento das demais estruturas organizacionais, pessoas, processos, regulamentações, ambiente e sua cultura, entre outros. Para fins da Política Nacional de Segurança da Informação (PNSI), instituída pelo Decreto nº 9.637, de 26 de dezembro de 2018 e suas alterações, a segurança da informação no âmbito da Administração Pública Federal abrange: I. segurança cibernética; II. defesa cibernética; III. segurança física; IV. proteção de dados organizacionais; e V. ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. Para atender aos requisitos de segurança da informação, os órgãos e entidades da Administração Pública Federal devem planejar e realizar continuamente a gestão da segurança da informação, mantendo o alinhamento com o desenvolvimento da tecnologia e de seus riscos e identificando os fatores diversos que possam impactar no alcance dos objetivos institucionais.

DAS DEFINIÇÕES, FINALIDADES E OBJETIVOS

Art. 3º São objetivos desta resolução definir a política sobre a utilização segura dos ativos

de Tecnologia da Informação e Comunicação (TIC) no IFRR, estabelecendo as diretrizes básicas a serem seguidas pelos comunidade acadêmica (Professores, Técnico-Administrativos em Educação e Estudantes), público externo e pela Diretoria de Tecnologia da Informação (DTI) no âmbito desta ferramenta. Isto para garantir a exclusividade de sua destinação às finalidades institucionais, a segurança das informações nela contidas e a adequação à legislação vigente, bem como às melhores práticas estabelecidas.

Art. 4º Para os fins desta regulamentação devem ser adotadas as seguintes definições:

I. ADMINISTRADOR: Profissional de TI responsável por administrar os sistemas no âmbito do IFRR;

II. USUÁRIO: os servidores e alunos do IFRR ou outros por interesse da administração pública;

III. E-MAIL: serviço que viabiliza a transferência eletrônica de informação, na forma de mensagem;

IV. E-MAIL INSTITUCIONAL: serviço de correio eletrônico (E-MAIL) de propriedade do IFRR (@IFRR.edu.br e @...IFRR.edu.br);

V. E-MAIL PESSOAL: serviço de correio eletrônico (E-MAIL) de uso pessoal do usuário, para vistas de recuperação de senha;

VI. PERFIL DE USUÁRIO: permissões de acesso a módulos e funcionalidades do sistema;

VII. SETOR: departamento onde o servidor/usuário está lotado;

VIII. INTERNET: rede mundial de computadores, que se comunicam utilizando de protocolos TCP/IP.

IX. Comitê de Governança Digital (CGD): Colegiado interno que possui natureza consultiva e é responsável pelo alinhamento e regulação das ações de TIC ao disposto no Plano de Diretor de TI (PDTI) e no Plano Estratégico de Tecnologia da Informação (PETI).

X. Comitê Gestor de Segurança da Informação e Comunicação (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.

XI. Diretoria 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 TIC, bem como por sua implementação e gestão.

XII. Coordenação de Tecnologia da Informação (CTI) de um campus: 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.

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

XIV. Usuário interno: qualquer pessoa física ou unidade interna que faça uso de informações e/ou equipamentos que estejam vinculados administrativamente ao do IFRR;

XV. Usuário externo: qualquer pessoa física ou jurídica que faça uso de informações e/ou equipamentos que não esteja vinculada administrativamente ao IFRR;

XVI. Política de Segurança da Informação e Comunicação (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;

XVII. Plano de continuidade de negócios: conjunto de procedimentos a serem adotados quando a Instituição se deparar com problemas que comprometam o andamento normal dos processos e a consequente prestação dos serviços;

XVIII. Termo de responsabilidade: acordo de confidencialidade e não divulgação de informações, que atribui responsabilidades ao servidor e ao administrador de serviço quanto ao sigilo e à correta utilização dos ativos de propriedade da Instituição ou por ela custodiados;

XIX. Segurança da Informação e Comunicação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

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

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

XXIII. 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;

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

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

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

XXVII. 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;

XXVIII. 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;

XXIX. 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.

XXX. Risco: combinação da probabilidade de ocorrência de um evento e de suas consequências;

XXXI. 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;

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

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

XXXIV. Análise/avaliação de riscos: processo completo de análise e avaliação de riscos;

XXXV. Tratamento do risco: processo de seleção e implementação de medidas para modificar um risco;

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

XXXVII. 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 à segurança da informação [ISO/IEC TR 18044:2004];

XXXVIII. 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];

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

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

XLI. 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.

XLII. 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;

XLIII. Ativos de software: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;

XLIV. Ativos físicos: equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;

XLV. 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.

XLVI. Domínio de rede: é um agrupamento lógico de contas e recursos, os quais compartilham políticas de seguranças de forma centralizada;

XLVII. Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

XLVIII. Gestão de mudanças: processo voltado a mitigar eventuais resistências e obter mudanças eficazes e eficientes em decorrência da evolução de processos e de tecnologias da informação, considerando a análise crítica de consequências em alterações, independentemente de terem sido planejadas.

CAPITULO II
DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 5º. Esta Política de Segurança da Informação e Comunicações (POSIC) 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.

Parágrafo único. Esta POSIC é constituída por um conjunto de 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.

I. Controle de Acesso a Sistemas e Recursos de TIC: A maior parte dos sistemas utilizados no âmbito deste Instituto, funciona através de servidor de autenticação integrado, entretanto, existem ainda alguns sistemas que não foram integrados ao serviço de autenticação centralizada. Seja qual for o caso, a utilização de senhas fortes e a responsabilidade pelo uso individual e intransferível dessas credenciais de acesso recaem sobre cada usuário, independentemente do perfil. A Nota Técnica publicada Pela DTI ou setor afim, que for mais recente e tratar do tema, indicará em detalhes as particularidades da Política de Credenciais de Acesso, indo desde padrões de senhas fortes, até o uso de certificados digitais e biometria, de acordo com cada caso;

II. Implicações: o descumprimento de normas, má gestão dos recursos, ações ou negligências que resultarem em prejuízo ao patrimônio ou funcionamento dos serviços prestados pelo IFRR poderá resultar em sanções administrativas, civis e/ou criminais, conforme legislação vigente.

CAPÍTULO III
PRINCÍPIOS E PREMISSAS

Art. 6º. Além dos princípios de confidencialidade, integridade, disponibilidade, autenticidade e não repúdio, bem como as normas da legislação brasileira em vigência, a POSIC do IFRR é regida também pelos seguintes princípios:

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

II. 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;

III. 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;

IV. 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;

V. 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;

VI. Privacidade: promover o respeito aos direitos humanos e às garantias fundamentais, de forma a assegurar a liberdade de expressão, o acesso à informação e a proteção dos dados e da privacidade.

CAPÍTULO IV
SISTEMA UNIFICADO DE ADMINISTRAÇÃO PÚBLICA

Art. 7º. O Sistema Unificado de Administração Pública (SUAP) foi desenvolvido originalmente pela equipe de Tecnologia da Informação do Instituto Federal do Rio Grande do Norte (IFRN) e vem sendo regularmente mantido e atualizado por eles. Através de acordos de cooperação técnica o SUAP está sendo utilizado e customizado por diversas instituições da Rede Federal de Ensino Técnico e Tecnológico, inclusive como solução integrada de processos no IFRR.

Art. 8º São condições gerais de utilização do SUAP

I . Veiculação de mensagens de conteúdo, EXCLUSIVAMENTE, acadêmico ou administrativo, não sendo permitido o uso para fins que não sejam consonantes com o uso institucional;

II. As informações inseridas no SUAP são elementos de formação da imagem institucional do IFRR e possuem caráter legal, portanto, devem merecer o mesmo tratamento de documentos impressos;

III. O acesso ao SUAP a pessoas que não fazem parte do quadro de pessoal do IFRR, será regido pelo constante no ITEM 6 desta regulamentação;

IV. Ao utilizar o SUAP o usuário o assume com suas características e normas;

V. Os dados de acesso e senha são pessoais e intransferíveis e devem seguir as orientações gerais para gestão de senhas na Nota Técnica mais recente que trate sobre o tema.

Art. 9º É considerado uso indevido do SUAP:

I. Tentativa de acesso a contas de terceiros;

II. Disponibilização de informações sobre usuários e senhas, mesmo que de sua responsabilidade para qualquer pessoa ou organização;

III. Veiculação de informações confidenciais, como de pessoas e/ou processos;

IV. Fornecimento de informações inverídicas;

V. Forjar a identidade de outra pessoa (por exemplo, usando o acesso dessa pessoa) ou fazer falsa declaração de sua identidade;

VI. Alterar qualquer página da web que faça parte do serviço do SUAP sem prévia autorização da DTI;

VII. Outras atividades que possam afetar negativamente o IFRR, bem como servidores, alunos, terceiros ou pessoas externas, e que não tenham finalidade amparada por norma.

§ 1º Caso ocorra constatação de má utilização do SUAP a Administração do IFRR poderá solicitar a equipe da DTI para investigar o acesso indevido do usuário e remeter aos setores correcionais pertinentes.

§ 2º O acesso ou permissões do usuário ao SUAP, em caso da comprovação de utilização inadequada, poderá ser suspenso se solicitado pela Administração, sem prejuízo das punições previstas na Lei 8.112 de 1990.

Art. 10. Serão fornecidos os seguintes perfis de acesso ao SUAP:

I. Perfil de usuário individual, para todos os servidores em exercício no Instituto;

II. Perfil de usuário individual, para docentes substitutos, durante a vigência de seus contratos;

III. Perfil de usuário individual, para funcionários terceirizados e prestadores de serviços durante a vigência de seus contratos, devendo ser solicitado pela chefia imediata, fiscal do contrato ou autoridade relacionada ao serviço;

IV. Perfil de usuário individual, para discentes, para todos os alunos matriculados em cursos ofertados pelo IFRR;

V. Perfil de usuário individual para assinatura digital ou outros fins pertinentes, para quaisquer Pessoas Externas não Terceirizados, durante a vigência de sua autorização para acesso ao sistema.

Art. 11. A criação de um perfil de acesso ao SUAP deverá seguir o procedimento conforme abaixo:

I. No caso de servidor, o mesmo deverá estar cadastrado no SIAPE (Sistema de controle de dados do servidor), vinculado ao IFRR e aguardar a importação dos dados para o SUAP, que ocorre periodicamente;

II. No caso de funcionários terceirizados ou prestadores de serviço, o acesso ao mesmo deverá ser solicitado via chamado na Central de Serviços do SUAP pela chefia imediata, fiscal do contrato ou autoridade relacionada;

III. No caso do discente, o mesmo deverá estar matriculado em um curso do IFRR;

IV. O acesso do Servidor é realizado pela matrícula SIAPE, o acesso do Aluno pela matrícula acadêmica e dos Terceirizados e Prestadores de Serviço, pelo CPF;

V. O primeiro acesso ao sistema será feito clicando na opção "Esqueceu ou deseja alterar sua senha?", disponível na tela de login do SUAP;

VI. Será enviada uma senha para o e-mail informado no cadastro, orientando a troca ou definição da senha;

VII. Após o cadastro da senha, o usuário estará habilitado para acesso ao SUAP e demais sistemas institucionais.

Art. 12. Serão excluídos os acessos no SUAP nos casos de:

I . Servidores, nos casos de vacância por posse em outro cargo inacumulável, exoneração, demissão, aposentadoria, falecimento ou qualquer outro que implique o desligamento do servidor do quadro de pessoal do IFRR, o acesso poderá ser alterado ou bloqueado, de acordo com cada caso, após sincronização com o SIAPE;

II. No caso de Funcionários Terceirizados, o perfil será alterado para usuário externo sem ocupação ativa quando ao final da vigência da ocupação, devendo a chefia imediata ou o fiscal de seu contrato informar imediatamente ao setor de TI do *Campus* ou Reitoria, para ajustes que se fizerem necessários;

III. No caso de Pessoas Externas não Terceirizadas, o nível de acesso padrão é significativamente restrito e poderá ser bloqueado quando da sua desautorização de acesso pela área concedente da autorização, por qualquer motivo, sendo o mesmo efetuado pelo setor de TI do *Campus* ou Reitoria;

Art. 13. Serão realocadas (mudança de setor) as contas de acesso ao SUAP:

I. Nos casos de transferência de setor, entre campi, ganho ou perda de função ou qualquer outro que implique na mudança de setor do servidor dentro do quadro de pessoal do IFRR;

II. A mudança poderá ocorrer de forma automática após o cadastramento, extração e sincronização dos dados oriundos do SIAPE para o SUAP, conforme seu funcionamento;

III. Em caso de realocação todos os acessos do usuário serão restaurados para o perfil de acesso básico de servidor, devendo a chefia do novo setor realizar solicitação de perfil aos módulos necessários para execução das atividades.

Parágrafo único. A chefia imediata será responsável por liberar os acessos para os módulos de Documento e Processo Eletrônico.

Art. 14. Deveres e responsabilidades relacionados ao SUAP

I. São deveres dos usuários do SUAP:

a. Não compartilhar certificado digital, logins, senhas ou qualquer meio de acesso ao SUAP. As senhas de acesso são de uso pessoal e intransferível e o usuário deverá realizar a substituição da mesma em caso de suspeita de violação;

b. Manter absoluta cautela quando da exibição de dados em tela, prints, documentos impressos, ou ainda na gravação em meios eletrônicos, a fim de que deles não venham tomar ciência pessoas não autorizadas;

c. Não se ausentar do terminal sem encerrar a sessão de uso do sistema, de forma a possibilitar o uso indevido por pessoas não autorizadas;

d. Notificar a DTI quando ocorrerem irregularidades na utilização das informações ou do acesso que venha a ter conhecimento;

e. Guardar sigilo funcional sobre as informações restritas contidas no SUAP;

f. Garantir a veracidade dos dados fornecidos bem como manter as informações do SUAP, de sua responsabilidade, sempre atualizadas;

g. Responder, em todas as instâncias devidas, pelas ações ou omissões que possam por em risco ou comprometer a exclusividade de conhecimento de senhas pessoais ou de informações decorrentes dos perfis de acesso em que esteja habilitado.

II. São deveres da Diretoria de Tecnologia da Informação (DTI):

a. Disponibilizar a utilização SUAP aos servidores do IFRR;

b. Prestar informações aos servidores do IFRR, quando solicitada, em relação ao uso do SUAP e seus módulos;

c. Administrar e propor políticas, procedimentos e melhores práticas relativos ao SUAP;

d. Verificar periodicamente o desempenho, a disponibilidade e a integridade do SUAP;

Art. 15. Infraestrutura e disponibilidade do SUAP

I. Das características tecnológicas e ocorrências:

a . A infraestrutura de serviços do SUAP possui recursos para disponibilidade de operação. No entanto, por características próprias da Internet, podem ocorrer interrupções de outras naturezas;

b. A DTI trabalha para garantir a segurança, sigilo, inviolabilidade, individualidade das informações, acessos e demais conteúdo armazenados e utilizados pelo SUAP, no entanto não se responsabiliza pela sua má utilização;

c. Manutenções programadas no sistema que exijam parada temporária serão avisadas com antecedência aos usuários;

CAPÍTULO IV
DIRETRIZES GERAIS

Art. 16. Quanto ao tratamento da informação, cabe ao IFRR classificar a informação tratada no âmbito da instituição observando, entre outros dispositivos legais, o Programa de Privacidade e Segurança da Informação (PPSI) do Governo Federal e o ciclo do Plano de Trabalho em andamento neste Instituto. O tratamento de toda e qualquer informação deve garantir os níveis de proteção adequados conforme sua classificação.

Art. 17. Quanto à segurança física do ambiente, cabe ao IFRR implementar os controles necessários para impedir perdas, danos, furto, ou comprometimento de ativos e interrupção das

operações, além de prevenir o acesso físico não autorizado, danos e interferências nas informações e em seus recursos de processamento da organização.

Art. 18. No tocante à gestão de incidentes de segurança da informação, cabe ao IFRR regulamentar, planejar e realizar a gestão de incidentes em segurança da informação com o objetivo de implantar processos, disponibilizar recursos e executar ações de prevenção, tratamento e resposta a qualquer evento adverso relacionado à segurança da informação. Tais incidentes devem ser comunicados à DTI, ou à equipe formalmente designada para esse tema, caso a designação esteja vigente;.

Art. 19. Na gestão de ativos de informação, cabe ao IFRR regulamentar, planejar e executar o processo de mapeamento de ativos de informação com o objetivo de subsidiar os processos de gestão de riscos, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.

.Art. 20. Em relação à comunicações, os recursos operacionais e de comunicações, tais como e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros, devem ser destinados, exclusivamente, a fins diretos e complementares às atividades administrativas e acadêmicas da instituição. O IFRR reserva-se o direito de monitorar e controlar o uso dos recursos operacionais e de comunicações disponibilizados, assim como revogar permissões de acesso caso sejam identificadas irregularidades

Art. 21. Em se tratando de Controle de Acessos, cabe ao IFRR regulamentar, planejar, implantar e gerenciar controles físicos e lógicos adequados para restringir o acesso à informação e aos recursos de processamento da informação às pessoas e entidades devidamente autorizadas, como forma de prevenção de incidentes de segurança.

Art. 22. A Gestão de Continuidade de Negócios de TI tem a finalidade de minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas, além de recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de resposta a incidentes e recuperação de desastres.

Art. 23. Gestão de Mudanças na TI: A gestão de mudanças nos aspectos de Tecnologia da Informação e segurança da informação tem a finalidade de mitigar eventuais resistências e obter mudanças eficazes e eficientes em decorrência da evolução de processos e de tecnologias da informação. Cabe ao IFRR regulamentar, planejar e executar o processo de mudanças nos aspectos de segurança da informação, com base no processo de gestão de riscos de segurança da informação.

Art. 24. O Comitê de Governança Digital (CGD) deve:

I. Nomear, como seu subcomitê, o Comitê Gestor de Segurança da Informação (CGSI).

II. Designar um Coordenador do CGSI;

III. Deliberar, quando necessário, sobre os casos encaminhados pelo CGSI.

Art. 25. O Comitê Gestor da Segurança da Informação (CGSI) deve:

I. Assessorar a implementação das ações de segurança da informação;

II. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III. Participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

IV. Propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;

V. Deliberar sobre normas internas de segurança da informação;

VI. Participar dos processos que envolvem a Continuidade de Negócio de TI, Recuperação de Incidentes de TI e Gestão de Mudanças de TI.

Art. 26. Os Dirigentes e Chefias do IFRR devem:

I. Garantir que as atividades desempenhadas sob sua gestão estejam de acordo com esta POSIC;

II. Promover a capacitação dos recursos humanos sob sua gestão em temas relacionados à segurança da informação em parceria com os setores de TI;

III. Acompanhar a execução das ações de segurança da informação no seu âmbito de atuação;

IV. Garantir a transmissão e a guarda de dados exclusivamente em infraestrutura provida ou homologada pelo IFRR;

V. Garantir a utilização exclusiva dos recursos, serviços e sistemas de tecnologia da informação providos ou homologados pelo IFRR, ainda que haja alternativas gratuitas;

VI. Estimular a cultura de segurança da informação;

VII. Disseminar normas e boas práticas de segurança da informação.

Art. 27. Membros da comunidade e demais recursos humanos e partes externas devem:

I. Estar cientes e cumprir diretrizes, princípios e regras estabelecidas por esta POSIC, incluindo suas atualizações;

II. Guiar-se pelos princípios e premissas destacados nesta POSIC no decorrer de suas atividades;

III. Zelar pelo sigilo e integridade das informações e dos ativos aos quais tiver acesso;

IV. Adotar boas práticas de segurança da informação;

V. Responder por seus atos e acessos que causem danos ou prejuízos às informações e aos ativos no âmbito da instituição, ou violem as regras dispostas nesta POSIC ou em seus instrumentos complementares;

VI. Respeitar a legislação e as normas de propriedade intelectual pertinentes;

VII. Respeitar a legislação e as normas de proteção de dados e privacidade de informações pessoais pertinentes;

VIII. Comunicar ao IFRR sempre que tomar ciência de evento adverso que possa configurar incidente de segurança da informação;

IX. Armazenar e preservar as informações em infraestrutura provida pela instituição, ou em nuvem, desde que aprovada e homologada pelo IFRR;

X. Utilizar exclusivamente os recursos, serviços e sistemas de tecnologia da informação providos ou homologados pelo IFRR, ainda que haja alternativas livres e gratuitas;

XI. Propor melhorias à segurança da informação no âmbito da instituição.

CAPITULO V
DISPOSIÇÕES FINAIS

Art. 28. Demais sistemas de informação utilizados no IFRR terão tratamento análogo a esta norma e os casos omissos ou não previstos nesta Resolução poderão ser analisados pela DTI ou ainda serem submetidos ao Comitê de Governança Digital (CGD) que, se considerar necessário, fará convocação de reunião do Comitê.

Art. 29. Procedimentos de Backup e Restauração de dados e arquivos inerentes aos sistemas do IFRR seguirão Manual Interno de Backup e Restauração a ser Publicado pelo Núcleo de Infraestrutura de Redes, conforme cada sistema e tipo de dado, para estabelecimento de prazo de preservação, incluindo os arquivos utilizados pelos usuários nas pastas de rede pessoais e setoriais.

Parágrafo único. Arquivos locais, nas estações de trabalho dos usuários, não serão

incluídos no procedimento de backups e restauração.

Art. 30. Os equipamentos em uso nas dependências das Unidades do IFRR estão sob a responsabilidade das respectivas Unidades. Os laboratórios de informática devem ser monitorados prioritariamente por servidores aptos para supervisão e manutenção preventiva dos equipamentos, podendo ainda a Unidade contar com estagiários e terceirizados treinados para essa atribuição. O funcionamento de cada laboratório é de competência da Unidade a qual pertence.

Art. 31. Fica revogada as disposições anteriores acerca da POSIC.

Art. 32. Esta Resolução entra em vigor na data de sua publicação.

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

Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia de Roraima, em Boa Vista-RR, 6 de maio de 2024.

Nilra Jane Filgueira Bezerra
Presidente do CONSUP

ANEXO ÚNICO

Referências e fundamentação legal para elaboração da POSIC

Decreto nº 1.171, de 24 de junho de 1994, que dispõe sobre o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive por meios digitais, por pessoa natural ou por pessoas jurídica de direito público ou privado, com objetivo de proteger os direitos fundamentais de liberdade e de privacidade, e o livre desenvolvimento da personalidade da pessoa natural;

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;

Decreto nº 9.637, de 26 de dezembro de 2018;

Decreto nº 10.748, de 16 de julho de 2021;

Instrução Normativa nº 1, de 27 de maio de 2020 do Gabinete de Segurança Institucional da Presidência da República;

Instrução Normativa nº 2, de 24 de julho de 2020 do Gabinete de Segurança Institucional da Presidência da República;

Instrução Normativa nº 3, de 28 de maio de 2021 do Gabinete de Segurança Institucional da Presidência da República;

Portaria nº 93, de 18 de outubro de 2021 do Gabinete de Segurança Institucional da Presidência da República;

Portaria SGD/MGI Nº 852, de 28 de março de 2023;

Norma técnica ABNT NBR ISO IEC 27001:2013, lançada em 08 de novembro de 2013;

Norma técnica ABNT NBR ISO IEC 27002:2013, lançada em 08 de novembro de 2013;

Norma técnica ABNT NBR ISO IEC 27701:2019, lançada em 09 de dezembro de 2019;

Apostila Gestão da Segurança da Informação: NBR 27001 e NBR 27002 (Escola Superior de Redes da Rede Nacional de Ensino e Pesquisa).