NORMA DE GESTÃO DE ACESSO A ATIVOS DE INFORMAÇÃO DA UNIVERSIDADE FEDERAL DE VIÇOSA (UFV)

O GESTOR DE SEGURANÇA DA INFORMAÇÃO DA UNIVERSIDADE FEDERAL DE VIÇOSA (UFV), NA CONDIÇÃO DE COORDENADOR DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO DA UFV, no uso de suas atribuições legais e regimentais, resolve aprovar a norma que estabelece a gestão de acessos a ativos de informação da UFV:

Capítulo I - Disposições Gerais

Art. 1º - Termos e Definições Gerais

Os termos e definições gerais utilizados nesta norma estão estabelecidos na Política de Segurança da Informação e Comunicações (POSIC) da UFV, conforme a Resolução CONSU-UFV Nº 16/2019, e no Glossário de Segurança da Informação do Governo Federal, segundo a Portaria GSI/PR Nº 93, de 18 de outubro de 2021.

Art. 2º - Definições Específicas

I. Ativo: tudo que tenha valor para a organização, material ou não.

II. **Ativos de Informação**: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais

onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

III. **Entidade**: Indivíduo, grupo ou sistema, humano ou não humano, que interage com os ativos de informação da UFV.

a) **Entidade Humana**: Entidade que é uma pessoa física que interage com os ativos de informação da UFV. Inclui estudantes, professores, técnicos administrativos, servidores, empregados ou prestadores de serviços habilitados pela administração para acessar os ativos de informação da UFV, formalizada por meio da assinatura de Termo de Responsabilidade. Possui identidades e credenciais próprias para autenticação e autorização nos sistemas da UFV, sendo seu acesso gerenciado e monitorado para assegurar a segurança e a conformidade com as políticas institucionais.
b) **Entidade Não Humana**: Entidade que não é uma pessoa física, mas que interage com os ativos de informação da UFV. Inclui dispositivos, aplicações, serviços, processos automatizados ou quaisquer componentes de sistema que executam ações sem intervenção humana direta. Possui identidades e credenciais próprias para autenticação e autorização nos sistemas da UFV, sendo seu acesso gerenciado e monitorado para garantir a segurança e a conformidade com as políticas institucionais.

IV. **Identidade**: Representação eletrônica de uma entidade, composta por um conjunto de atributos que a identificam nos sistemas da UFV.

a) **Identidade Interna**: Identidade de entidades com vínculo permanente ou prolongado à UFV, como estudantes, professores, técnicos administrativos, servidores, dispositivos institucionais, serviços de TI internos e processos automatizados regulares.
b) **Identidade Externa**: Identidade de entidades com vínculo temporário ou transitório com a UFV, como colaboradores externos, participantes de programas de extensão, visitantes acadêmicos, dispositivos de

terceiros, serviços externos ou processos automatizados de fornecedores.

V. **Identificador Único**: Nome ou código exclusivo atribuído a cada identidade, usado para identificação nos sistemas da UFV.

VI. **Conta**: Conjunto de informações operacionais associadas a uma identidade, permitindo a autenticação e autorização de acesso a sistemas específicos. No contexto da UFV, a identidade pode estar vinculada a múltiplas contas (matrículas), conforme as funções desempenhadas.

VII. **Autenticação**: Processo que verifica a autenticidade de uma identidade ao solicitar acesso a um sistema, com base em credenciais registradas.

VIII. **MFA (Autenticação Multifator)**: Método de autenticação que utiliza mais de um fator de verificação para autenticar uma identidade.

IX. **Perfis de Acesso**: Conjunto de recursos associados aos ativos de informação da UFV que o portador de uma conta (identidade) poderá acessar e executar, em consonância com suas funções na Universidade.

X. **Acesso Padrão**: Nível de acesso com privilégios mínimos, associado a uma conta, que permite à identidade executar tarefas necessárias ao cumprimento de suas funções, sem permissões para modificar configurações ou acessar informações sensíveis.

XI. **Acesso Privilegiado**: Nível de acesso restrito exclusivamente ao pessoal técnico autorizado, oferecendo permissões ampliadas que possibilitam executar ações capazes de impactar significativamente a segurança, integridade ou operação dos sistemas.

XII. **Bloqueio de Conta**: Interrupção temporária do acesso de uma identidade a um sistema ou ativo de informação, podendo ocorrer por inatividade ou questões de segurança.

XIII. **Desativação de Conta**: Suspensão permanente do acesso de uma conta que não está mais em uso ou necessária, conforme as políticas de retenção de dados.

XIV. **Exclusão de Conta**: Remoção definitiva de uma conta e de todos os dados associados, em conformidade com as políticas de privacidade e retenção de dados.

XV. **RBAC (Controle de Acesso Baseado em Função na UFV)**: Modelo em que as permissões são concedidas com base nos perfis de acesso associados às identidades, alinhados às funções desempenhadas na Universidade.

XVI. **ABAC (Controle de Acesso Baseado em Atributos na UFV)**: Modelo que utiliza atributos das identidades, recursos, ações solicitadas e contexto ambiental para determinar permissões de acesso associadas às identidades.

XVII. **IAM-UFV (Identity and Access Management da UFV)**: Macroprocesso responsável pela gestão segura de identidades e pelo controle de acessos aos ativos de informação da Universidade.

XVIII. **Usuário:** Entidade Humana (pessoa física) que utiliza sistemas, serviços ou recursos de informação da UFV por meio de uma Identidade (Interna ou Externa) e Conta associada, para executar atividades relacionadas ao seu vínculo ou função na Universidade. O usuário possui direitos de acesso definidos conforme seu perfil de acesso (RBAC/ABAC), alinhados ao princípio do menor privilégio e à necessidade de conhecer.

Art. 3º - Referências Legais e Normativas

Esta norma está fundamentada nas seguintes referências legais e normativas:

I. Política de Segurança da Informação e Comunicações da UFV (POSIC-UFV): Define as diretrizes de segurança da informação no âmbito da UFV, promovendo a proteção e controle de acessos a ativos de informação.

II. Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei Nº 13.709/2018: Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

III. Lei Nº 12.965/2014 (Marco Civil da Internet): Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

IV. Decreto Nº 9.637, de 26 de dezembro de 2018: Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

V. Decreto Nº 10.641, de 2 de março de 2021: Altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24,caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

VI. Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-Ciber): É uma orientação manifesta do Governo federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética.

VII. Portaria GSI/PR Nº 93, de 18 de outubro de 2021: Padroniza termos e definições relacionados à segurança da informação, visando uniformizar a linguagem e práticas de gestão de riscos no setor público.

VIII. ABNT NBR ISO/IEC 27001:2022: Estabelece os requisitos para implementar e manter um Sistema de Gestão de Segurança da Informação (SGSI).

IX. ABNT NBR ISO/IEC 27002:2022: Complementa a ISO/IEC 27001, oferecendo orientações detalhadas sobre os controles de segurança da informação mencionados na ISO/IEC 27001.

X. ISO/IEC 24760-1:2019: IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts.

XI. Modelo de Política de Gestão de Controle de Acesso da Secretaria de Governo Digital (SGD): Fornece diretrizes para a implementação de políticas de controle de acesso em órgãos públicos, com base nas melhores práticas de segurança digital.

XII. Controles CIS (*Account and Credential Management Policy Template - CIS Critical Security Controls*): Template fornecido pelo CIS para gerenciamento de contas e credenciais, visando a proteção contra acessos indevidos e o controle de autenticação robusta.

XIII. PPSI - SGD/MGI Nº 852, de 28 de Março de 2023: Institui o Programa de Privacidade e Segurança da Informação (PPSI), voltado para elevar a maturidade e a resiliência dos órgãos públicos em privacidade e segurança da informação, incluindo o Centro Integrado de Segurança Cibernética do Governo Digital.

XIV. NIST SP 800-63B - *Digital Identity Guidelines*: Diretrizes do NIST para o gerenciamento de identidades digitais, incluindo autenticação e verificação de credenciais para garantir a segurança dos acessos a sistemas.

XV. **NIST SP 800-53** - Fornece um conjunto de controles de segurança recomendados pelo NIST para sistemas de informação, abordando controle de acesso, autenticação e monitoramento contínuo de atividades, assegurando a proteção de ativos digitais.
XVI. **NIST SP 800-162** - Fornece diretrizes para a implementação e gestão do controle de acesso baseado em atributos (ABAC), com foco em como essa abordagem pode melhorar a flexibilidade e segurança de sistemas de informação, permitindo que decisões de acesso sejam baseadas em múltiplos atributos do usuário, do ambiente e dos recursos.
XVII. **Lei Nº 12.527/2011 (Lei de Acesso à Informação)**: Regula o acesso a informações previsto na Constituição Federal, estabelecendo regras para a divulgação de informações públicas e proteção de informações sigilosas.

Art. 4º - Escopo

Esta norma aplica-se a todas as entidades que requerem acesso autorizado aos ativos de informação da UFV, em todos os seus campi e unidades, abrangendo

identidades internas e externas, visando garantir a proteção, integridade, confidencialidade e disponibilidade desses ativos.

Art. 5º - Objetivos

Estabelecer diretrizes claras para a gestão de identidades e acessos, assegurando que o acesso aos ativos de informação seja concedido de maneira controlada, segura e alinhada com as necessidades operacionais e institucionais, em conformidade com os princípios de confidencialidade, integridade e disponibilidade da informação.

Capítulo II - Governança e Administração de Identidades e Acessos na UFV

Art. 6º - Governança de Identidades e Acessos

§ 1º A governança da administração de identidades e acessos é responsabilidade do Comitê de Segurança da Informação e Comunicações (CSIC-UFV), com orientação do Comitê de Governança Digital (CGD).

§ 2º O CSIC-UFV deve:

I. Estabelecer diretrizes específicas sobre controle de acesso, alinhadas aos requisitos de segurança e necessidades institucionais.

II. Garantir a comunicação das regras de controle de acesso a todas as partes interessadas.

III. Participar de auditorias e revisões periódicas dos processos de gestão de identidades e acessos.

IV. Analisar os relatórios fornecidos pela DTI e propor ajustes nas políticas e procedimentos de segurança.

V. Promover a cultura de segurança da informação, assegurando que o acesso aos ativos seja controlado conforme os princípios de necessidade de conhecer e menor privilégio.

Art. 7º - Gestor de Identidades e Acessos

§ 1º As funções de gestão de identidades e acessos são desempenhadas pelo Gestor de Segurança da Informação e Comunicações da UFV.

§ 2º Compete ao Gestor:

I. Definir e supervisionar a implementação de normas e procedimentos de gestão de identidades e acessos, em alinhamento com as diretrizes estabelecidas pelo CSIC-UFV.

II. Coordenar a gestão completa do ciclo de vida das identidades, em parceria com a DTI.

III. Assegurar que cada identidade seja única e vinculada a uma entidade específica, evitando duplicidades.

IV. Verificar a autenticidade das identidades.

V. Colaborar com o CSIC-UFV na análise de relatórios e auditorias, bem como na implementação de melhorias nas políticas e procedimentos.

§ 3º O Gestor de Segurança da Informação pode designar agentes responsáveis pela administração de identidades e acessos, assegurando a segregação de funções e responsabilidades.

Art. 8º - Responsabilidades da DTI e Órgãos Proprietários dos Sistemas

§ 1º A Diretoria de Tecnologia da Informação (DTI) deve:

I. Implementar mecanismos automatizados de controle de acessos e gestão de identidades.

II. Manter atualizadas as definições dos perfis de acesso correspondentes a cada função ou tipo de identidade.

III. Assegurar que os sistemas suportem os controles de acesso necessários, incluindo registros de eventos significativos.

IV. Fornecer ao CSIC-UFV os relatórios e informações necessárias para a análise e melhoria contínua das políticas de gestão de identidades e acessos.

§ 2º Os órgãos proprietários dos sistemas devem colaborar com a DTI e o CSIC-UFV na gestão de identidades e acessos, conforme diretrizes estabelecidas.

Art. 9º - Administração de Identidades e Acessos

§ 1º A administração deve incluir a solicitação, aprovação, criação, modificação e revogação de acessos de forma controlada e documentada.

I. A concessão de uma conta deve ser precedida pela verificação da entidade solicitante.

II. Os direitos de acesso devem ser atribuídos às contas com base em autorizações formais, aprovadas pelo gestor imediato do solicitante e, quando aplicável, pelo gestor do sistema ou ativo de informação, e limitados ao mínimo necessário.

§ 2º O processo deve observar:

I. Segregação de funções, evitando concentração de atividades críticas.

II. Revisão periódica dos direitos de acesso, ajustando-os conforme mudanças nas funções ou necessidades.

III. Manutenção de registros detalhados de todas as atividades relacionadas à administração de identidades e acessos.

Art. 10 - Inventário de Contas e Revisões Periódicas

§ 1º A DTI deve manter um inventário atualizado de todas as contas gerenciadas.

§ 2º O inventário deve conter, no mínimo:

I. Identificação da identidade responsável pela conta.

II. Identificador único da conta.

III. Registros importantes no contexto do IAM-UFV (criação, modificação, exclusão de contas e atribuição de perfis de acesso).

IV. Unidade ou setor responsável.

V. Classificação do tipo de acesso.

VI. Status da conta (ativa, bloqueada, desativada, excluída).

§ 3º O inventário deve ser revisado periodicamente para garantir:

I. Conformidade dos acessos com as funções atribuídas.

II. Desativação ou remoção de contas desnecessárias ou inativas.

III. Atualização das credenciais conforme padrões de segurança.

§ 4º O processo de revisão deve ser documentado, mantendo registros para requisitos legais e auditorias.

Capítulo III - Gestão de Acesso

Subcapítulo I - Disposições Gerais

Art. 11 - Princípios Gerais de Gestão de Acesso

§ 1º O acesso aos ativos de informação deve ser controlado com base nos requisitos de segurança e institucionais.

§ 2º Devem ser aplicados os princípios de:

I. Necessidade de Conhecer: Acesso somente às informações necessárias para as funções da identidade.

II. Menor Privilégio: Concessão do mínimo de privilégios necessários.

III. Segregação de Funções: Separação de funções conflitantes.

§ 3º O controle de acesso deve considerar:

I. Determinação de quais entidades requerem acesso a quais informações.

II. Segurança de aplicações e sistemas.

III. Controle de acesso físico e lógico, conforme estabelecido na Norma de Controle de Acesso Físico da UFV.

IV. Classificação da informação e níveis de acesso.

V. Restrições ao acesso privilegiado.

VI. Requisitos legais, regulatórios e contratuais.

Art. 12 - Controle de Acesso Baseado em Função (RBAC) e Atributo (ABAC)

§ 1º Devem ser implementados controles de acesso que associem direitos às funções (RBAC) e, quando aplicável, com base em atributos específicos (ABAC).

§ 2º Os controles devem garantir que apenas identidades autorizadas tenham acesso aos ativos de informação da UFV.

Art. 13 - Gestão de Identidades

§ 1º A gestão de identidades deve assegurar o controle completo de seu ciclo de vida, incluindo:

I. Assegurar a unicidade das identidades e a adequação dos atributos associados às funções desempenhadas.

II. Verificação da autenticidade de cada identidade.

III. Gerenciar os atributos necessários para o exercício das funções.

IV. Evitar duplicidades de identidades.

§ 2º A UFV deve adotar padrões claros para os identificadores únicos, adequados ao tipo de identidade e vínculo.

§ 3º Os padrões de identificadores devem ser revisados periodicamente para evitar conflitos ou duplicidades.

Art. 14 - Gestão de Contas

§ 1º A gestão de contas deve incluir:

I. Criação, modificação e exclusão de contas associadas às identidades, conforme as necessidades operacionais, mediante aprovação dos gestores pertinentes, incluindo o gestor imediato do solicitante e, quando aplicável, o gestor do sistema ou ativo de informação.

II. Garantir que cada conta esteja corretamente associada a uma identidade válida e autenticada.

III. Atribuição e revisão periódica dos perfis de acesso associados às contas, alinhando-os com as funções desempenhadas e limitando-os ao mínimo necessário.

IV. Manutenção de registros detalhados de todas as atividades relacionadas à administração de contas.

§ 2º O processo de gestão de contas deve observar:

I. Segregação de funções, evitando concentração de atividades críticas.

II. Revisão periódica dos direitos de acesso atribuídos às contas, ajustando-os conforme mudanças nas funções ou necessidades.

III. Garantir que as contas desnecessárias ou inativas sejam desativadas ou removidas prontamente.

Subcapítulo II - Gestão de Informações de Autenticação

Art. 15 - Políticas de Senhas e Autenticação

§ 1º Devem ser estabelecidas políticas de autenticação que assegurem a segurança dos mecanismos de acesso, observando:

I. A implementação de métodos de autenticação únicos e apropriados para cada conta.

II. A adoção de medidas que garantam a robustez e a confiabilidade das credenciais de acesso.

III. A proteção das informações de autenticação contra uso indevido ou não autorizado.

IV. A responsabilização individual pelo uso adequado e seguro das credenciais de acesso.

§ 2º As informações de autenticação devem ser protegidas durante transmissão e armazenamento, utilizando criptografia e outras técnicas.

Art. 16 - Autenticação Multifator (MFA)

§ 1º O uso de autenticação multifator (MFA) é obrigatório para garantir a segurança dos acessos, sendo aplicado, no mínimo, aos seguintes cenários:

I. Acessos remotos à rede interna da UFV, incluindo conexões via VPN, devem, preferencialmente, utilizar autenticação multifator (MFA).

II. Contas com acesso privilegiado.

III. Acessos a sistemas ou serviços críticos com dados sensíveis, conforme classificados pelo processo de gestão de riscos de segurança da informação.

§ 2º A DTI é responsável por:

I. Implementar e manter soluções de MFA.

II. Assegurar que os sistemas internos e os sistemas externos sob responsabilidade da UFV sejam compatíveis com o MFA implementado.

III. Promover conscientização e treinamento sobre o uso do MFA.

IV. Monitorar e ajustar implementações de MFA conforme necessário.

Subcapítulo III - Gestão de Direitos de Acesso

Art. 17 - Concessão de Acessos

§ 1º O acesso deve ser concedido somente após:

I. Solicitação formal e aprovação pelo gestor imediato do solicitante e pelo gestor do sistema ou ativo de informação, quando aplicável.

II. Verificação da autenticidade da identidade.

§ 2º Os direitos de acesso devem ser alinhados às funções atribuídas e configurados nos perfis de acesso das contas, limitados ao mínimo necessário.

Art. 18 - Modificação e Revogação de Acessos

§ 1º Alterações nos direitos de acesso devem ser processadas imediatamente quando houver:

I. Mudança nas funções, responsabilidades ou necessidades de acesso da entidade.

II. Término do vínculo ou da relação da entidade com a UFV.

§ 2º Excepcionalmente, conforme políticas internas da UFV, poderá ser concedido acesso controlado a serviços específicos após o término do vínculo ou da necessidade de acesso, desde que não comprometa a segurança dos ativos de informação.

Art. 19 - Bloqueio e Desbloqueio de Contas

§ 1º Contas devem ser bloqueadas temporariamente em caso de incidentes de segurança ou uso indevido.

§ 2º O desbloqueio deve seguir procedimentos formais, incluindo:

I. Solicitação pelo responsável autorizado.

II. Verificação e aprovação pelo gestor responsável.

§ 3º A desativação aplica-se a identidades não mais necessárias, prevenindo acessos indevidos.

Subcapítulo IV - Responsabilidades das Entidades Humanas

Art. 20 - Responsabilidades Gerais

§ 1º As entidades humanas devem:

I. Utilizar recursos e informações somente para fins autorizados.

II. Manter a confidencialidade das informações acessadas.

III. Seguir diretrizes e procedimentos de segurança.

IV. Reportar incidentes de segurança ou atividades suspeitas.

V. Proteger suas credenciais individuais de acesso, não as compartilhando com terceiros.

VI. Possuir somente os acessos mínimos necessários para a execução de suas tarefas laborais.

§ 2º É responsabilidade das entidades humanas garantir que suas senhas sejam fortes, seguras, mantidas em sigilo e não reutilizadas em outros sistemas ou serviços.

Subcapítulo V - Gestão de Acesso Privilegiado

Art. 21 - Uso de Contas com Acesso Privilegiado

§ 1º Contas privilegiadas permitem ações que podem afetar significativamente a segurança e operação dos sistemas, incluindo:

I. Administração de sistemas operacionais, bancos de dados, aplicações e equipamentos de rede.

II. Modificação de configurações de segurança ou políticas de sistema.

III. Gestão de contas e privilégios.

IV. Acesso a dados sensíveis ou confidenciais.

§ 2º Entidades humanas com acesso privilegiado devem:

I. Utilizar acesso privilegiado exclusivamente para tarefas que requerem tais privilégios.

II. Manter segregação entre contas privilegiadas e de acesso padrão.

III. Seguir políticas e procedimentos de segurança estabelecidos.

IV. Participar de treinamentos periódicos específicos sobre segurança da informação e uso adequado de privilégios elevados.

Art. 22 - Segurança das Credenciais Privilegiadas

§ 1º As credenciais devem:

I. Ter senhas ou mecanismos de autenticação com critérios mais rigorosos do que os aplicados às contas de acesso padrão.

II. Utilizar MFA obrigatoriamente.

III. Ser armazenadas e gerenciadas em repositórios seguros.

§ 2º A DTI deve:

I. Implementar controles e mecanismos de monitoramento contínuo para registrar o uso e as atividades realizadas com contas privilegiadas.

II. Realizar auditorias periódicas das atividades realizadas.

III. Garantir que apenas pessoal autorizado tenha acesso às credenciais privilegiadas.

IV. Manter registros detalhados para assegurar rastreabilidade.

Subcapítulo VI - Gestão de Acesso para Identidades Externas

Art. 23 - Concessão de Acesso a Identidades Externas

§ 1º O acesso deve ser:

I. Solicitado formalmente pela unidade responsável, especificando necessidade e período.

II. Aprovado por autoridade competente.

III. Vinculado à assinatura de termos de confidencialidade e conformidade com as políticas da UFV, por parte da entidade externa.

IV. Após aprovação, o acesso para entidades não humanas deve ser adequadamente configurado, limitando o escopo de acesso conforme necessário.

Art. 24 - Autenticação e Verificação de Entidades Externas

§ 1º Devem ser aplicados processos rigorosos de autenticação:

I. Para entidades humanas: apresentação de documentos oficiais ou contratos válidos.

II. Para entidades não humanas: uso de certificados digitais ou tokens de segurança.

III. Uso obrigatório de autenticação multifator (MFA) para todos os acessos realizados por identidades externas vinculadas a entidades externas em sistemas ou serviços críticos (classificados pelo processo de gestão de riscos em segurança da informação), conforme estabelecido no Art. 15 desta norma.

Art. 25 - Monitoramento e Revogação de Acessos Externos

§ 1º O monitoramento deve ser contínuo, garantindo utilização apropriada.

§ 2º O acesso será revogado:

I. Ao término do período estabelecido.

II. Em caso de descumprimento das políticas de segurança.

III. Por decisão do CSIC-UFV para proteger os ativos de informação.

§ 3º A revogação deve incluir desativação de credenciais e remoção de métodos de autenticação.

§ 4º Devem ser implementados procedimentos automatizados, quando possível, para garantir que os acessos temporários sejam revogados imediatamente ao término do período autorizado, incluindo:

I. Configuração de datas de expiração nos sistemas de autenticação.

II. Notificações prévias ao término do acesso, tanto para a identidade externa quanto para a unidade responsável.

III. Verificação periódica, pela DTI e unidades responsáveis, dos acessos externos ativos (realizados pelas entidades externas).

Subcapítulo VII - Gestão de Acesso a Serviços em Nuvem

Art. 26 - Gestão de Acesso a Serviços em Nuvem

§ 1º A utilização de serviços em nuvem deve observar as diretrizes de segurança da UFV.

§ 2º A gestão de identidades e acessos deve:

I. Estar em conformidade com as políticas e normas de segurança e privacidade de dados da UFV.

II. Garantir acesso somente aos recursos necessários.

III. Utilizar mecanismos de autenticação seguros, preferencialmente com MFA.

§ 3º A DTI é responsável por:

I. Administrar e monitorar os acessos, quando aplicável.

II. Garantir que os provedores de serviços em nuvem adotem práticas compatíveis com as políticas e normas de segurança e privacidade de dados da UFV.

III. Manter registros das atividades realizadas, quando aplicável.

§ 4º A contratação deve ser formalmente aprovada, seguindo procedimentos internos e legislações aplicáveis.

Art. 27 - Responsabilidades dos Usuários em Serviços em Nuvem

§ 1º As entidades humanas (usuários) devem:

I. Respeitar as políticas estabelecidas para uso dos serviços em nuvem.

II. Proteger as informações institucionais, evitando compartilhamento não autorizado.

III. Reportar incidentes de segurança ou atividades suspeitas.

§2º É proibido o armazenamento ou processamento de informações sensíveis em serviços não autorizados. Os serviços autorizados são aqueles formalmente aprovados e listados pela DTI em conformidade com as políticas internas da UFV.

Art. 28 - Segurança dos Serviços em Nuvem

§ 1º A UFV deve assegurar que os serviços atendam aos padrões de segurança, incluindo:

I. Criptografia de dados em trânsito e em repouso.

II. Mecanismos de backup e recuperação de dados.

III. Conformidade com legislações vigentes, como a LGPD.

§ 2º A DTI deve avaliar periodicamente os serviços utilizados.
§ 3º Antes da adoção de novos serviços em nuvem, deve ser realizada uma avaliação de riscos, conduzida pela DTI em conjunto com as unidades solicitantes, incluindo:

I. Análise de segurança e conformidade do serviço com as políticas da UFV e legislações aplicáveis.

II. Identificação de potenciais ameaças e vulnerabilidades associadas ao uso do serviço.

III. Definição de controles e medidas de segurança necessárias para mitigar os riscos identificados.

Art. 29 - Monitoramento e Auditoria em Serviços em Nuvem

§ 1º Devem ser implementados mecanismos de monitoramento contínuo, incluindo:

I. Registro de acessos e ações.

II. Detecção e resposta a incidentes.

§ 2º Logs e registros devem ser armazenados de forma segura.

§3º Auditorias periódicas devem ser realizadas conforme definido nas políticas internas da UFV, verificando a conformidade dos serviços em nuvem com as políticas institucionais e requisitos legais aplicáveis, incluindo a reavaliação dos riscos associados aos serviços utilizados.

Capítulo IV - Monitoramento e Auditoria

Art. 30 - Monitoramento de Acessos

§ 1º A DTI deve implementar mecanismos para:

I. Registrar e acompanhar atividades das contas associadas às identidades nos sistemas.

II. Detectar e responder a acessos não autorizados.

III. Gerar relatórios sobre as atividades de acesso, fornecendo-os ao CSIC-UFV em prazos acordados.

§2º Logs devem ser mantidos seguros e armazenados pelo período definido nas políticas internas de retenção de dados da UFV, em conformidade com a legislação aplicável.

§ 3º O monitoramento deve ser contínuo e abrangente, permitindo a detecção imediata de atividades não autorizadas ou suspeitas.

Art. 31 - Auditorias de Segurança

§ 1º Auditorias periódicas devem:

I. Verificar aderência às políticas e procedimentos.

II. Identificar vulnerabilidades, propondo melhorias.

III. Revisar o uso de contas privilegiadas.

§ 2º O CSIC-UFV é responsável por designar a equipe de auditoria, que pode ser composta por membros internos ou por auditores externos autorizados, garantindo independência.

§ 3º Os resultados das auditorias devem ser documentados e encaminhados ao CSIC-UFV.

§ 4º O CSIC-UFV, em conjunto com a DTI e outros órgãos envolvidos, deve supervisionar a implementação das ações corretivas recomendadas nas auditorias.

Capítulo V - Considerações Finais

Art. 32 - Sanções

§ 1º O descumprimento desta norma sujeita o infrator a sanções administrativas, civis e penais, conforme legislação vigente e regulamentos internos da UFV.

§ 2º Sanções podem variar de advertências a penalidades severas, conforme a gravidade da infração e processos disciplinares da instituição.

§ 3º Em casos com indícios de crime, medidas judiciais serão tomadas e reportadas às autoridades competentes.

Art. 33 - Resolução de Casos Omissos

§ 1º Casos omissos ou não previstos serão avaliados pelo CSIC-UFV, que decidirá com base nas melhores práticas de gestão de identidades e segurança da informação.

§ 2º O CSIC-UFV pode consultar órgãos externos ou especialistas para auxílio na resolução de casos complexos.

Art. 34 - Revisão e Atualização da Norma

§ 1º Esta norma será revisada no máximo a cada dois anos, ou em prazos menores caso haja alterações legais, tecnológicas ou institucionais, para garantir sua adequação às necessidades da UFV.

§ 2º Sugestões de melhorias podem ser encaminhadas ao CSIC-UFV.

Art. 35 – Revogação da Portaria Normativa nº 0005/2020/RTR

Fica revogada a Portaria Normativa nº 0005/2020/RTR, de 31 de julho de 2020, que normatiza o controle de acesso (lógico e físico) aos ativos de informação da Universidade Federal de Viçosa (UFV), visando preservar a confidencialidade, integridade, disponibilidade e autenticidade das informações.

Art. 36 - Entrada em Vigor

Esta norma entra em vigor na data de sua publicação, revogando disposições anteriores sobre gestão de acesso a ativos de informação da UFV.