RESOLUÇÃO Nº 333, DE 21 DE MARÇO DE 2024. (*)

Aprova a Política de Segurança da Informação da Fundação Universidade Federal de Mato Grosso do Sul - PSI/UFMS.

O CONSELHO UNIVERSITÁRIO da Fundação Universidade Federal de Mato Grosso do Sul, o 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 na 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 23104.038008/2023-81, resolve:

Art. 1º Fica aprovada a Política de Segurança da Informação da Fundação Universidade Federal de Mato Grosso do Sul - PSI/UFMS-2024-2028, na forma do Anexo a esta Resolução.

Art. 2º Fica revogada a Resolução nº 222, de 16 de setembro de 2022.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

MARCELO AUGUSTO SANTOS TURINE,

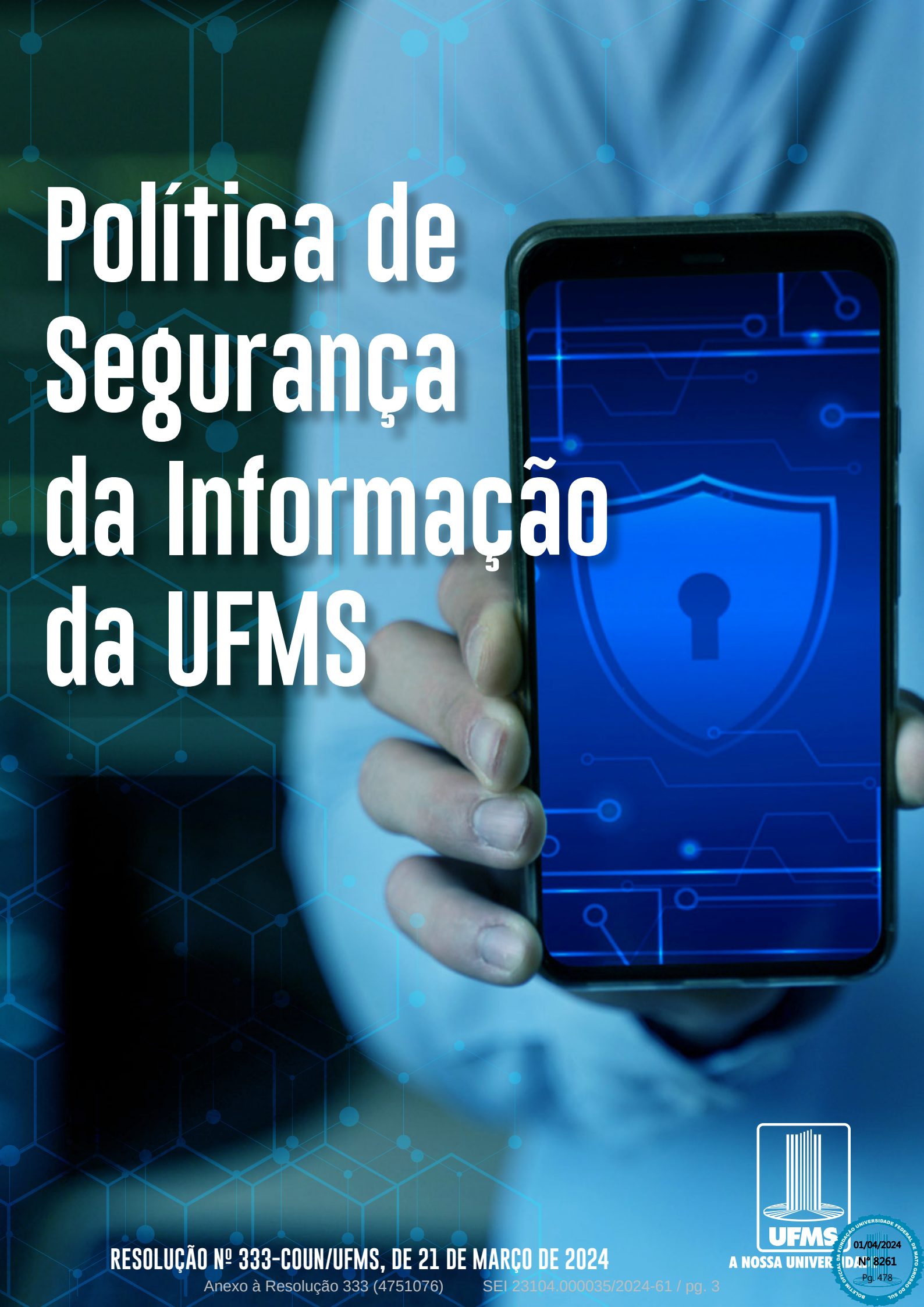
Presidente.

(*) Republicada por ter constado incorreção, quanto ao original, na Edição nº 8.257 do Boletim Oficial da UFMS, de 25-03-2024.

Documento assinado eletronicamente por **Marcelo Augusto Santos Turine**, **Presidente de Conselho**, em 26/03/2024, às 20:29, conforme horário oficial de Mato Grosso do Sul, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

CONSELHO UNIVERSITÁRIO
Av Costa e Silva, s/nº - Cidade Universitária
Fone: (67) 3345-7041
CEP 79070-900 - Campo Grande - MS

Política de Segurança da Informação da UFMS



RESOLUÇÃO Nº 333-COUN/UFMS, DE 21 DE MARÇO DE 2024

UFMS
A NOSSA UNIVERSIDADE

UNIDADES DA ADMINISTRAÇÃO CENTRAL
Reitoria
Marcelo Augusto Santos Turine
Vice-Reitoria
Camila Celeste Brandão Ferreira Ítavo
Pró-Reitoria de Administração e Infraestrutura
Augusto Cesar Portella Malheiros
Pró-Reitoria de Assuntos Estudantis
Albert Schiaveto de Souza
Pró-Reitoria de Extensão, Cultura e Esporte
Marcelo Fernandes Pereira
Pró-Reitoria de Gestão de Pessoas
Gislene Walter da Silva
Pró-Reitoria de Graduação
Cristiano Costa Argemon Vieira
Pró-Reitoria de Pesquisa e Pós-Graduação
Maria Ligia Rodrigues Macedo
Pró-Reitoria de Planejamento, Orçamento e Finanças
Dulce Maria Tristão

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

UNIDADES DA ADMINISTRAÇÃO SETORIAL
Escola de Administração e Negócios
Claudio César da Silva
Faculdade de Artes, Letras e Comunicação
Gustavo Rodrigues Penha
Faculdade de Ciências Farmacêuticas, Alimentos e Nutrição
Fabiane La Flor Ziegler Sanches
Faculdade de Ciências Humanas
Vivina Dias Sol Queiroz
Faculdade de Computação
Henrique Mongelli
Faculdade de Direito
Fernando Lopes Nogueira
Faculdade de Educação
Milene Bartolomei Silva
Faculdade de Engenharias, Arquitetura e Urbanismo e Geografia
Robert Schiaveto de Souza
Faculdade de Medicina
Marcelo Luiz Brandão Vilela
Faculdade de Medicina Veterinária e Zootecnia
Fabrício de Oliveira Frazilio
Faculdade de Odontologia
Fabio Nakao Arashiro
Instituto de Biociências
Ramon José Correa Luciano de Mello
Instituto de Física
Além-Mar Bernardes Gonçalves
Instituto Integrado de Saúde
Marcos Antonio Ferreira Júnior
Instituto de Matemática
Bruno Dias Amaro
Instituto de Química
Carlos Eduardo Domingues Nazário

Câmpus de Aquidauana
Ana Graziele Lourenço Toledo
Câmpus de Chapadão do Sul
Kleber Augusto Gastaldi
Câmpus de Coxim
Silvana Aparecida da Silva Zanchett
Câmpus de Naviraí
Marco Antonio Costa da Silva
Câmpus de Nova Andradina
Solange Fachin
Câmpus de Paranaíba
Wesley Ricardo de Souza Freitas
Câmpus de Ponta Porã
Leonardo Souza Silva
Câmpus do Pantanal
Aguinaldo Silva
Câmpus de Três Lagoas
Larissa da Silva Barcelos

UNIDADE SUPLEMENTAR
Hospital Universitário
Maria Aparecida Pedrossian (Humap/Ebserh)
Andréia de Siqueira Campos Lindenberg

Sumário

1. Introdução

A informação e os processos de apoio, sistemas e infraestruturas de informação são importantes ativos de patrimônio da UFMS, e devem ser apropriadamente protegidos. Todas as informações geradas no pleno exercício das atividades ou no desenvolvimento do trabalho, dentro ou fora dos limites físicos da organização, são consideradas parte do patrimônio da UFMS, devendo ser usadas exclusivamente para atender aos interesses da Instituição. 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 da UFMS (PSI/UFMS) e de leis e normativos vigentes.

A Segurança da Informação visa 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, Instrução Normativa nº 1, de 27 de maio de 2020, no Decreto nº 10.641, de 2 de março de 2021 e no Decreto nº 10.748 de 16 de Julho de 2021. O PSI/UFMS segue as recomendações dos Órgãos nacionais relacionados à Segurança da Informação como o CTIR Gov (Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo) e atende às normas da Política Nacional de Segurança da Informação - PNSI.

A PSI/UFMS alinha-se ao Projeto de Desenvolvimento Institucional integrado ao Projeto Pedagógico Institucional da UFMS, de forma a garantir a autenticidade, a confidencialidade, a disponibilidade e a integridade das informações produzidas ou custodiadas pela Instituição. A PSI/UFMS é fundamentada nos seguintes conceitos:

a. cultura organizacional: a Segurança da Informação é primordial para a cultura da instituição;
b. confidencialidade: somente pessoas devidamente autorizadas devem ter acesso às informações institucionais;
c. integridade: somente alterações, supressões e adições autorizadas devem ser realizadas nas informações;
d. disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado;
e. autenticidade: garantia de que uma informação, produto ou documento é do autor a quem se atribui; e
f. não repúdio: é a garantia de segurança que impede que uma pessoa jurídica ou física participante de uma operação negue sua participação.

Como benefícios da implementação da PSI/UFMS, espera-se obter:

a. posicionamento estratégico institucional;
b. estabelecimento de critérios sistêmicos e adoção de soluções de segurança integradas;
c. garantia segura de interoperabilidade e padronização entre os sistemas de informação institucionais;
d. disseminação da cultura e das normas e padronização de procedimentos de Segurança da Informação;
e. aumento do nível de conformidade às normatizações de Segurança da Informação e aumento do nível de segurança da informação; e
f. fortalecimento da conscientização em Segurança da Informação por parte da comunidade universitária.

2. Objetivos

A PSI/UFMS tem por objetivo principal formalizar o direcionamento estratégico acerca da Segurança da Informação, 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. Elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos e da Comunidade Universitária, visando garantir a Segurança da Informação no âmbito da UFMS;

III. Promover manutenção de matérias afetas à Segurança da Informação, assim como aferir o nível de segurança dos Sistemas de Informação e implementar as ações necessárias à implementação;

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

V. 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

Constituem como princípios gerais da PSI/UFMS:

I. Toda informação gerada ou recebida por qualquer pessoa, em consequência da função exercida e/ou atividade profissional contratada, pertence à UFMS, sendo que em caso de exceção deverá estar formalizado em instrumento jurídico;

II. Todos os recursos de TIC da UFMS devem ser projetados para uso consciente e responsável e devem ser utilizados para a consecução da missão institucional;

III. Devem ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas necessários, para redução dos riscos dos ativos de informação; com detecção de vulnerabilidades pró-ativa;

IV. A Auditoria Interna Governamental, a Corregedoria e os gestores dos Sistemas Computacionais possuem, pelas credenciais como usuários, permissão para acessar arquivos e dados de outros usuários, quando tal atividade for necessária para a execução de atividades operacionais sob sua responsabilidade;

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

VI. Utilização de 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; com revisão e testagem periódica;

IX. Todos os requisitos de Segurança da Informação e Comunicação devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implementados e testados durante a fase de execução;

X. O conceito de Segurança por Design deve ser aplicado nos sistemas gerados e/ou mantidos pela UFMS; e

XI. Todos os ativos de TIC devem ser mantidos sempre atualizados conforme as boas práticas de Segurança da Informação.

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 e de informação da UFMS:

a. promover a segurança do usuário, bem como de seus respectivos dados e credenciais de acesso;

b. seguir, de forma colaborativa, as orientações 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 PSI 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	DESCRIÇÃO
USUÁRIO	Todos aqueles que utilizam serviços digitais da UFMS.
GESTORES	Todos aqueles que exercem funções de gerência no âmbito da organização, administrando pessoas e/ou processos.
ÁREA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Unidade organizacional responsável pela gestão e operação dos recursos de TIC na organização e customização da informação.
GESTOR DE SI	Servidor responsável pela gestão da segurança da informação em todos os seus aspectos.
COMITÊ DE GOVERNANÇA DIGITAL	Comitê Temático, responsável pelas decisões de alto nível relacionadas à gestão de Tecnologia da Informação e Comunicação, incluindo Segurança da Informação.
AUDITORIA INTERNA GOVERNAMENTAL	Equipe técnica responsável pela fiscalização e avaliação de Segurança da Informação e dos recursos informacionais.
EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS	Equipe técnica responsável pelo tratamento de incidentes cibernéticos com o objetivo de conter, tratar, responder, erradicar e orientar sobre o incidente de segurança da informação e comunicação na Rede UFMS, em tempo compatível a sua natureza, visando assegurar a continuidade dos serviços de TIC para o alcance dos objetivos institucionais.

4.1.1. Usuários

Será de inteira responsabilidade do 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 PSI/UFMS e nas normas e procedimentos específicos.

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 PSI/UFMS ou das normas e procedimentos específicos dela decorrentes. O uso, manuseio e guarda de assinaturas de certificados digitais individuais, físicos ou digitais, e do Passaporte UFMS, com login e senha, será de responsabilidade do detentor.

4.1.2 Gestores

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, diante, sobretudo, dos usuários sob sua gestão.

Deverá constar em todos os instrumentos jurídicos com empresas fornecedoras e por toda pessoa física ou jurídica, brasileira ou estrangeira, que desempenhe suas atividades na UFMS, quando pertinente, cláusula de confidencialidade e de obediência às normas de Segurança da Informação.

Deverá estar prevista, por parte das empresas e profissionais prestadores de serviço, a 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 PSI;

f. criar e manter trilhas para auditoria em meio eletrônico, realizando guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação, de acordo com as normas vigentes;

g. 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 indivíduos que possam excluir logs e trilhas de auditoria das suas próprias ações;

h. administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos considerados críticos para a UFMS;

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

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

k. 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, sendo a responsabilidade pelos usuários externos do setor solicitante;

l. 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;

m. 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, o que deve estar no contrato com terceiros, quando for o caso,

n. definir as regras formais para instalação de software e hardware em ambiente de produção, bem como em ambiente exclusivamente educacional e/ou dedicados à visitação externa;

o. definir metodologia e realizar auditorias periódicas de configurações técnicas e análise de riscos;

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

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

r. 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; e demais incidentes de segurança.

4.1.4. Diretor da Agetic

Compete ao Diretor da Agetic:

a. emitir ato formalizando a criação ato de constituição da ETIR/UFMS;

b. indicar e designar o Gestor de Segurança da Informação;

c. coordenar a preparação da infraestrutura necessária à ETIR/UFMS;

d. criar, revisar, aprovar, revogar, divulgar as definições das atribuições e das responsabilidades dos membros da ETIR/UFMS, além das normas, dos processos e dos subprocessos que orientarão as atividades e os trabalhos da Equipe;

e. acompanhar as investigações e as avaliações dos danos decorrentes de quebras e violações de segurança da informação;

f. revisar e submeter às instâncias superiores, para análise e aprovação, as estratégias e os processos de tratamento e resposta a incidentes cibernéticos e os processo de coleta e preservação de evidências propostos pela ETIR/UFMS e pela área de segurança da Agetic;

g. encaminhar os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação à Alta Administração e ao Comitê de Governança Digital da UFMS - CGD/UFMS, e, quando for o caso, remissão ao Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR GOV;

h. interagir com os Grupos de Coordenação de Resposta a Incidentes Cibernéticos - CSIRTs de Coordenação, de acordo com os protocolos estabelecidos pela UFMS;

i. prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos integrantes da Equipe; e

j. administrar os indícios de ilícitos criminais no que se refere a incidentes cibernéticos, formalizando e comunicando à autoridade máxima da UFMS para a adoção dos procedimentos legais necessários com base nos normativos vigentes de segurança da informação.

4.1.5. Gestor de Segurança da Informação

Compete ao Gestor de Segurança da Informação da UFMS:

a. promover cultura de Segurança da Informação na 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 com o Gabinete de Segurança Institucional da Presidência da República - GSI/PR e interagir com os Grupos de Coordenação de Resposta a Incidentes Cibernéticos - CSIRTs;

f. propor normas internas relativas à Segurança da Informação;

g. coordenar e gerenciar as atividades da ETIR/UFMS, inclusive as atividades de caráter proativo para cumprimento da missão, com definição do ferramental tecnológico de apoio técnico-gerencial,;

h. elaborar e manter atualizado os processos e procedimentos internos da ETIR/UFMS no gerenciamento de incidentes cibernéticos;

i. utilizar metodologia e melhores práticas no tratamento e resposta a incidentes cibernéticos, assim como na coleta e preservação de evidências para fins forenses e de conformidade à legislação do Governo Federal;

j. identificar as necessidades de capacitação e, se necessário, treinar os integrantes da ETIR/UFMS; e

k. intermediar a comunicação com o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR GOV, ETRIC/ETIR de outros órgãos da Administração Pública Federal e com o Centro de Atendimento a Incidentes de Segurança – CAIS/RNP.

4.1.6. Comitê de Governança Digital

Compete ao Comitê de Governança 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 PSI/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 Governamental

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.

4.1.8. Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes Computacionais

É de Responsabilidade da Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR/UFMS):

a. receber, analisar e responder às notificações e atividades relacionadas a incidentes cibernéticos;

b. prestar o serviço de tratamento de incidentes cibernéticos com o objetivo de conter, tratar, responder, erradicar e orientar sobre o incidente de Segurança da Informação na rede de dados da UFMS, em tempo compatível a sua natureza, visando assegurar a continuidade dos serviços de TIC;

c. atuar nas atividades de resposta a incidentes de segurança da informação na rede UFMS, provendo atendimento a todas as Unidades e ao público externo, no gerenciamento da segurança cibernética;

d. agir proativamente para evitar que ocorram incidentes de segurança da informação, divulgando práticas e recomendações e avaliando as condições de segurança da Rede UFMS por meio de verificações sistêmicas de conformidade e identificação de vulnerabilidades e artefatos maliciosos;

e. realizar ações reativas que incluem recebimento de notificações de incidentes cibernéticos, atuando no reparo aos danos causados e no restabelecimento dos serviços de TIC e sistemas comprometidos, com investigação das causas, danos e responsáveis e recomendação de procedimentos ou medidas de recuperação a serem adotados durante um incidente de segurança;

f. disponibilizar relatórios gerenciais periodicamente ou quando solicitado pelo Diretor da Agetic ou pelo Gestor de Segurança da Informação;

g. cooperar com outras ETIRs de acordo com acordo de cooperação estabelecidos pela UFMS;

h. manter contato com o Gabinete de Segurança Institucional da Presidência da República - GSI/PR e com o CTIR Gov – Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo concernente a assuntos de segurança cibernética; e

i. subsidiar o Gestor de Segurança da Informação, o Diretor da Agetic e o Comitê de Governança Digital da UFMS com informações e evidências apuradas quando da suspeita de ocorrências de quebras de segurança e/ou violações de segurança da informação e comunicação.

5. Diretrizes

Para um melhor gerenciamento da Segurança da Informação na UFMS, é importante se atentar para as diretrizes descritas nas Seções 5.1 a 5.10, que estão alinhadas com a Instrução Normativa nº 1, de 27 de maio de 2020 do GSI/PR.

5.1. Tratamento da Informação

Tratamento da informação define os requisitos e regras para classificação e tratamento da informação no ambiente de tecnologia da UFMS, considerando que:

a. arquivos fundamentais para as atividades institucionais deverão ser salvos em drives de rede da UFMS, pois a gravação local não garante backup, sendo 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 da UFMS, pois podem sobrecarregar o armazenamento nos servidores ou ferir direitos autorais. Caso se.jam identificados, esses arquivos serão excluídos definitivamente sem necessidade de comunicação prévia ao usuário; e

c. classificação de informações, acesso à informação, uso e descarte de ativos de informação, entre outros temas afins, ocorrem em estrita aderência às leis e normas atinentes à Administração Pública Federal, considerando o Decreto nº 7.724, de 16 de maio de 2012.

As informações produzidas ou custodiadas pela Universidade serão classificadas em função do seu grau de confidencialidade, disponibilidade, integridade e prazo de retenção conforme for estabelecido pelo gestor da informação, pelo Comitê de Governança Digital, e/ou por quem receber a delegação para definir as classificações, de acordo com as normas da UFMS e legislação em vigor.

Quando um conjunto de informações não puder sofrer fracionamento para fins de acesso deverá ser atribuído o grau de confidencialidade da sua parte cuja classificação seja a mais restritiva.

As instalações de infraestrutura computacional, de armazenamento de dados, de rede e telecomunicações, deverão ser planejadas, operacionalizadas e continuamente monitoradas, observando:

- sistemas de proteção física para mitigar o risco de acesso não autorizado;
- sistema alternativo de provisão de energia elétrica;
- proteção contra descargas elétricas e atmosféricas;
- planos e sistemas de proteção contra incêndio e outros sinistros;
- sítio alternativo que garanta a disponibilidade do sistema em caso de sinistro; e
- utilização de infraestrutura de redes e telecomunicações seguras.

As informações produzidas e/ou custodiadas pela UFMS são classificadas quanto à disponibilidade em função do impacto que a indisponibilidade da informação acarretaria à imagem ou às operações vitais das atividades finalísticas da Universidade. Esse impacto deve ser classificado como:

- baixo: quando a indisponibilidade ou interrupção de acesso não comprometer a imagem ou as operações vitais ao negócio da Universidade, nem causar qualquer tipo de perda ou dano à Universidade;
- médio: quando a indisponibilidade ou interrupção de acesso comprometer a imagem, a tomada de decisões ou a produtividade das operações vitais ao negócio da Universidade, mas sem interrompê-las, ou causar perda ou dano à Universidade;
- alto: quando a indisponibilidade ou interrupção de acesso comprometer severamente a imagem ou as operações vitais ao negócio da Universidade, ou causar perda ou dano severo à Universidade.

As informações produzidas e/ou custodiadas pela UFMS são classificadas quanto à integridade em função do impacto que a alteração, inclusão ou exclusão indevida ou não autorizada da informação acarretaria à imagem ou às operações vitais ao negócio da Universidade. Esse impacto deve ser classificado como:

- baixo: quando a perda de integridade não comprometer a imagem ou as operações vitais ao negócio da Universidade, nem causar qualquer tipo de perda ou dano à Universidade;
- médio: quando a perda de integridade comprometer a imagem, a tomada de decisões ou a produtividade das operações vitais ao negócio da Universidade, mas sem interrompê-las, ou causar perda ou dano à Universidade;
- alto: quando a perda de integridade comprometer severamente a imagem ou as operações vitais ao negócio da Universidade, ou causar perda ou dano severo à Universidade.

Em caso de compartilhamento de informações, todas as informações compartilhadas no âmbito da UFMS devem utilizar o padrão Traffic Light Protocol (TLP) v. 2.0 para sinalização do acesso que for autorizado, conforme definido pelo Forum of Incident Response and Security Teams (FIRST), de maneira que as informações que possuam as designações CLEAR, GREEN, AMBER, AMBER+STRICT ou RED, conforme indicado no padrão TLP, deverão ser tratadas da maneira apropriada.

O tratamento da informação deve seguir a Política de Privacidade e Proteção de Dados no âmbito da UFMS e a legislação vigente.

5.2. Segurança Física e do Ambiente

A UFMS possui um centro de dados localizado na Agetic, em posição estratégica, e está protegido de pessoas e acessos não autorizados e mantido e operado por Técnicos e Analistas de TI da UFMS.

O acesso de pessoas ao centro de dados é realizado por um sistema de autenticação biométrica e os logs de acesso são armazenados e passíveis de auditoria. 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. Servidores que não tiverem mais vínculo com prestação de serviço da Agetic terão as vias de acesso revogadas (senha, chaves, etc.).

Todos os acessos de visitantes ou terceiros deverão ser realizados por meio de acompanhamento de um servidor da Agetic autorizado, mediante assinatura de termo de acesso e com anuência de pelo menos um dos Diretores da AGETIC.

O centro de dados possui um sistema de videomonitoramento, monitoramento de condições climáticas adversas que possam causar danos à sua estrutura, sistema de energia ininterrupta e gerador em caso de falhas de energia da concessionária.

5.3. Gestão de Incidentes em Segurança da Informação

A Gestão de Incidentes em Segurança da Informação será realizada pela Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes Computacionais da UFMS - ETIR/UFMS, que é subordinada à Agetic.

É missão da ETIR/UFMS prestar o serviço de tratamento de incidentes cibernéticos com o objetivo de conter, tratar, responder, erradicar e orientar sobre o incidente de segurança da informação na rede UFMS em tempo compatível a sua natureza, visando assegurar a continuidade dos serviços digitais para o alcance dos objetivos institucionais.

5.3.1. Formação e Atuação da ETIR

A ETIR/UFMS será estabelecida segundo o Modelo de Implementação nº 1, da Norma Complementar nº 05/IN01/DSIC/GSIC/PR, e será composta por servidores efetivos da Agetic, de diversas áreas, em caráter multidisciplinar, com conhecimento, habilidades e experiência técnica compatíveis com a missão, e que, além de suas funções regulares, desempenhem atividades relacionadas ao tratamento e resposta a incidentes cibernéticos na rede UFMS.

A ETIR/UFMS será constituída por integrantes titulares, suplentes e pelo Gestor de Segurança da Informação, designados por ato do Diretor da Agetic e funcionará como um grupo de trabalho permanente, multidisciplinar, e considerada prestação de serviço público relevante, não remunerada.

A ETIR/UFMS seguirá o Modelo de Autonomia “Compartilhada”, trabalhando em conjunto com toda a Agetic e demais unidades da UFMS, a fim de auxiliar o processo de tomada de decisão envolvendo incidentes cibernéticos e desenvolvendo os seguintes serviços:

I – reativos:

a) tratamento de incidentes de segurança cibernéticos;

b) tratamento de artefatos maliciosos; e

c) tratamento de vulnerabilidades.

II – proativos:

a) detecção de intrusão;

b) varredura de vulnerabilidades; e

c) testes de penetração (PenTest).

A dedicação às atividades proativas, assim como a atuação por convocação, deverá ser acordada entre o Gestor de Segurança da Informação e o respectivo gestor de cada integrante da ETIR/UFMS, com anuência do Diretor da Agetic.

A ETIR/UFMS atuará nas atividades de resposta a incidentes de segurança da informação na rede UFMS, provendo atendimento à toda a UFMS e ao público externo nas questões relacionadas ao gerenciamento da segurança cibernética.

5.3.2. Procedimentos

O processo de tomada de decisão relacionado a incidentes de segurança da informação na UFMS, com repercussão interna, será exercido pelo Gestor de Segurança da Informação, com supervisão do Diretor da Agetic.

As demais decisões de caráter sensível serão avaliadas pelo Diretor da Agetic, consultando o CGD/UFMS e a Alta Administração, sempre que necessário para a situação exigida.

O processo de gerenciamento de incidentes cibernéticos orientará as ações da ETIR/UFMS e contemplará:

- notificação do Incidente: o recebimento de notificações de incidentes permite à ETIR/UFMS atuar como ponto central para articulação de soluções dos problemas provocados por incidentes cibernéticos mediante a coleta de atividades e incidentes reportados, análise das informações e correlação destas no âmbito da UFMS;
- análise do incidente: a ETIR/UFMS examina todas as informações disponíveis sobre o incidente, incluindo artefatos e outras evidências relacionadas ao evento; analisa e identifica o escopo do incidente, sua extensão, sua natureza e quais os prejuízos causados, e propõe estratégias de contenção e recuperação;
- suporte à resposta a incidente: a ETIR/UFMS atua no processo de recuperação, e este serviço é prestado por **e-mail** ou pela indicação de documentos que possam auxiliar no processo de recuperação, podendo, envolver a interpretação dos dados coletados e na recomendação de estratégias de contenção e recuperação;
- coordenação na resposta a incidente: a ETIR/UFMS coordena as ações entre os envolvidos em um incidente, o que pode incluir redes e outros centros de tratamento (CSIRTs) externos ao seu âmbito de atuação, envolvendo a coleta de informações de contato, a notificação dos responsáveis pelas redes, computadores ou sistemas que possam estar envolvidos ou comprometidos e a geração de indicadores e estatísticas relativas aos incidentes; e
- distribuição de alertas, recomendações e estatísticas: esta atividade consiste em disseminar informações relativas a novos ataques ou tendências de ataques observadas pela ETIR/UFMS, por outros centros de tratamento.

Os incidentes de segurança cibernéticos na rede UFMS devem ser notificados e comunicados pelos usuários dos serviços digitais da UFMS e agentes internos e externos por meio dos canais:

I – e-mail: etir@ufms.br;

II – web: https://agetic.ufms.br/etir;

III – telefone: (67) 3345-7700;

IV – pessoalmente – em casos emergenciais; ou

V – por intermédio de ferramenta tecnológica e eventos de risco detectados pelo monitoramento de segurança.

5.4. Gestão de Ativos

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

5.5 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 das Normas para Uso dos Recursos de Tecnologia da Informação e Comunicação (TIC) da UFMS e da Política de Comunicação da UFMS.

5.6. Controle de Acesso

O Controle de Acesso estabelece critérios para a disponibilização dos serviços digitaus da UFMS levando em consideração:

a. o acesso à rede e demais serviços digitais da UFMS estará disponível a usuários previamente cadastrados;

b. é de responsabilidade da AGETIC o registro (log) e o armazenamento das atividades de login e logoff realizado pelos usuários em todos os recursos e sistemas da UFMS;

c. para o acesso aos serviços digitais da UFMS o usuário deverá utilizar o Passaporte UFMS (usuário e senha), que é pessoal e intransferível;

d. o compartilhamento de senha de acesso ao e-mail é autorizado somente em caso de e-mails administrativos institucionais, sendo o acesso controlado pela chefia imediata, ou pelo chefe hierárquico superior, quando houver necessidade;

e. o cadastro do Passaporte implica no aceite do Termo de Responsabilidade, com pleno conhecimento dos termos e condições desta Política, das Normas de Utilização dos Recursos de Tecnologia da Informação e Comunicação da UFMS e das demais políticas e normas vigentes;

f. o compartilhamento de senha do Passaporte Institucional é proibido, assim como a abertura de conexão autenticada para utilização por outra pessoa. O usuário será responsabilizado por qualquer ação realizada mediante o uso de seu Passaporte UFMS e senha pessoal nos serviços digitais da UFMS;

g. é dever do usuário zelar pelo sigilo de senhas de autenticação, bem como a escolha de senhas fortes de acordo com as normas vigentes;

h. é de responsabilidade do usuário realizar a correta desconexão (deslogar) dos serviços em que estiver logado com seu Passaporte.

i. o Passaporte UFMS do usuário poderá ser bloqueado em casos de incidentes de Segurança da Informação, podendo ser restabelecido após a solução dos problemas causados e reorientação ao usuário, desde que não existam outros impedimentos;

j. a Agetic poderá restringir os administradores de equipamentos computacionais da UFMS;

k. o cadastro de acesso para usuário visitante pode ser concedido mediante solicitação pelo responsável, contendo justificativa e prazo, encaminhados à Agetic;

l. os serviços digitais da UFMS contemplam uma conta de e-mail institucional, que deve ser utilizada exclusivamente para fins institucionais, sendo vedado o uso de e-mail de outros provedores para este fim;

m. 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;

n. 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;

o. as credenciais de acesso aos serviços digitais da UFMS devem ser canceladas por meio de solicitação da Unidade de vínculo à Agetic, após o desligamento do usuário da UFMS ou a saída da unidade de vínculo;

p. cada Gestor deve fazer uma análise crítica dos direitos de acessos que usuários possuem aos ativos de informação que estejam sob sua responsabilidade. Para ativos regulares essa revisão deve ser feita em intervalos máximos de 6 (seis) meses, para ativos de informações sensíveis e/ou sigilosas essa análise deve ser feita a cada 3 (três) meses.

q. o acesso da Rede da UFMS será concedido a instituições de acordo com instrumento jurídico, com definição da responsabilização dos usuários por incidentes causados e a adoção de procedimentos de controle favoráveis à Segurança da Informação; e

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

5.7. Gestão de Riscos

A Gestão de Riscos da UFMS é realizada por meio do Plano de Gestão de Processos e Riscos da UFMS, no qual a Agetic mapeia e faz tratamento de riscos dos seus principais processos.

5.8. Gestão de Continuidade

A Gestão de Continuidade da UFMS é realizada por meio do Plano de Continuidade de Negócios da UFMS.

5.9. Auditoria e Conformidade

Para garantir a aplicação da PSI/UFMS, além de fixar normas e procedimentos complementares, 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 acessos, bem como material manipulado;

b. tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial e de órgãos de controle, solicitação do gerente do sistema ou por determinação do Comitê de Governança Digital;

c. realizar, a qualquer tempo, inspeção física nos equipamentos da UFMS;

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.

5.10. Obrigações e Penalidades

O descumprimento das disposições da Política e de Normas Complementares sobre Segurança da Informação caracteriza infração, 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, no Regulamento Disciplinar do Estudante e demais legislações pertinentes.

6. Disposições Finais

A PSI/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.

Para auxiliar no cumprimento das diretrizes previstas, a Agetic poderá elaborar Planos, Instruções Normativas e Programas que visem melhorar a Segurança da Informação no âmbito da UFMS.

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 Governança Digital da UFMS.

UFMS
A NOSSA UNIVERSIDADE

www.ufms.br /ufmsbr @ufmsoficial

Educativa UFMS @UFMSbr /school/ufms /tvufms