RESOLUÇÃO Nº 87-COUN/UFMS, DE 9 DE ABRIL DE 2021.

Aprova a Política de Segurança da Informação da Fundação Universidade Federal de Mato Grosso do Sul.

O CONSELHO UNIVERSITÁRIO da Fundação Universidade Federal de Mato Grosso do Sul, no uso de suas atribuições legais, e tendo em vista o disposto no Decreto nº 9.637, de 26 de dezembro de 2008, e no Decreto nº 10.641, de 2 de março de 2021, e n a Instrução Normativa nº 1, de 27 de maio de 2020, do Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República, e considerando o contido no Processo nº 23104.009019/2021-91, resolve:

Art. 1º Fica aprovada a Política de Segurança da Informação da Fundação Universidade Federal de Mato Grosso do Sul (Posic/UFMS), na forma do Anexo a esta Resolução.

Art. 2º Esta Resolução entra em vigor em 3 de maio de 2021.

MARCELO AUGUSTO SANTOS TURINE,

Presidente.

Documento assinado eletronicamente por **Marcelo Augusto Santos Turine**, **Reitor(a)**, em 13/04/2021, às 14:27, conforme horário oficial de Mato Grosso do Sul, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufms.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2504472** e o código CRC **4599E952**.

POSIC
UFMS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

A NOSSA UNIVERSIDADE

POSIC

UFMS

**Resolução nº 87, COUN-UFMS,
de 9 de abril de 2021**

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

UFMS
A NOSSA UNIVERSIDADE

UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL

Reitor
Marcelo Augusto Santos Turine

Vice-Reitora
Camila Celeste Brandão Ferreira Ítavo

Pró-Reitor de Administração e Infraestrutura
Augusto Cesar Portella Malheiros
Pró-Reitor de Assuntos Estudantis
Albert Schiaveto de Souza
Pró-Reitor de Extensão, Cultura e Esporte
Marcelo Fernandes Pereira
Pró-Reitora de Gestão de Pessoas
Lívia Gaigher Bosio Campello
Pró-Reitor de Graduação
Cristiano Costa Argemon Vieira
Pró-Reitora de Pesquisa e Pós-Graduação
Maria Ligia Rodrigues Macedo
Pró-Reitora de Planejamento, Orçamento e Finanças
Dulce Maria Tristão

Agência de Comunicação Social e Científica
Rose Mara Pinheiro
Agência de Internacionalização e Inovação
Saulo Gomes Moreira
Agência de Educação Digital e a Distância
Hércules da Costa Sandim
Agência de Tecnologia da Informação e Comunicação
Luciano Gonda
Diretoria de Gabinete da Reitoria
Sabina Avelar Koga
Diretoria de Avaliação Institucional
Caroline Pauletto Spanhol Finocchio
Diretoria de Desenvolvimento Sustentável
Leonardo Chaves de Carvalho
Diretoria de Governança Institucional
Erotilde Ferreira dos Santos

Projeto Gráfico: Secretaria de Produção Visual/AGECOM

Sumário

1. Introdução

A informação e os processos de apoio, sistemas e infraestruturas de Comunicação e Informação são importantes ativos de patrimônio da UFMS, e devem ser apropriadamente protegidos. Todas as informações geradas no pleno exercício das atividades internas ou no desenvolvimento do trabalho externo, ou seja, fora dos limites físicos da organização, são consideradas parte do patrimônio da UFMS, devendo serem usadas exclusivamente para atender aos interesses da Instituição podendo, ainda, serem fornecidas a terceiros, respeitadas as restrições da classificação das informações. Todos os servidores, estudantes, terceiros autorizados, ou qualquer membro que possua vínculo direto ou indireto com a UFMS, são responsáveis pela segurança das informações da UFMS e devem atuar em conformidade com os princípios e diretrizes estabelecidos na Política de Segurança da Informação e Comunicação da UFMS (Posic-UFMS).

A Segurança da Informação e Comunicação pretende garantir a proteção da informação de vários tipos de ameaças, mantendo a continuidade dos negócios, minimizando os danos e, consequentemente, maximizando o retorno dos investimentos e as oportunidades de atuação da UFMS. O conceito de Segurança da Informação e Comunicação, que norteia este documento, baseia-se nas definições instituídas no Decreto nº 9.637, de 26 de dezembro de 2008, no Decreto nº 9.832, de 12 de junho de 2019, no Decreto nº 10.641, de 2 de março de 2021, e na Instrução Normativa nº 1, de 27 de maio de 2020.

A Posic-UFMS alinha-se às estratégias da Universidade, de forma a garantir a autenticidade, a confidencialidade, a disponibilidade e a integridade das informações produzidas ou custodiadas pela Instituição. A Posic-UFMS é fundamentada nos seguintes conceitos:

a) democracia: a segurança dos Sistemas de Informações deve ser compatível com os valores essenciais das sociedades democráticas;

b) cultura: os participantes devem edificar a Segurança da Informação e Cmunicação como um elemento primordial para sua organização;

c) confidencialidade: somente pessoas devidamente autorizadas devem ter acesso às informações institucionais;

d) integridade: somente alterações, supressões e adições autorizadas devem ser realizadas nas informações;

e) disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado;

f) autenticidade: garantia de que uma informação, produto ou documento é do autor a quem se atribui; e

g) não repúdio: é a garantia de segurança que impede uma entidade participante numa dada operação de negar essa participação.

Como benefícios da implementação da Posic-UFMS, espera-se obter:

a) posicionamento estratégico dos aspectos relacionadas à segurança da informação e comunicação;

b) estabelecimento de critérios sistêmicos relacionados ao tema;

c) garantia da interoperabilidade de uma maneira segura e buscando padronização entre os sistemas de informação institucionais;

d) possibilidade de adoção de soluções de segurança integradas no âmbito da UFMS;

e) aumento do nível de segurança da informação das Unidades da UFMS;

f) disseminação da cultura de Segurança da Informação e das suas normas no âmbito da UFMS;

g) padronização de procedimentos de Segurança da Informação e Comunicação entre as Unidades da UFMS;

h) aumento do nível de conformidade às normatizações de Segurança da Informação e Comunicação pelas entidades da UFMS; e

i) aumento do nível de conscientização em Segurança da Informação e Comunicação por parte dos Agentes Públicos e prestadores de serviço da UFMS .

2. Objetivos

A Posic-UFMS tem por objetivo principal formalizar o direcionamento estratégico acerca da Segurança da Informação e Comunicação, por meio da adoção dos seguintes objetivos específicos:

I - Assegurar a confidencialidade, a integridade, a autenticidade, o não repúdio e a disponibilidade dos dados e das informações tratadas e classificadas;

II - Eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos Sistemas de Informação; acompanhando, em âmbito nacional e internacional, a evolução doutrinária e tecnológica das atividades inerentes à Segurança da Informação e Comunicação;

III - Elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos e da Comunidade Universitária, visando garantir a Segurança da Informação e Comunicação;

IV - Promover manutenção de matérias afetas à segurança da informação, assim como aferir o nível de segurança dos respectivos Sistemas de Informação;as ações necessárias à implementação, regulamentação e

V - Promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de Segurança da Informação e Comunicação; e

VI - Estabelecer normas relativas à implementação dos Sistemas de Segurança da Informação, com vistas a garantir a sua interoperabilidade e a obtenção dos níveis de segurança desejados, assim como assegurar a permanente disponibilidade dos dados e das informações de interesse da Administração Pública Federal.

3. Princípios Gerais

Constituem como princípios gerais da Posic-UFMS:

I - Toda informação gerada ou recebida pelos servidores, colaboradores, fornecedores e prestadores de serviço, em consequência da função exercida e/ou atividade profissional contratada, pertence à UFMS. As exceções devem ser explícitas e formalizadas entre as partes por vias contratuais;

II - Todos os recursos de informação da UFMS devem ser projetados para que seu uso seja consciente e responsável. Os recursos de comunicação e computacionais da instituição devem ser utilizados para a consecução de seus objetivos finais;

III - Devem ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e Sistemas em que a instituição julgar necessário, objetivando a redução dos riscos dos seus ativos de informação;

IV - A Auditoria Interna Governamental da UFMS, a Corregedoria e os gestores dos Sistemas Computacionais poderão, pela característica de suas credenciais como usuários (privilégios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários. Tal operação só será permitida quando necessária para a execução de atividades operacionais sob sua responsabilidade;

V - Todo o acesso a redes e sistemas do órgão deverá ser feito, preferencialmente, por meio de login de acesso único, pessoal e intransferível;

VI - A UFMS pode utilizar tecnologias e ferramentas para monitorar e controlar o conteúdo e o acesso a quaisquer tipos de informação, alocadas na infraestrutura provida pela Instituição;

VII - Cada usuário será responsável pela segurança das informações que envolvem a UFMS, principalmente daquelas que estão sob sua responsabilidade e/ou carga patrimonial;

VIII - Deverão ser estabelecidos planos de contingência e de continuidade para os principais serviços e sistemas; tais planos devem ser revisados e testados periodicamente;

IX - Todos os requisitos de Segurança da Informação e Comunicação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução;

4. Responsabilidades

São responsabilidades gerais de todos os usuários e gestores de serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos computacionais da UFMS:

a) promover a segurança de seu usuário corporativo, setorial ou de rede local, bem como de seus respectivos dados e credenciais de acesso;

b) seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos computacionais e informacionais da UFMS;

c) utilizar de forma ética, legal e consciente os recursos computacionais e informacionais da UFMS; e

d) manter-se atualizado em relação a esta Posic e às normas e procedimentos relacionados, buscando informação com o Gestor de Segurança da Informação da Instituição, sempre que não estiver absolutamente seguro quanto à obtenção, uso e/ou descarte de informações.

4.1. Responsabilidades Específicas

RESPONSÁVEL	PERFIL ASSOCIADO	DESCRIÇÃO
USUÁRIO INTERNO	Servidores, estudantes e docentes contratados e voluntários.	Todos os servidores, gestores, técnicos, estagiários, bolsistas de programas educacionais, estudantes, consultores e colaboradores internos, que fazem uso dos recursos informacionais e computacionais da UFMS.
USUÁRIO EXTERNO	Prestadores de serviço e demais colaboradores externos e servidores aposentados.	Prestadores de serviços contratados direta ou indiretamente pela UFMS, visitantes e demais colaboradores externos que fazem uso de seus recursos informacionais e computacionais.
GESTORES	Coordenadores de Curso, Cargos de Direção e detentores de FG.	Todos aqueles que exercem funções de gerência no âmbito da organização, administrando pessoas e/ou processos.
ÁREA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Agência de Tecnologia da Informação e Comunicação (Agetic)	Unidade organizacional responsável pela gestão e operação dos recursos de TIC na organização e custo diante da informação.
GESTOR DE SI	Secretário de Serviços e Segurança da Informação	Servidor responsável pela gestão da segurança da informação em todos os seus aspectos.
EQUIPE TÉCNICA DE SI	Equipe técnica da Sein/Dintec/Agetic	Equipe técnica responsável por implementar e administrar as soluções de segurança da informação.
COMITÊ DE GOVERNANÇA DIGITAL	Alta Administração	Comitê Temático, responsável pelas decisões de alto nível relacionadas à gestão da Segurança da Informação.
AUDITORIA INTERNA GOVERNAMENTAL	Fiscalização/Auditoria	Equipe técnica responsável pela fiscalização e avaliação de Segurança da Informação e dos recursos informacionais.

4.1.1. Usuários internos e externos

Será de inteira responsabilidade de cada usuário (interno ou externo) todo prejuízo ou dano que vier a sofrer ou causar a UFMS em decorrência da não obediência às diretrizes e normas referidas na Posic-UFMS e nas normas e procedimentos específicos dela decorrentes.

Os usuários externos devem entender os riscos associados à sua condição e respeitar e cumprir rigorosamente as políticas, normas e procedimentos específicos vigentes. A UFMS poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento da Posic-UFMS ou das normas e procedimentos específicos dela decorrentes. O uso, manuseio e guarda de assinaturas de certificados digitais individuais será de responsabilidade de seus respectivos portadores.

4.1.2. Gestores

Os gestores da UFMS devem ter postura exemplar em relação à Segurança da Informação, diante, sobretudo, dos usuários sob sua gestão. Cada gestor deverá manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de Segurança da Informação da UFMS, tomando as ações necessárias para cumprir tal responsabilidade.

Deverá constar em todos os contratos da UFMS, quando o objeto for pertinente, cláusula de confidencialidade e de obediência às normas de Segurança da Informação a ser observada por empresas fornecedoras e por todos os profissionais que desempenham suas atividades na UFMS, inclusive provenientes de organismos internacionais;

Deverá estar prevista, por parte das empresas e profissionais prestadores de serviço, entrega de declaração expressa de compromisso em relação à confidencialidade e de Termo de Ciência das normas vigentes, como condição imprescindível para que possa ser concedido acesso aos ativos de informação disponibilizados pela Instituição;

4.1.3. Agência de Tecnologia da Informação e Comunicação

Compete à Agência de Tecnologia da Informação e Comunicação (Agetic):

a) implementar ações de Segurança da Informação;

b) propor grupos de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação;

c) zelar pela eficácia dos controles de Segurança da Informação utilizados e informar aos gestores e demais interessados os riscos residuais;

d) negociar e acordar com os gestores os níveis de serviço relacionados à Segurança da Informação, incluindo os procedimentos de resposta a incidentes;

e) configurar os recursos de TIC concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos pelos procedimentos, normas e Posic;

f) criar e manter trilhas para auditoria, com nível de detalhe o bastante para rastrear possíveis falhas e fraudes; para as trilhas geradas e/ou mantidas em meio eletrônico, devem ser implantados controles de integridade, de modo a torná-las juridicamente válidas como evidências;

g) garantir nível satisfatório de segurança para Sistemas com acesso público, realizando guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;

h) zelar pela segregação de funções gerenciais e operacionais, a fim de restringir ao mínimo necessário os privilégios de cada indivíduo e eliminar a existência de pessoas que possam excluir logs e trilhas de auditoria das suas próprias ações;

i) administrar, proteger e testar cópias de segurança de Sistemas e dados relacionados aos processos

considerados críticos para a UFMS;

j) implantar controles que gerem registros auditáveis para retirada e transporte de mídias que contenham informações custodiadas pela TIC, nos ambientes totalmente controlados por ela;

k) planejar, implantar, fornecer e monitorar a capacidade de armazenamento, processamento e transmissão necessários para garantir a segurança requerida pelas áreas internas da organização;

l) atribuir cada conta ou dispositivo de acesso a computadores, Sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, responsável pelo uso da conta (a responsabilidade pela gestão dos logins de usuários externos é do gestor do contrato de prestação de serviços ou do gestor do setor em que o usuário externo desempenha suas atividades);

m) proteger continuamente todos os ativos de informação da UFMS contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado;

n) assegurar-se de que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da UFMS ou em fase de mudança de ambiente de desenvolvimento, teste, homologação ou produção de sistemas (quando tais ambientes forem acessados por terceiros, a responsabilização deve ser explicitada nas cláusulas dos instrumentos contratuais);

o) definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional e/ou dedicados à visitação externa, exigindo o seu cumprimento dentro da Universidade;

p) definir metodologia e realizar auditorias periódicas de configurações técnicas e análise de riscos;

q) responsabilizar-se pelo uso, manuseio, guarda de assinatura de Certificados digitais corporativos utilizados nos serviços de TIC oferecidos pela UFMS;

r) garantir, após recebimento de solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da UFMS, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Universidade; e

s) monitorar o ambiente de TIC, gerando indicadores e históricos de uso da capacidade instalada da rede e dos equipamentos; tempo de resposta no acesso à internet e aos sistemas críticos; períodos de indisponibilidade no acesso à internet e aos sistemas críticos; incidentes de segurança.

4.1.4. Gestor de Segurança da Informação

Compete ao Gestor de Segurança da Informação da UFMS, representado pelo Secretário de Serviços e Segurança da Informação – Sein/Dintec/Agetic:

a) promover cultura de Segurança da Informação, no âmbito de suas atribuições dentro da UFMS;

b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

c) propor recursos necessários às ações de Segurança da Informação;

d) realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na Segurança da Informação;

e) manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República;

f) propor normas internas relativas à Segurança da Informação; e

g) estabelecer normas, padrões e demais aspectos necessários para assegurar a confidencialidade dos dados e das informações, do uso dos recursos criptográficos, dando-se preferência, em princípio, no

emprego de tais recursos, a produtos manufaturados de origem nacional; em vista da possibilidade de interceptações de transmissões com fio e sem fio, inclusive proveniente de recursos computacionais.

4.1.5. Equipe Técnica de Segurança da Informação

Compete à Equipe Técnica de Segurança da Informação, que é composta pela equipe da Sein/Dintec/Agetic:

a) propor metodologias e processos específicos para a Segurança da Informação, como classificação da informação e avaliação de risco;

b) propor e apoiar iniciativas que visem a segurança dos ativos de informação da UFMS;

c) auxiliar na publicação e promoção da Posic-UFMS, das normas, e procedimentos específicos decorrentes, aprovados pelo Comitê de Gestão Digital;

d) Promover a conscientização dos usuários em relação à relevância da segurança da informação para a UFMS, mediante campanhas, palestras, treinamentos e outros meios de divulgação interna;

e) apoiar a avaliação e a adequação de controles específicos de Segurança da Informação para novos sistemas ou serviços;

f) manter comunicação efetiva com o Comitê de Gestão Digital sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar o órgão;

g) buscar alinhamento das práticas de Segurança da Informação com as diretrizes corporativas da Instituição;

h) atuar, quando necessário, com atribuições da Equipe de Tratamento de Incidentes Cibernéticos - ETIR;

4.1.6. Comitê de Governança Digital

Compete ao Comitê de Gestão Digital:

a) estabelecer grupos de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação;

b) propor, aprovar, alterar e revisar a Posic-UFMS e normas complementares e procedimentos internos de Segurança da Informação, em conformidade com a legislação existente sobre o tema; e

c) subsidiar a Agetic nas decisões relativas à Segurança da Informação.

4.1.7. Auditoria Interna

É de Responsabilidade da Auditoria Interna Governamental:

a) realizar trabalho de avaliação das ações de Segurança da Informação da UFMS, e da eficiência dos Sistemas e recursos informacionais; e

b) solicitar acesso à área de TIC aos Sistemas e Informações Institucionais, para subsidiar trabalhos de auditoria no âmbito de sua competência.

5. Controle de Acesso

O Controle de Acesso visa estabelecer critérios para a disponibilização e administração do acesso aos serviços de TIC da UFMS levando em consideração os seguintes itens:

a) O acesso à rede e demais Sistemas da UFMS 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 da UFMS, observando-se a necessidade de utilização para a realização de suas atividades, e a respectiva autorização por parte dos responsáveis por estes Sistemas;

c) para o ingresso aos recursos da rede UFMS, o usuário deverá ser cadastrado, possuindo assim o Passaporte UFMS (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) o usuário deverá assinar o Termo de Responsabilidade, estando ciente, dessa forma, que terá pleno conhecimento dos termos e condições explicitados ou referidos pelo documento de Normas de Utilização dos Recursos de Tecnologia da Informação e Comunicação da UFMS;

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 Passaporte UFMS do usuário poderá ser bloqueado, em casos de incidentes de Segurança da Informação causados por ele. A conta será restabelecida após a solução dos problemas causados e reorientação ao usuário, desde que não existam outros impedimentos;

h) a Agetic poderá restringir as pessoas que poderão ser administradoras dos respectivos equipamentos computacionais patrimoniados da UFMS;

i) poderá ser feito o cadastro da conta de acesso, para usuário visitante, desde que solicitado pelo responsável do setor onde realizará suas atividades, informando para Agetic o prazo de validade para a conta a ser criada;

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

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

l) o acesso à Rede sem fio disponibilizada em áreas de estudo estará disponível aos usuários da UFMS, sendo necessária sua identificação por meio do Passaporte UFMS, para a realização de estudos e pesquisas;

m) as credenciais de acesso à Rede e demais Sistemas devem ser canceladas após o desligamento do usuário da UFMS pelos setores responsáveis;

n) o acesso fornecido a instituições que utilizarem a Rede da UFMS 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 atendendo, no mínimo, aos controles definidos na Posic-UFMS;

o) 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 considerada crime, previsto na Lei nº 9.609, de 19 de fevereiro de 1998.

6. Tratamento da Informação

Tratamento da informação define os requisitos e regras para classificação e tratamento da informação no ambiente de tecnologia da UFMS, 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 da UFMS (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, entre 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.

7. Monitoramento

Para garantir a aplicação das diretrizes mencionadas nesta Posic, além de fixar normas e procedimentos complementares sobre o tema, a Agetic poderá:

a) implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de modo que a informação gerada por esses Sistemas possa ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

b) tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Governança Digital;

c) realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade;

d) instalar sistemas de proteção, preventivos e detectáveis, para garantir segurança das informações e dos perímetros de acesso;

e) desinstalar, a qualquer tempo, qualquer software ou sistema que represente risco ou esteja em desconformidade com as políticas, normas e procedimentos vigentes.

8. Centro de Dados (Data Center)

A administração do centro de dados será realizada por Técnicos e Analistas de TI da UFMS autorizados e capacitados. O centro de dados fica localizado na Agetic ~~da~~ e tem posição estratégica. O centro de dados deve estar protegido de pessoas e acessos não autorizados, bem como de condições climáticas adversas que possam causar danos à sua estrutura.

Os acessos de pessoas ao centro de dados deverão ser realizados por um sistema de autenticação forte. O acesso por chaves será realizado apenas em situações de emergência, ou enquanto a infraestrutura não permitir a implantação da tecnologia de autenticação. Situações de emergência podem incluir incêndio, inundação, comprometimento da estrutura do prédio ou mau funcionamento do sistema de autenticação.

Todos os acessos realizados por pessoas consideradas visitantes ou terceiros deverão ser realizados por meio de acompanhamento de um servidor da Agetic autorizado. Com a infraestrutura de autenticação no centro de dados, todos os acessos também deverão ser auditados periodicamente por meio dos relatórios disponíveis no sistema de registro.

Servidores que não tiverem mais vínculo com prestação de serviço da Agetic terão as vias de acesso revogadas (senha, chaves, etc.). Os usuários com acesso autorizado ao centro de dados são os responsáveis diretos por qualquer acesso ou processo não autorizado que venha a comprometer os dados e a infraestrutura deste. Os procedimentos para a administração do centro de dados deverão ser fixados em norma própria a serem publicadas posteriormente. Por ser uma tarefa não trivial em seu sentido técnico, deve-se levar em consideração as melhores práticas de mercado, incluindo a alocação de profissionais com perfil técnico adequado.

9. Gestão de Incidentes em Segurança da Informação

A Gestão de Incidentes em Segurança da Informação é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas, e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

Na gestão de incidentes de Segurança da Informação, o responsável pelo tratamento e resposta ao incidente, deverá considerar, no mínimo, as seguintes diretrizes:

a) todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades desenvolvidas;

b) O tratamento da informação deverá ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo e;

c) durante o gerenciamento de incidentes de segurança, havendo indícios de ilícitos criminais, o Gestor de Segurança da Informação ou membros da Equipe Técnica de Segurança da Informação tem como dever, sem prejuízo de suas demais atribuições, acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários, observar os procedimentos para preservação das evidências, exigindo consulta às orientações sobre cadeia de custódia, e priorizar a continuidade dos serviços da Instituição.

10. Gestão de Ativos

A Gestão de Ativos na UFMS é norteada pela Política de Gestão de Ativos da UFMS vigente.

11. Gestão do Uso dos Recursos Operacionais e de Comunicações

A Gestão de Usos dos Recursos Operacionais e de Comunicações na UFMS é realizada por meio dos seguintes atos normativos: Norma para Uso dos Recursos de Tecnologia da Informação e Comunicação (TIC); e Política de Comunicação.

12. Obrigações e Penalidades

O descumprimento das disposições pertinentes da Política e nas Normas Complementares sobre Segurança da Informação caracteriza infração funcional, a ser averiguada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

O usuário que realizar uso de forma indevida ou não autorizada dos Recursos de Tecnologia da Informação, bem como agir em desacordo com os termos desta Política, ficará sujeito à aplicação das penalidades previstas na Lei 8.112, de 11 de dezembro de 1990, e demais legislações pertinentes.

13. Disposições Finais

A Posic-UFMS deverá ser difundida a todos os usuários e gestores na UFMS, com a finalidade de assegurar melhor gestão dos ativos de informação organizacional, garantindo todos os aspectos no âmbito da Segurança da Informação.

Esta política deverá ser atualizada a cada quatro anos ou sempre que houver necessidade de alteração. Os casos omissos deverão ser submetidos à Agetic e ao Comitê de Gestão Digital da UFMS.

UFMS
A NOSSA UNIVERSIDADE

www.ufms.br /ufmsbr @ufmsoficial

Educativa UFMS @ufmsbr /tvufms