Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul

POLÍTICA

DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO - PoSIC

INSTITUTO FEDERAL
Mato Grosso do Sul

Missão

Promover a educação de excelência por meio do ensino, pesquisa e extensão nas diversas áreas do conhecimento técnico e tecnológico, formando profissional humanista e inovador, com vistas a induzir o desenvolvimento econômico e social local, regional e nacional.

Visão

Ser reconhecido como uma instituição de ensino de excelência, sendo referência em educação, ciência e tecnologia no Estado de Mato Grosso do Sul.

Valores

Inovação;
Ética;
Compromisso com o desenvolvimento local e regional;
Transparência;
Compromisso Social.

INSTITUTO FEDERAL
Mato Grosso do Sul

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO DO SUL IFMS	
Endereço:	Rua Treze de Maio, 3439, Centro – Campo Grande/MS – CEP: 79002-352 (Endereço provisório)
CNPJ:	10.673.078/0001-20

IDENTIFICAÇÃO	
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO	
Elaborado por:	Comitê de Segurança de Tecnologia da Informação e Comunicação
Data de publicação:	Agosto/2021

TRAMITAÇÃO	
CONSELHO SUPERIOR	
Processo n°:	23347.016572.2018-22
Relator:	Claudia Santos Fernandes
Discussão:	39ª Reunião Ordinária do Conselho Superior
Data da reunião:	25/03/2021
Aprovação:	Resolução 19/2021 - COSUP/RT/IFMS de 30 de julho de 2021
Boletim de Serviço:	Nº 37 de 30 de julho de 2021

HISTÓRICO	
DATA	ALTERAÇÃO
07/02/2011	Regulamento Nº 002: Política da Segurança da Informação
30/07/2021	Política de Segurança da Informação e Comunicação (PoSIC)

RESOLUÇÃO Nº 19, DE 30 DE JULHO DE 2021

Aprova a Política da Segurança da Informação e Comunicação (PoSIC) no âmbito do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul.

O CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO DO SUL (IFMS), no uso das atribuições que lhe conferem o art. 10, §3º, da Lei n° 11.892, de 29 de dezembro de 2008, e o art. 13, inciso XVI, do Estatuto do IFMS; e tendo em vista o Processo nº 23347.016572.2018-22 apreciado na 39ª Reunião Ordinária, em 25 de março de 2021,

RESOLVE

Art. 1º Aprovar a Política da Segurança da Informação e Comunicação (PoSIC) no âmbito do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

Elaine Borges Monteiro Cassiano
Presidente do Conselho Superior

Documento assinado eletronicamente por:

- **Elaine Borges Monteiro Cassiano**, **REITORA - CD1 - IFMS**, em 30/07/2021 15:48:18.

Este documento foi emitido pelo SUAP em 29/07/2021. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifms.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 214680
Código de Autenticação: 4acfe740d2

SUMÁRIO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (POSIC) DO IFMS

Dispõe sobre a Política de Segurança da Informação e Comunicação no âmbito do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul.

CAPÍTULO I

Disposições Gerais

Art 1º A Política de Segurança da Informação e Comunicação (PoSIC) tem por objetivo estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados e a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, assegurando os princípios básicos de segurança da informação: disponibilidade, integridade, confidencialidade e autenticidade das informações e comunicações que suportam os objetivos estratégicos do IFMS.

Art 2º Para fins desta Política, entende-se por:

I - ativos de patrimônio do IFMS: qualquer bem, tangível ou intangível, que tenha valor para a organização;

II - Coirt: Coordenação de Infraestrutura, Redes e Telecomunicações;

III - colaborador(a): pessoa que presta serviço para a Administração Pública, em caráter eventual, sem vínculo com nenhum órgão da esfera pública;

IV - consultor(a) externo: profissional que realiza orçamentos e consultorias, não pertencente aos quadros de funcionários/colaboradores e não mantém nenhum vínculo contratual formal;

V - Dirti: Diretoria de Gestão de Tecnologia da Informação;

VI - drives de rede: unidade de armazenamento de dados alocada em um servidor de arquivos e compartilhado por meio da intranet do IFMS;

VII - Equipe de Tratamento de Incidentes em Segurança da Informação e Comunicação (Etir): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;

VIII - estagiário(a): o(a) estudante regularmente matriculado nos Cursos de Educação Profissional Técnica de Nível Médio, nos Cursos Técnicos Subsequentes, nos Cursos Superiores de Tecnologia e Bacharelado do IFMS nas modalidades presencial e a distância,

aceitos por pessoas jurídicas de direito privado, órgãos de administração pública e instituições de ensino, para o desenvolvimento de atividades nas modalidades obrigatórias e relacionadas ao PPC;

IX - Gestão de Continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio; caso as ameaças se concretizem, busca a oferta de uma estrutura que desenvolva a resiliência organizacional capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;

X - Gestão de Riscos de Segurança da Informação e Comunicação: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

XI - Gestor(a) da Informação: qualquer servidor(a) ou unidade que, no exercício de suas competências, é responsável pela produção de informação ou pelo tratamento, ainda que temporário, de informações de propriedade de pessoa física ou jurídica entregues ao IFMS;

XII - Gestor(a) de Segurança da Informação e Comunicação: responsável pelas ações de segurança da informação e comunicação no âmbito do IFMS;

XIII - IFMS: Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul;

XIV - informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XV - Política de Segurança da Informação e Comunicação (PoSIC): documento com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficiente à implementação da segurança da informação e comunicação neste órgão;

XVI - prestador(a) de serviço: quem trabalha para empresa prestadora de serviços contratada ou conveniada para a execução de atividade, de qualquer natureza, desenvolvida no IFMS;

XVII - recurso de TI: pode ser considerado como qualquer elemento utilizado para alcançar um determinado fim, isto é, aplicação, software, equipamento, etc;

XVIII - resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre;

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

XX - Serti: Serviço de Tecnologia da Informação e Suporte Técnico;

XXI - servidor(a) público: pessoa física que presta serviços ao estado e às entidades da administração indireta, com vínculo empregatício e mediante remuneração paga pelos cofres públicos;

XXII - 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;

XXIII - trilhas de auditoria: arquivos de Logs do sistema, que contém as gravações das ações realizadas no sistema, de modo a identificar quem ou o que causou algo;

XXIV - usuário externo: qualquer pessoa física ou jurídica que faça uso de informações e que não tenha vínculo administrativo ou acadêmico com o IFMS;

XXV - usuário interno: qualquer pessoa física ou unidade interna que faça uso de informações e que tenha vínculo administrativo ou acadêmico com o IFMS;

XXVI - usuários: usuários internos e externos; servidores, terceirizados, colaboradores, consultores, auditores e estagiários/bolsistas que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão.

CAPÍTULO II

Princípios

Art 3º Esta PoSIC e suas ações serão norteadas pelos seguintes princípios:

I - confidencialidade: as informações somente estarão disponíveis ou reveladas à pessoa, sistema, órgão ou entidade autorizada e credenciada;

II - integridade: as informações não são modificadas ou excluídas de maneira não autorizada ou acidental;

III - disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado;

IV - autenticidade: princípio de segurança que assegura ser do autor a responsabilidade pela criação ou divulgação de uma informação;

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

VI - não repúdio: garantia de que o autor da informação não irá negar posteriormente a autoria da mensagem ou transação, permitindo sua identificação;

VII - equanimidade: as normas e regras de segurança da informação são obedecidas por todos, estudantes e servidores do IFMS, sem distinção de cargo ou função;

VIII - ciência: todos os servidores, colaboradores, consultores externos, estagiários, prestadores de serviço e estudantes devem ter ciência das normas, procedimentos, orientações e outras informações que permitam a execução de suas atribuições sem comprometer a segurança;

IX - proporcionalidade: o nível, a complexidade e os custos das ações de Segurança da Informação e Comunicação no âmbito do IFMS serão adequados ao entendimento administrativo e ao valor do ativo a proteger.

CAPÍTULO III

Referências Legais e Normativas

Art 4º As ações de Segurança da Informação e Comunicação do IFMS deverão observar os seguintes requisitos legais e normativos:

I - Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei nº 2.848/40 (Código Penal Brasileiro), de modo a prever a tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

II - Lei nº 7.232, de 29 de outubro de 1984, que dispõe sobre a Política Nacional de Informática;

III - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados;

IV - Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.

V - Decreto nº 7.724, de 16 de maio de 2012, que dispõe sobre as normas de classificação de informações, acesso à informação, uso e descarte de ativos de informação, dentre outros temas afins;

VI - Decreto Nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação;

VII - Acórdão do Tribunal de Contas da União nº 461 de 28 de abril de 2004;

VIII - Norma ISO/IEC TR nº 13335-3:1998, que fornece técnicas para a gestão de segurança na área de tecnologia da informação, baseada nas normas ISO/IEC nº 13335-1 e TR ISO/IEC nº 13335-2;

IX - Norma ISO 31.000:2018 - Diretrizes para a implementação da gestão de riscos;

X - Norma NBR ISO/IEC 27002:2005 - Código de Práticas para a Gestão da Segurança da Informação;

XI - Norma Complementar nº 04/IN01/DSIC/GSIPR, de 17 de agosto de 2009, diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal;

XII - Norma Complementar nº 09/IN01/DSIC/GSIPR, de 16 de julho de 2014, que estabelece orientações específicas para o uso de recursos criptográficos em Segurança da

Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta;

XIII - Instrução Normativa nº 1, de 27 de maio de 2020, dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

XIV - a Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação.

CAPÍTULO IV

Diretrizes Gerais

Art 5º Cada servidor(a) público é responsável pela Segurança da Informação no âmbito do IFMS.

Art 6º Toda informação gerada ou recebida pelos servidores, colaboradores, fornecedores e prestadores de serviço, em função exercida e/ou atividade profissional contratada, pertence ao IFMS. As exceções devem ser explícitas e formalizadas entre as partes por vias contratuais.

Art 7º Os usuários internos e externos devem observar que:

I - o acesso à informação será regulamentado por normas específicas de tratamento da informação. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo IFMS é considerada seu patrimônio e deve ser protegida;

II - os recursos disponibilizados pelo IFMS, e de sua propriedade, são fornecidos com o propósito único de garantir o desempenho das suas atividades;

III - as normas para as operações de armazenamento, divulgação, reprodução, recuperação e destruição da informação serão definidas de acordo com a classificação desta, sem prejuízo de outros cuidados que vierem a ser especificados pelo gestor.

Art 8º É condição para acesso dos usuários externos aos recursos de informação do IFMS, a adesão formal aos termos desta PoSIC, mediante assinatura de Termo de Responsabilidade.

Art 9º O serviço de correio eletrônico disponibilizado pelo IFMS 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 IFMS e, portanto, passível de auditoria.

Art. 10 O acesso à Internet será concedido para todos os servidores, com utilização exclusiva para fins diretos e complementares às atividades do setor.

Art. 11 acesso à Internet será concedido para todos os estudantes com utilização para fins acadêmicos e/ou atividades que não infrinjam a esta PoSIC.

Art. 12 Todo acesso à Internet será monitorado e passível de auditoria.

Art. 13 Todo o acesso a redes e sistemas do órgão deverá ser realizado, preferencialmente, por meio de login de acesso único, pessoal e intransferível.

CAPÍTULO V

Diretrizes Específicas

Art. 14 Esta política aplica-se tanto no ambiente informatizado quanto nos meios convencionais de processamento, comunicação e armazenamento da informação é regida pelas seguintes diretrizes:

I - Tratamento da Informação - define os requisitos e regras para classificação e tratamento da informação no ambiente de Tecnologia da Informação e Comunicação (TIC) do IFMS, considerando as seguintes diretrizes gerais:

a) arquivos fundamentais para as atividades dos usuários da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário;

b) arquivos pessoais e/ou não pertencentes às atividades do IFMS (fotos, músicas, vídeos etc.) não deverão ser copiados ou movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso sejam identificados, esses arquivos poderão ser excluídos definitivamente sem necessidade de comunicação prévia ao usuário;

c) as normas de classificação de informações, acesso à informação, uso e descarte de ativos de informação, dentre outros temas afins, serão fixadas em estrita aderência às leis e normas atinentes à Administração Pública Federal, considerando as competências regimentais baseados no Decreto nº 7.724, de 16 de maio de 2012;

d) cada setor será responsável por classificar a informação sob sua custódia, respeitando os critérios estabelecidos.

II - Tratamento de Incidentes de Rede:

a) cabe à Dirti a responsabilidade pela infraestrutura necessária para fins de registro e resposta aos incidentes de segurança da informação no âmbito da rede corporativa do IFMS;

b) a Equipe de Tratamento de Incidentes de Rede (Etir) será instituída na Coirt;

c) todo usuário é responsável por notificar, imediatamente, incidentes que afetem a segurança da informação por meio de recursos de TIC ou o descumprimento da PoSIC/IFMS à Serti/Dirti, para que as providências necessárias sejam adotadas a fim de sanar as causas.

III - Gestão de Riscos é um conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias, especificamente, para mitigar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos:

a) cabe ao Comitê de Segurança de Tecnologia da Informação e Comunicação (CSTIC) a responsabilidade pela Gestão de Riscos de Segurança da Informação e Comunicação;

b) fica estabelecido o Processo de Gestão de Riscos de Segurança da Informação e Comunicação (PGRSIC), com vistas a minimizar possíveis impactos associados aos ativos de informação e comunicação;

c) o PGRSIC baseia-se nas melhores práticas, na Norma ISO 31.000:2018 - Diretrizes para a implementação da gestão de riscos e na Norma Complementar nº 04/IN01/DSIC/GSI/PR;

IV - Gestão de Continuidade tem como objetivo evitar situações de interrupção e manter em funcionamento os sistemas de informação e comunicação do IFMS, o Comitê de Segurança de Tecnologia da Informação e Comunicação (CSTIC), com a participação da Diretoria de Gestão da Tecnologia da Informação (Dirti), deverá manter um Programa de Gestão da Continuidade de Negócios:

a) determinar estratégias de continuidade de negócios adequada para proteger, estabilizar, continuar, retomar e recuperar as atividades prioritárias;

b) constituir planos de redundância e backup em equipamentos essenciais para o funcionamento dos serviços básicos da instituição;

c) estabelecer planos de administração de crises, contingência, recuperação de desastres e continuidade operacional;

d) identificar ameaças, vulnerabilidades, consequências e estimar riscos que possam comprometer a continuidade das atividades essenciais do IFMS;

e) estabelecer níveis adequados de autoridade e competência para assegurar a continuidade das atividades críticas; e

f) viabilizar a continuidade e recuperação de atividades críticas e realizar treinamentos periódicos para garantir o funcionamento dos planos de continuidade.

V - Auditoria e Conformidade - define que o uso dos recursos de TIC disponibilizados pelo IFMS é passível de monitoramento e auditoria, conforme o previsto no

item 9.1.4 do acórdão do Tribunal de Contas da União nº 461 de 28 de abril de 2004, que dispõe sobre a análise regular de arquivos logs com utilização, sempre que possível, de softwares utilitários específicos para monitoramento do uso dos sistemas, e serão implementados e mantidos, sempre que possível, mecanismos que permitam a rastreabilidade desse uso.

a) todos os usuários estão sujeitos à auditoria em sua utilização dos recursos;

b) os procedimentos de auditoria e de monitoramento de uso dos recursos serão realizados periodicamente pela Dirti e Serti, com o objetivo de observar o cumprimento das políticas pelos usuários e com vistas à gestão de desempenho e segurança;

c) 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 ao CSTIC 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 à Reitoria do IFMS dependendo da gravidade;

d) será 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.

VI - Controle de Acesso - visa estabelecer critérios para a disponibilização e administração do acesso aos serviços de TIC do IFMS levando em consideração os seguintes itens:

a) o acesso à rede e demais sistemas do IFMS estará disponível a usuários previamente credenciados;

b) poderão ser credenciados servidores (docentes ou técnico-administrativos), estudantes, prestadores de serviço autorizados, e usuários de instituições conveniadas que operam dentro da rede do IFMS, observando-se a necessidade de utilização dos mesmos para a realização de suas atividades, e a respectiva autorização por parte dos responsáveis por esses sistemas;

c) para o ingresso aos recursos da rede IFMS, o usuário deverá ser cadastrado, possuindo, assim, o Passaporte IFMS (usuário e senha) pessoal e intransferível, para efetuar o processo de login e, consequentemente, ter acesso aos recursos de rede necessários à sua atividade na Instituição;

d) ao realizar o ingresso aos recursos da rede IFMS, o usuário, automaticamente, aceita e declara ciência dos termos e condições explicitados ou referidos pelo documento de Normas para Uso de Recursos de Tecnologia da Informação e Comunicação, Uso e Manutenção de Sites e e-mails institucionais do IFMS;

e) o compartilhamento de senhas individuais é proibido para todos os níveis da Instituição. Da mesma forma, abrir uma conexão autenticada para deixar que outra pessoa a

utilize. Em hipótese alguma, um usuário poderá passar sua senha pessoal de acesso para outrem;

f) é dever de todos zelar pelo sigilo de suas senhas de autenticação, bem como escolher senhas fortes dificultando ser descoberta facilmente por outra pessoa;

g) o acesso do usuário poderá ser bloqueado em casos de incidentes de segurança da informação e comunicação causadas pelo mesmo. A conta será restabelecida após a solução dos problemas causados e reorientação ao usuário, desde que não existam outros impedimentos;

h) a Dirti poderá restringir as pessoas que serão administradoras dos respectivos equipamentos computacionais patrimoniados do IFMS;

i) em caso de usuário visitante, poderá ser feito o cadastro da sua conta de acesso desde que solicitado pelo responsável do setor no qual realizará suas atividades, informando para a Dirti/Serti o prazo de validade para a conta a ser criada;

j) será fornecida aos usuários da rede do IFMS conta de e-mail institucional, devendo ser utilizada pelos servidores, estudantes e possíveis prestadores de serviço autorizados exclusivamente para fins institucionais, sendo vedado aos setores administrativos do IFMS a utilização de e-mail de outros provedores para este fim;

k) a rede sem fio acadêmica disponibilizada deverá estar separada da rede administrativa, não sendo recomendada sua utilização para tráfego de informações institucionais do IFMS;

l) a solicitação de cancelamento do acesso à rede e demais sistemas deverá ser encaminhada à Dirti/Serti pelos setores responsáveis, após o desligamento do usuário do IFMS;

m) o acesso fornecido a instituições que utilizarem a rede do IFMS será concedido de acordo com o convênio firmado, sendo necessário definir controles que garantam a responsabilização dos seus usuários por incidentes causados, e a adoção de procedimentos favoráveis à segurança da informação e comunicação, atendendo, no mínimo, aos controles definidos na Política de Segurança da Informação do IFMS; e

n) somente será permitido o uso de recursos homologados e autorizados pela Instituição e atendendo a legislação pertinente em vigor. A utilização desses sem licenças correspondentes é crime, previsto na Lei nº 9.609, de 19 de fevereiro de 1998.

VII - Uso de e-mail é o serviço de correio eletrônico que tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos vinculados às atividades do usuário dentro do IFMS.

a) é vedado ao usuário o uso de serviço de correio eletrônico com o objetivo de executar atividades lesivas, tendentes a comprometer a privacidade de usuários, a segurança e a disponibilidade do sistema, ou a imagem institucional. A violação de qualquer um desses princípios implicará penalidades ao usuário;

b) compete ao IFMS a responsabilidade de disponibilizar o serviço de correio eletrônico, manter o seu funcionamento e oferecer suporte aos usuários;

c) as regras de acesso ao e-mail e utilização serão definidas por norma específica, em conformidade com esta PoSIC/IFMS e demais orientações e diretrizes legais.

VIII - O uso e acesso à internet só poderá ser efetivado pelos membros da Comunidade do IFMS após o cadastro obrigatório de usuários, de acordo com os sistemas de registros implementados na Instituição, considerando os seguintes itens:

a) o IFMS deverá possuir mecanismos de autenticação, que determinam a titularidade de todos os acessos à internet feitos por seus usuários;

b) o usuário será responsável por todas as atividades realizadas por intermédio de sua conta de usuário e senhas de acesso;

c) todos os membros vinculados ao IFMS terão direito de acesso à internet para fins de ensino, pesquisa, extensão e outras finalidades institucionais;

d) a internet poderá ser acessada pelos membros da comunidade acadêmica por meio da rede administrativa ou pela rede sem fio acadêmica, de acordo com os perfis pré-definidos nas normas de Instituição;

e) qualquer informação que seja acessada, transmitida, recebido ou produzida na internet estará sujeita à auditoria. Portanto, o IFMS, em total conformidade legal, reserva-se o direito de monitorar e registrar os acessos à rede mundial de computadores;

f) é proibido o acesso a sites de pornografia, pedofilia e outros contrários à lei, ainda que não estejam bloqueados nos Sistemas de Segurança do IFMS;

g) as regras de acesso e uso da internet serão definidas por norma específica, em conformidade com esta PoSIC/IFMS e demais orientações e diretrizes legais.

IX - Gestão de Ativos de Informação do IFMS - deverá observar normas operacionais e procedimentos específicos para garantir a sua operação segura e contínua.

a) os ativos de informação do IFMS deverão ser inventariados, com a classificação em termos de valor, requisitos legais, sensibilidade e criticidade da informação para o IFMS, e serão atribuídos aos respectivos responsáveis. Seu uso deverá estar em conformidade com os princípios e normas operacionais, sendo destinados exclusivamente ao uso institucional, vedada a utilização para fins em desconformidade com os interesses da instituição;

b) o usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho, respeitando as recomendações de sigilo, conforme disposto em norma e legislação específica de classificação de informação;

c) é vedado comprometer a integridade, a confiabilidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo IFMS.

X - Segurança Física e do Ambiente

a) as informações relevantes deverão ser armazenadas em ambientes seguros bem como os ambientes onde elas serão processadas deverão respeitar normas e padrões de armazenamento;

b) as áreas de segurança deverão ser protegidas por perímetros de segurança definidos com barreiras e controles apropriados;

c) as informações relevantes ao IFMS armazenadas em sistemas de informação também deverão estar protegidas fisicamente de acesso não autorizado, danos e interferências.

XI - Segurança em recursos humanos

a) as responsabilidades pela segurança da informação devem ser definidas nas descrições de cargos e funções, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimentos do IFMS;

b) todos os usuários devem ser informados e conscientizados quanto aos procedimentos de segurança da informação;

c) o controle operacional de uma atividade crítica não pode ser atribuição exclusiva de uma única pessoa;

d) quando do afastamento, mudança de responsabilidades e de lotação ou atribuições dentro da organização faz se necessária a revisão imediata dos direitos de acesso e uso dos ativos;

e) quando da efetivação do desligamento de usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos a ele atribuído;

f) ações de segurança deverão garantir a operação segura e correta dos recursos de processamento da informação desta Autarquia.

XII - Gestão de operações e comunicações

a) o gerenciamento dos serviços terceirizados deverá manter os níveis apropriados de segurança da informação e da entrega dos serviços;

b) as informações e os recursos de processamento de informação deverão ter controles específicos que garantam a integridade e a disponibilidade dos mesmos;

c) as trocas de informações, tanto internamente, quanto externamente, deverão ser reguladas de forma a manter o nível adequado da segurança;

d) as operações deverão ser adequadamente monitoradas de forma a detectar atividades não autorizadas;

XIII - Criptografia: o(a) Gestor(a) de Segurança da Informação do IFMS é responsável pela implementação dos procedimentos relativos ao uso de recursos criptográficos, em conformidade com as orientações contidas em normas específicas.

XIV - Desenvolvimento de Software Seguro – DSS:

a) deverão ser identificados os responsáveis pela definição e validação dos requisitos de segurança que o software deva atender;

b) deverão ser definidos os requisitos de segurança para aplicação logo no início de qualquer projeto de desenvolvimento ou aquisição de software;

c) deverá ser definida a execução de testes pela contratada e homologação pelo IFMS antes da instalação do software em ambiente de produção;

d) deverá ser realizado teste de mesa do software desenvolvido por terceiros;

e) não será permitida a implantação de software se nele houver qualquer falha de segurança considerada crítica;

f) o tratamento das vulnerabilidades constitui um dos requisitos para a aceitação do sistema.

CAPÍTULO VI

Penalidades

Art. 15 O desrespeito, descumprimento ou violação de um ou mais itens constantes nesta PoSIC caracteriza infração funcional e resultará na suspensão temporária ou permanente de privilégios de acesso aos recursos de TIC, em penas e sanções legais impostas por meio de medidas administrativas sem prejuízo das demais medidas administrativas, cíveis e penais cabíveis.

CAPÍTULO VII

Competências e Responsabilidades

Art. 16 Compete ao Cosup a aprovação das diretrizes da PoSIC e suas regulamentações, que visam preservar a disponibilidade, integridade e confidencialidade das informações do IFMS.

Art. 17 O(A) Reitor(a) nomeará um(a) servidor(a) público(a) que atuará como Gestor(a) de Segurança da Informação e Comunicação (GSIC), sem ônus para o IFMS, com as seguintes competências:

I - promover a cultura de segurança da informação e comunicação;

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III - propor recursos necessários às ações de segurança da informação e comunicação;

IV - coordenar o Comitê de Segurança de Tecnologia da Informação e Comunicação e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

V - realizar e acompanhar estudos de novas tecnologias quanto a possíveis impactos na segurança da informação e comunicação;

VI - manter contato permanente e estreito com o Departamento de Segurança da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicação; e

VII - propor normas e procedimentos relativos à segurança da informação e comunicação no âmbito do órgão ou entidade da Administração Pública Federal.

Art. 18 Compete ao Comitê de Segurança de Tecnologia da Informação e Comunicação (CSTIC):

I - assessorar na implementação das ações de segurança da informação e comunicação no IFMS;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicação;

III - propor normas e procedimentos relativos à segurança da informação e comunicação no âmbito do IFMS; e

IV - revisar e analisar periodicamente esta política, diretrizes e as normas dela decorrentes, visando à sua aderência e concordância aos objetos do IFMS e às legislações vigentes.

Art. 19 É dever do grupo de trabalho constituído no inciso II, Art. 18:

I - investigar, diagnosticar e registrar os incidentes de segurança;

II - prover o tratamento do incidente de segurança, quando cabível;

III - reportar ao Comitê de Segurança de Tecnologia da Informação e Comunicação (CSTIC) o incidente e as providências tomadas, podendo propor medidas de prevenção a futuros incidentes.

Art. 20 O(A) Gestor(a) da Informação deve assegurar que os ativos:

I - sejam inventariados e protegidos;

II - tenham entrada e saída nas dependências da IFMS autorizadas e registradas por autoridade competente;

III - sejam passíveis de monitoramento, garantindo a rastreabilidade do seu uso;

IV - tenham identificados os seus custodiantes responsáveis;

V - sejam utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins, observando a legislação em vigor; e

VI - quando se tratarem de dispositivos portáteis, tenham registrada sua cessão.

Parágrafo único. Ocorrências como extravio ou roubo devem ser imediatamente comunicadas a um membro do Dirti/Serti, para que sejam registradas como incidente de segurança da informação, sem prejuízo das demais providências necessárias.

Art. 21 Aos gestores compete zelar pelo cumprimento das diretrizes da PoSIC.

Art. 22 A todos usuários compete:

I - conhecer a PoSIC e manter níveis de segurança adequados, seguindo as suas diretrizes e normas complementares.

II - adotar comportamento seguro, assumindo atitude proativa e engajada no que diz respeito à proteção das informações do IFMS.

CAPÍTULO VIII

Atualização

Art. 23 Esta PoSIC e todos os instrumentos normativos gerados a partir dela devem ser revisados sempre que se fizer necessário, não devendo exceder o período máximo de 3 (três) anos.

CAPÍTULO IX

Disposições Finais

Art. 24 Esta Política entra em vigor a partir da aprovação pelo Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul.

INSTITUTO FEDERAL
Mato Grosso do Sul

Rua Ceará, 972, Bairro Santa Fé – Campo Grande, MS – CEP: 79021-000
Telefone: (67) 3378-9501