MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais
Reitoria

PORTARIA Nº 3999/IFMG, DE 07 DE JULHO DE 2025

Dispõe sobre a instituição da Política de Controle de Acesso, que trata de controles de identificação, autenticação e autorização para proteger e preservar as informações e os recursos tecnológicos do IFMG.

O **REITOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MINAS GERAIS**, no uso das atribuições que lhe são conferidas pelo Estatuto da Instituição, republicado com alterações no Diário Oficial da União do dia 08/05/2018, Seção 1, Páginas 09 e 10, e pelo Decreto de 11 de setembro de 2023, publicado no DOU de 12 de setembro de 2023, Seção 2, Edição nº 174, página 01

Considerando a Portaria SGD/MGI nº 852, de 28 de março de 2023 que Dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI;
Considerando a Política de Segurança da Informação do IFMG;

Considerando a deliberação do Comitê de Segurança da Informação do IFMG e o que consta no Processo nº **23208.003392/2024-13**,

RESOLVE

Instituir a Política de Controle de Acesso do IFMG

Política de Controle de Acesso

Objetivo

A Política de Controle de Acesso estabelece controles de identificação, autenticação e autorização para proteger e preservar as informações e os recursos tecnológicos do IFMG, estejam eles armazenados ou processados em ambientes físicos ou digitais. O propósito dessa política é prevenir incidentes de segurança da informação, como acessos indevidos, alterações não autorizadas, perda ou destruição de dados, roubo e divulgação indevida, garantindo, assim, a confidencialidade, integridade e disponibilidade das informações institucionais.

A ausência de mecanismos eficazes de identificação, autenticação e autorização expõe a operação das áreas a riscos significativos, como acessos ilegítimos a sistemas e dados, comprometimento da segurança cibernética e possíveis impactos negativos às atividades acadêmicas, administrativas e à reputação institucional.

Neste contexto, fica definido que as credenciais institucionais como crachás funcionais ou de estudantes, e logins de acesso aos sistemas, são pessoais, intransferíveis e representam o único método legítimo pelo qual os direitos de acesso físico e lógico devem ser exercidos no âmbito do IFMG.

Dessa forma, a implementação e o gerenciamento eficaz dos controles definidos nesta política asseguram que apenas usuários expressamente autorizados possam ter acesso físico às dependências institucionais e lógico aos sistemas de informação e demais recursos tecnológicos do IFMG.

Escopo

Esta política aplica-se a todas as informações cujo IFMG figure como agente de tratamento, independentemente do meio utilizado para esse tratamento, digital ou físico, bem como às suas dependências físicas e tecnológicas. Além disso, abrange todas as pessoas que acessem as instalações físicas ou que exerçam qualquer tipo de controle administrativo, técnico ou operacional sobre os sistemas e informações, ainda que de forma eventual.

Especificamente, estão sujeitos à aplicação desta política:

- Todos alunos, servidores efetivos e temporários do IFMG.

- Todos os colaboradores terceirizados, estagiários, prestadores de

serviços e contratados que atuam para o IFMG.

- Todos os funcionários de organizações parceiras que acessam fisicamente as dependências ou que fazem uso das redes e sistemas de informação do IFMG.

Termos e Definições

ACESSO - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

CONTA DE SERVIÇO - conta de acesso à rede corporativa de computadores, necessária a um procedimento automático (aplicação, script, entre outros) sem qualquer intervenção humana no seu uso;

CONTROLE DE ACESSO - conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

MFA - sigla de autenticação de multifatores (multifactor authentication), é uma tecnologia de segurança que exige mais do que uma senha para fazer login em uma conta;

VPN - significa Virtual Private Network (Rede Privada Virtual). É uma tecnologia que cria uma conexão segura entre um dispositivo e a internet.

Referência legal e de boas práticas

Orientação	**Secção**
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II art. 50

Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo, art.3, Inciso I
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso XI CAPÍTULO VI - Seção IV – Art.15
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Instrução Normativa 01/GSI/PR	Art.12, Inciso IV, alínea f
ABNT NBR ISO/IEC 27002: 2013. Código de Prática para controles de Segurança da Informação	Itens 9 – 11.2.9 (Páginas 23 - 47)
CIS V8	CAPÍTULO 6
Guia do Framework de Privacidade e Segurança da Informação (PPSI)	Controles 5, 6, 12 e 31
Instrução Normativa Nº 04/GSI/PR, de 26 de março de 2020	Capítulo II
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
Account and Credential Management Policy Template for CIS Controls 5 and 6	Em sua íntegra
ABNT NBR ISO/IEC 27701: 2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e Diretrizes	Itens 6 – 6.6.2 (Página 16)
ISO/IEC FDIS 29151:2016(E). Information technology — Security techniques — Code of practice for personally identifiable information protection	Itens 9 – 9.2.2 e 9.2.3 (Página 11)
GSI 09/2023. OSIC (ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA) — Gestão de Acesso Privilegiado (Privileged Access Management – PAM) – parte 2 de 2. Disponível em: https://www.gov.br/gsi/pt-br/ssic/osic/OSIC%2009.23	Em sua íntegra

I. Declarações da política

Art. 1º Fica aprovada, no âmbito do IFMG, a Política para Criação e Administração de contas de acesso, em complemento às diretrizes estabelecidas pela Política de Segurança da Informação - POSIN do IFMG.

Art. 2° O IFMG deve definir regras de limitação ou restrição de acesso aos colaboradores e estudantes, para que estes disponham de privilégios mínimos

necessários para exercerem suas atividades, funções e responsabilidades pré-definidas.

CAPÍTULO I

ACESSO LÓGICO

Art. 3º O acesso lógico aos recursos da Rede Local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela Diretoria de Tecnologia da Informação e Coordenação de TI das unidades do IFMG, baseado nas responsabilidades e tarefas de cada usuário.

I. O IFMG deve implementar protocolos de comunicação e redes seguros.

II. Terão direito a acesso lógico da Rede Local os usuários de recursos de tecnologia da informação.

III. Para fins desta Política, consideram-se usuários de recursos de tecnologia da informação servidores ocupantes de cargo efetivo ou cargo em comissão, ocupantes de emprego público em exercício, assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade no IFMG.

IV. O acesso remoto deve ser realizado por meio de VPN – Rede Virtual Privada, após as devidas autorizações.

V. Deve ser utilizado o MFA para a autenticação de acesso remoto, quando disponível.

VI. O acesso a todas as aplicações institucionais ou de terceiros que estejam hospedadas em fornecedores deve utilizar MFA.

VII. O IFMG deve centralizar a autenticação, autorização e auditoria (AAA) dos ativos de informação da sua infraestrutura de rede.

VIII. O IFMG deve adotar técnicas de segmentação de rede visando limitar o acesso de forma eficiente e segura, assegurando que apenas colaboradores e dispositivos autorizados possam interagir com partes específicas da rede.

Art. 4º A DTI e a Coordenação de TI das unidades do IFMG, devem

estabelecer e manter um inventário de todas as contas gerenciadas, este deve incluir contas de usuário, administrativas, testes e serviços. Em caso de contas de serviço, o inventário deve conter no mínimo informações de:

I. Departamento proprietário.

II. Data de criação/última autorização de renovação de acesso;

III. Data de validade previamente definida, de forma a evitar sua permanência ativa após o término do vínculo ou da necessidade de uso. Essa exigência se aplica, especialmente, às contas de bolsistas, estagiários, visitantes, professores temporários ou substitutos, contas destinadas a testes, suporte externo ou quaisquer outras com finalidade transitória.

a) As contas de serviço devem conter, obrigatoriamente, a informação sobre a data de expiração do vínculo com o IFMG. No momento da criação, essas contas já devem ser configuradas com prazo máximo de expiração de até 180 dias após o término do referido vínculo.

Art. 5º A DTI deve implementar a centralização da gestão de contas por meio de serviço de diretório e/ou identidade.

Art. 6º Deve-se estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, tal inventário deve ser revisado periodicamente.

Art. 7º Deve-se centralizar o controle de acesso para todos os ativos de informação da organização por meio de um serviço de diretório.

Art. 8º Deve-se definir e manter o controle de acesso dos usuários baseado em funções.

I. Deve ser elaborada a documentação dos direitos dos acessos para cada função dentro da organização.

II. Deve-se realizar análises de controle de acesso aos ativos institucionais para validar se todos os privilégios estão autorizados para a execução de atividades de cada função, este processo deve ser repetido de forma periódica ou quando novas funções e ativos de informação forem inseridos na organização.

III. Ao conceder acesso a usuários que lidam com dados pessoais, deve-se limitar, estritamente, o acesso aos sistemas que processam esses dados ao

mínimo necessário para cumprir os objetivos essenciais do processamento, em conformidade com o princípio da minimização de dados. Ao atribuir ou revogar os direitos de acesso concedidos deve-se incluir:

a) Verificação de que o nível de acesso concedido é apropriado às políticas de acesso, além de ser consistente com outros requisitos, tais como, segregação de funções;

b) Garantia de que os direitos de acesso não estão ativados antes que o procedimento de autorização esteja completo;

c) Manutenção de um registro preciso e atualizado dos perfis dos usuários criados para os que tenham sido autorizados a acessar o sistema de informação e os dados pessoais neles contidos;

d) Mudança dos direitos de acesso dos usuários que tenham mudado de função ou de atividades, e imediata remoção ou bloqueio dos direitos de acesso dos usuários que deixaram o IFMG;

e) Analisar criticamente os direitos de acesso em intervalos regulares.

CAPÍTULO II

CONTA DE ACESSO LÓGICO E SENHA

Art. 9º Para utilização das estações de trabalho do IFMG, será obrigatório o uso de uma única identificação (*login*) e de senha de acesso, fornecidos pela DTI ou Coordenação de TI das unidades, mediante solicitação formal pelo titular da unidade do requisitante.

I. O formulário de solicitação de acesso deve ser disponibilizado de forma digital para preenchimento.

II. Os privilégios de acesso dos usuários à Rede Local devem ser definidos pela unidade requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

III. Na necessidade de utilização de perfil diferente do disponibilizado, o responsável da unidade do usuário deverá encaminhar a solicitação para a DTI ou Coordenação de TI da unidade que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Art. 10 O *login* e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo titular da unidade do requisitante.

Art. 11 O padrão adotado para o formato da conta de acesso do usuário é a sequência primeiro nome + ponto + último nome do usuário, como por exemplo, joao.silva.

I. Nos casos de já existência de conta de acesso para outro usuário, será realizada outra combinação utilizando o nome completo do usuário para o qual a conta está sendo criada.

II. A DTI e as Coordenações de TI deverão criar uma norma complementar para definir o padrão de criação de contas de visitantes, bolsistas, terceirizados e outros colaboradores devidamente vinculados à instituição.

Art. 12 O padrão adotado para o formato da senha é o definido pela DTI, que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores.

I. A formação da senha de validação da identificação (*login*) de acesso à Rede Local deve seguir as regras de:

a) Possuir tamanho mínimo de dez caracteres, sendo obrigatório o uso de letras e números, para contas que utilizam MFA e 14 caracteres para contas que não utilizam MFA;

b) Recomenda-se a utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &,...);

c) Não ser formada por sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações;

d) Não utilizar termos óbvios, tais como: Brasil, senha, usuário, *password* ou *system*.

e) Não reutilizar senhas tendo em vista os constantes vazamentos.

Art. 13 As senhas de acesso serão renovadas a cada 12 meses ou 365 dias 365 trezentos e sessenta e cinco) dias, devendo o usuário ser informado antecipadamente a fim de que ele próprio efetue a mudança.

Parágrafo único: Caso não efetue a troca no prazo estabelecido, será bloqueado seu acesso à Rede Local até que a nova senha seja configurada.

Seção I

Do Controle de Acesso Lógico para Alunos

Art. 14 Cada aluno do IFMG deverá possuir credencial, pessoal e intransferível, composta por RA (matrícula) e senha individual.

Parágrafo único: A credencial deve ser utilizada obrigatoriamente para acesso aos ambientes institucionais, sistemas acadêmicos, plataformas de aprendizagem e demais recursos disponibilizados pela instituição. Os alunos são responsáveis pela proteção e confidencialidade de suas credenciais, ficando vedado compartilhá-las com terceiros, inclusive colegas ou familiares.

Art. 15 O acesso dos alunos às plataformas digitais de ensino (Ambiente Virtual de Aprendizagem – AVA), sistemas acadêmicos e demais recursos disponibilizados pelo IFMG será controlado por autenticação pessoal (RA e senha).

Parágrafo único: Será permitido aos alunos acessar exclusivamente os recursos para os quais estão formalmente autorizados e de acordo com seu perfil educacional e acadêmico, respeitando a necessidade educacional e institucional.

CAPÍTULO III

BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

Art. 16 A conta de acesso (email, login de rede) será bloqueada nos seguintes casos:

I. Após 5 (cinco) tentativas consecutivas de acesso errado;

II. Solicitação do superior imediato do usuário com a devida justificativa;

III. Quando da suspeita de mau uso dos serviços disponibilizados pelo IFMG ou descumprimento da Política de Segurança da Informação – POSIN e normas correlatas em vigência.

IV. Após 180 cento e oitenta) dias consecutivos sem movimentação pelo usuário.

V. Após 60 dias de expiração de senha, sem haver atualizações.

VI. No caso de alunos após 3 meses de conclusão de cursos a conta será bloqueada.

VII. No caso de servidor, bolsista, terceirizado, prestador de serviços deve ser bloqueado imediatamente após a perda de vínculo.

VIII. No caso da situação de matrícula como Transferência Externa ou Evasão do aluno, sua conta será suspensa imediatamente.

Art. 17 As solicitações de criação de contas de acesso temporárias, tais como para bolsistas, estagiários, professores substitutos e visitantes, devem obrigatoriamente informar a data de expiração do vínculo com o IFMG. A conta deverá ser criada já configurada com prazo de expiração automático, não excedendo 180 (cento e oitenta) dias após o fim do vínculo informado.

Art. 18 Quando não for possível determinar previamente a data de encerramento do vínculo, o prazo máximo de validade da conta será de até 24 (vinte e quatro) meses, salvo exceções justificadas e autorizadas pela autoridade competente.

Art. 19 Contas de acesso destinadas a testes devem ser criadas com prazo de validade igual ou inferior a 6 (seis) meses, sendo vedada sua renovação automática sem análise formal da necessidade e autorização expressa.

Art. 20 Todas as contas de usuários, tanto no diretório LDAP quanto nos serviços de correio eletrônico institucional, deverão ser organizadas em containers ou unidades organizacionais (OU) específicas, de modo a permitir a identificação do setor, unidade ou finalidade da conta, facilitando o processo de auditoria, revisão e controle de acessos.

Art. 21 É vedado o uso de contas genéricas compartilhadas, inclusive para uso em laboratórios ou ambientes educacionais. Caso haja necessidade de contas locais para fins pedagógicos, estas não deverão ser criadas na base LDAP institucional nem possuir permissão para acesso a informações sensíveis ou sistemas institucionais.

Art. 22 As únicas contas autorizadas a utilizar o atributo “senha nunca expira” são aquelas classificadas como contas de serviço para autenticação de equipamentos, mediante justificativa técnica.

Art. 23 Credenciais com privilégios avançados deverão ser exclusivas para atividades administrativas e restritas aos recursos a que se destinam. É expressamente proibido que contas de uso diário possuam pertencimento a grupos como Domain Admins, Domain Administrators ou Enterprise Admins. Em casos excepcionais, privilégios limitados poderão ser concedidos de forma temporária para uso local em estações de trabalho específicas, mediante controle e registro formal.

Art. 24 O desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do superior imediato do usuário.

Art. 25 Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato.

Art. 26 A DTI deve garantir a implementação de um processo formal de cancelamento de usuários que administram ou operem sistemas e serviços que tratem de dados pessoais. Tal processo deverá incluir:

I. A imediata remoção ou desabilitação de usuário que tenha deixado o IFMG;

II. A remoção e identificação, de forma periódica, ou a desabilitação de usuários com os mesmos identificadores.

Art. 27 A DTI e Coordenação de TI das unidades, devem configurar o bloqueio automático de sessão nos ativos após um período de inatividade preestabelecido. Tal prazo pode ser específico para cada tipo de ativo.

Art. 28 O IFMG deve manter um processo estruturado de gestão de acessos, abrangendo o fornecimento, a revisão periódica, a atualização e a revogação de autorizações. Este processo deve contemplar, no mínimo, as seguintes diretrizes:

I. Anualmente, preferencialmente no primeiro semestre, o setor de Tecnologia da Informação, em conjunto com o setor de Gestão de Pessoas e demais diretorias, deverá realizar a validação das contas de usuários (servidores) ativas na base LDAP e nos serviços de e-mail institucional.

II. Contas de e-mail de alunos inativas ou vinculadas a usuários com perda de vínculo com o IFMG há mais de 12 (doze) meses poderão ser excluídas.

III. Contas de e-mail de ex-servidores, desativadas há mais de 5 (cinco) anos, poderão ser excluídas por questões de otimização de armazenamento e segurança.

IV. Contas de serviços ou de e-mail de bolsistas, terceirizados, estagiários e demais usuários sem vínculo efetivo com o IFMG, que estejam desativadas há mais de 3 (três) anos, também poderão ser excluídas pelos mesmos motivos.

V. A criação de contas de e-mail acadêmico vinculadas ao domínio do Office 365 ficará restrita a:

a) Alunos regularmente matriculados em cursos formais do IFMG; e

b) Servidores efetivos, estagiários, bolsistas ou terceirizados com carga horária semanal igual ou superior a 30 (trinta) horas.

c) Nos casos de criação automatizada de contas vinculadas a unidades organizacionais (OU), credenciais que não atenderem aos requisitos acima deverão

ser alocadas em OUs distintas, de modo a evitar a geração indevida de e-mails institucionais.

VI. Cada campus do IFMG deverá manter, em sua respectiva unidade organizacional (OU) na base LDAP, uma subunidade denominada “Desativados”, destinada a armazenar os objetos de usuários desativados há mais de 12 (doze) meses. Da mesma forma, nas OUs sincronizadas com o Office 365 (Alunos), deverá existir uma subunidade “Desativados” que funcione como área de quarentena por até 12 (doze) meses, antes da exclusão definitiva do e-mail e de login de acesso a rede de ex-alunos.

VII. Para contas Office 365 referente a docentes e técnicos administrativos a remoção/exclusão poderá ocorrer após 5 (cinco) anos de desativação da conta.

VIII. Considerando a natureza especial do vínculo dos servidores aposentados com a instituição, que se estende para além de sua inatividade laboral, suas contas de e-mail institucionais não estarão sujeitas ao bloqueio imediato previsto para a perda de vínculo de servidor em geral. Em vez disso, as contas de e-mail dos servidores aposentados permanecerão ativas por um período de 10 (dez) anos a partir da data de sua aposentadoria. Após esse período de 10 anos ativas, essas contas serão desativadas e, subsequentemente, poderão ser excluídas conforme as diretrizes aplicáveis a ex-servidores para otimização de armazenamento e segurança.

IX. A criação de e-mails institucionais setoriais no domínio acadêmico estará condicionada à prévia existência do respectivo setor cadastrado no SIORG (Sistema de Organização e Inovação Institucional do Governo Federal). A nomenclatura dos endereços poderá ser adaptada para facilitar a identificação e a comunicação institucional.

X. Devem ser disponibilizadas, na base de conhecimento institucional, informações resumidas desta Política de Gestão de Acessos, a fim de orientar os responsáveis pela criação e administração de contas de usuários quanto às diretrizes vigentes.

Art. 29 Em situações excepcionais, como abandono de cargo, ausência injustificada, impedimento legal ou falecimento de servidor público, e sendo este o único titular de conta de e-mail institucional que contenha informações relevantes à continuidade das atividades administrativas ou acadêmicas, a Diretoria de Tecnologia da Informação (DTI) poderá, mediante autorização formal da Direção-Geral ou do

Comitê de Segurança da Informação (CSI), realizar acesso emergencial e controlado à respectiva conta institucional respeitando os princípios da Lei Geral de Proteção de Dados.

§1º O acesso emergencial terá finalidade exclusiva de recuperar informações institucionais indispensáveis à manutenção das atividades do IFMG.

§2º A operação deverá ser formalizada por meio de processo administrativo específico aberto no SEI, contendo: justificativa detalhada, data da ação, identificação dos servidores envolvidos no acesso e a devida autorização da autoridade competente.

§3º Sempre que possível, o acesso deverá ser realizado na presença do gestor imediato do servidor titular da conta. Na impossibilidade, a operação deverá contar com a participação de, no mínimo, dois servidores da área de Tecnologia da Informação, previamente designados, visando garantir a transparência, a rastreabilidade e a responsabilização da ação.

§4º Após a recuperação das informações, a conta será imediatamente bloqueada de forma preventiva, até que haja decisão administrativa quanto à sua exclusão, redirecionamento ou reativação.

Art. 30 O IFMG deve implementar e manter seguro logs ou registro físico de todos os acessos aos ativos de informação.

Art. 31 O acesso a ambientes seguros ou ativos de tratamento e armazenamento de dados por fornecedores ou prestadores de serviços será concedido somente quando necessário e de acordo com as seguintes diretrizes:

I. Para fins específicos e autorizados;

II. Supervisionado e monitorado;

Art. 32 Os ativos de armazenamento e tratamento de dados que se encontrem fora do IFMG devem ser protegidos contra perda, roubos, danos e acesso físico não autorizados conforme as seguintes diretrizes:

I. Não deixar o ativo sem vigilância em locais públicos e inseguros;

II. Proteger o ativo contra riscos associados a visualização de informações por outra pessoa;

III. Implementar as funcionalidades de rastreamento e limpeza remota.

Art. 33 O IFMG deve estabelecer uma política ou normativo equivalente sobre a gestão de mídias de armazenamento consideradas críticas, de acordo com as seguintes diretrizes:

I. Exigir autorização para a saída de mídias de armazenamento para locais externos;

II. Armazenar mídias em local seguro de acordo com a classificação de suas informações.

III. Criptografar as mídias de acordo com a classificação de suas informações.

IV. Manter cópias de segurança de mídias de acordo com a classificação de suas informações;

CAPÍTULO IV

ACESSO FÍSICO

Art. 34 O IFMG deve definir perímetros de segurança para proteger ambientes e ativos contra acesso físico não autorizado, danos e interferências de acordo com as diretrizes a seguir:

I. Definir a localização e resistência dos perímetros de acordo com os requisitos de segurança da informação relacionados aos ativos que se encontram dentro dos perímetros.

II. Proteger os ambientes seguros contra acessos não autorizados por meio de mecanismos de controle de acesso, como fechaduras tradicionais ou digitais, que possibilitem autenticação por biometria, senhas, PINS ou cartões de acesso.

a) O IFMG deve executar testes nos mecanismos de controle de acesso em períodos pré-definidos para assegurar a funcionalidade total do equipamento.

b) Os mecanismos de controle de acesso devem ser monitorados.

III. Estabelecer uma área de recepção ou outros meios de controle de acesso físico a ambientes que não for conveniente a implementação de mecanismos de controle de acesso.

Art. 35 O acesso físico a ambientes seguros ou ativos de tratamento e armazenamento de dados do IFMG é destinado apenas a pessoal autorizado.

Seção I

Do Controle de Acesso Físico para Alunos

Art. 36 Para acesso físico às dependências institucionais, é fortemente recomendada a adoção de mecanismos formais de controle de acesso, tais como identificação por meio de documento oficial com foto, carteirinha estudantil emitida pelo IFMG ou sistema biométrico.

Parágrafo único. A identificação dos alunos deve ser exigida sempre que houver a possibilidade de acesso a ambientes com equipamentos, informações ou serviços institucionais sensíveis, sendo responsabilidade da direção da unidade assegurar a existência de procedimentos mínimos de controle.

Art. 37 As áreas de acesso restrito ou laboratórios que contenham equipamentos sensíveis, ativos críticos ou que exijam controles adicionais de segurança devem possuir sistemas de controle de acesso físico, tais como fechaduras digitais, autenticação biométrica, cartões de acesso ou outros mecanismos compatíveis com o grau de risco identificado.

Parágrafo único. A direção da unidade é responsável por avaliar os ambientes sob sua gestão e implementar controles apropriados, cabendo à área técnica de TI ou segurança patrimonial prestar apoio na seleção e operação desses mecanismos.

CAPÍTULO V

MOVIMENTAÇÃO INTERNA

Art. 38 Quando houver mudança do usuário para outro setor ou o usuário ocupar uma nova função, os direitos de acesso à Rede Local devem ser revogados.

I. O novo superior imediato deve realizar a solicitação de novos acessos de acordo com novo setor / função do usuário.

II. Os direitos de acesso antigos devem ser imediatamente cancelados conforme solicitação do antigo superior imediato.

CAPÍTULO VI

CONTA DE ACESSO BIOMÉTRICO

Art. 39 A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para se obter um acesso, a fim de atender os conceitos da autenticação de multifatores.

Parágrafo único. O IFMG deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO VII

ADMINISTRADORES

Art. 40 A utilização de identificação (*login*) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

I. Somente os técnicos da Diretoria de Tecnologia da Informação e

Coordenação de TI das unidades, devidamente habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede.

II. Na necessidade de utilização de *login* com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para o setor responsável pela gestão dos acessos que poderá negar os casos em que entender desnecessária a utilização.

III. Se concedida a permissão ao usuário como administrador local na estação de trabalho, esse será responsável por manter a integridade da máquina, não podendo instalar, desinstalar ou remover qualquer programa sem autorização formal do setor responsável pela Tecnologia da Informação.

IV. Caso constatada a irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão.

V. A identificação (*login*) com privilégio de administrador nos equipamentos locais será fornecida em caráter provisório, podendo ser renovada por solicitação formal do titular da unidade requisitante.

VI. Excepcionalmente, poderão ser concedidas identificações (*login*) de acesso à rede de comunicação de dados a visitante em caráter temporário após apreciação do setor responsável pela gestão dos acessos.

VII. Deverá ser implementado o MFA para todas as contas de administrador.

VIII. Deve-se restringir os privilégios de contas de administrador dedicados nos ativos de informação, para que o usuário com privilégio de administrador local não consiga realizar atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, estas atividades deverão ser realizadas preferencialmente a partir da conta primária não privilegiada do usuário.

IX. Ao tratar dados pessoais o IFMG deve observar o princípio do privilégio mínimo como regra, para garantir que o usuário receba apenas os direitos mínimos necessários para executar suas atividades, para tanto podem ser realizadas as seguintes ações:

a) Remover os direitos de administrador nos dispositivos finais;

b) Remover todos os direitos de acesso root e admin aos servidores e

utilizar tecnologias que permitam a elevação granular de privilégios conforme a necessidade, ao mesmo tempo em que fornecem recursos claros de auditoria e monitoramento;

c) Eliminar privilégios permanentes (privilégios que estão “sempre ativos”) sempre que possível;

d) Limitar a associação de uma conta privilegiada ao menor número possível de pessoas;

e) Minimizar o número de direitos para cada conta privilegiada.

CAPÍTULO VIII

RESPONSABILIDADES

Art. 41 A Coordenação de Gestão de Pessoas (CGP) deve comunicar formalmente à Diretoria de Tecnologia da Informação (DTI) ou a Coordenação de TI da unidade as seguintes movimentações de pessoal para que as permissões de acesso à Rede Local sejam atualizadas:

I – Ingresso de servidores, estagiários ou contratados, informando nome completo, matrícula/identificador, unidade de lotação e data prevista de início;

II – Afastamentos temporários (ex: licenças, cessões, aposentadorias), com datas de início e término;

III – Desligamentos definitivos (ex: exoneração, término de contrato, demissão), com data efetiva da saída;

§ 1º A comunicação deve ser realizada em formato padronizado, preferencialmente por meio digital (SUAP ou SEI), com periodicidade mínima mensal

ou sempre que houver atualização.

§ 2º A DTI e as Coordenações de TI das unidades utilizarão essas informações para realizar o bloqueio, suspensão ou exclusão das contas de acesso, conforme o caso.

Art. 42 É responsabilidade do setor responsável pela gestão de mão-de-obra terceirizada a comunicação imediata sobre desligamentos, férias e licenças de funcionários de empresas prestadoras de serviços, para que seja efetuado o bloqueio momentâneo ou revogação definitiva da permissão de acesso aos recursos.

Parágrafo único: A ausência dessa comunicação poderá acarretar responsabilização da contratada, conforme cláusulas contratuais vigentes, além da imediata suspensão dos acessos não regularizados.

Art. 43 É de responsabilidade do setor responsável pela Tecnologia da Informação o monitoramento da utilização de serviços de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como bloquear, temporariamente, sem aviso prévio, a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica do IFMG.

Art. 44 O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à Rede Local e a recursos de tecnologia custodiados ou de propriedade do IFMG.

I. O usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos.

II. O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à Rede Local.

Art. 45 O usuário deve informar ao setor responsável pela Tecnologia da

Informação qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 46 É dever de o usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a Instituição, a saber:

I. Não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;

II. Evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;

III. Interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentar do local de trabalho por qualquer motivo;

IV. Não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;

V. Não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

VI. Utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;

VII. Não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis;

VIII. Assinar o Termo de Responsabilidade (Modelo – Anexo I) quanto a utilização da respectiva conta de acesso.

Seção I

Das Responsabilidades dos Alunos

Art. 47 Os alunos deverão manter atualizados seus dados cadastrais

junto à secretaria de registro e controle acadêmico para garantir a validade das informações utilizadas para controle de acesso.

Art. 48 Caso identifique qualquer comprometimento, perda ou uso indevido de suas credenciais ou informações pessoais, o aluno deverá comunicar imediatamente a Coordenadoria de Registro e Controle Acadêmico ou setor de Tecnologia da Informação da unidade do IFMG onde estuda.

Art. 49 Os alunos deverão cumprir integralmente esta política e demais normas de segurança da informação vigentes no IFMG, estando sujeitos às penalidades previstas no regulamento disciplinar da instituição em caso de descumprimento.

CAPÍTULO IX

DISPOSIÇÕES GERAIS

Art. 50 Os incidentes que afetem a Segurança das Informações, assim como o descumprimento da Política de Segurança da Informação e Normas de Segurança devem ser obrigatoriamente comunicados pelos usuários ao setor responsável pela Tecnologia da Informação.

Art. 51 Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, o setor responsável pela Tecnologia da Informação fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

I. Nos casos em que o autor da quebra de segurança for um usuário, a Diretoria de Tecnologia da Informação comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis.

II. Ações que violem a POSIN ou que quebrem os controles de Segurança da Informação serão passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

III. Processo administrativo disciplinar específico deverá ser instaurado para apurar as ações que constituem em quebra das diretrizes impostas por esta Norma e pela POSIN.

IV. A resolução de casos de violação/transgressões omissas nas

legislações correlatas será resolvida pelo Comitê de Segurança da Informação - CSI do IFMG.

Art. 52 Esta Política é aprovada pelo Comitê de Segurança da Informação (CSI) do IFMG e entra em vigor na data de sua publicação.

ANEXO I

IFMG

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, e lotado no(a)_____deste Ministério, DECLARO , sob pena das sanções cabíveis nos termos da _____ (legislação vigente) que assumo a responsabilidade por:

I. Tratar o(s) ativo(s) de informação como patrimônio do IFMG;

II. Utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do IFMG;

III. Contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 27 de maio de 2020, que Dispõe sobre Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal;

IV. Utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do IFMG;

V. Responder, perante o IFMG, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

VI. Acessar a rede corporativa, computadores, Internet e/ou utilização de e-mail, somente com autorização (usuário/senha), por necessidade de serviço.

VII. Utilizar o correio eletrônico (*e-mail*) colocado a minha disposição somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail;

VIII. Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

IX. Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

X. Não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador (*browser*), bloquear estação de trabalho, bem como encerrar a sessão do cliente de correio, garantindo assim a impossibilidade de acesso indevido por terceiros;

XI. Não revelar minha senha de acesso à rede corporativa, computadores, Internet e/ou do correio eletrônico (e-mail) a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

XII. Responder em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

Local, UF, _____de _____de _____. _____
Assinatura Nome do usuário e seu setor organizacional
_____
Nome da autoridade responsável pela autorização do acesso

Publicação: Transparência Ativa em 07 de julho de 2025

Documento assinado eletronicamente sob fundamentação, por:
RAFAEL BASTOS TEIXEIRA | Reitor

Data da Assinatura:
07 de julho de 2025 as 16:58 (America/Sao_Paulo)

Tipo de Documento:
Portaria

Autenticidade