RESOLUÇÃO CGAG/CONSUNI/UFOB Nº 025, DE 23 DE OUTUBRO DE 2025.

Institui a Política de Controle de Acesso da Universidade Federal do Oeste da Bahia – UFOB.

A CÂMARA DE GESTÃO ADMINISTRATIVA E GOVERNANÇA, ASSESSORA AO CONSELHO UNIVERSITÁRIO DA UNIVERSIDADE FEDERAL DO OESTE DA BAHIA, no uso de suas atribuições legais, considerando a deliberação extraída da sua 33ª Reunião Ordinária, realizada no dia 23 de outubro de 2025, homologada na 61ª Reunião Ordinária do Conselho Universitário, realizada no dia 5 de novembro de 2025, resolve:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Resolução institui a Política de Controle de Acesso da Universidade Federal do Oeste da Bahia – UFOB.

Parágrafo único. Esta Política tem o objetivo de estabelecer controles de identificação, autenticação e autorização para salvaguardar as informações pessoais e institucionais, estejam elas em qualquer meio, seja digital ou físico, a fim de evitar a quebra da segurança da informação e quaisquer acessos não autorizados que implique em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Art. 2º Esta Política está alinhada às Diretrizes Gerais estabelecidas na Política de Segurança da Informação – PSI da UFOB.

Art. 3º Os termos e definições que seguem são adotadas nesta política:

I - 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;

II - AUDITORIA: consiste na avaliação dos registros e procedimentos, como trilhas de auditoria e outros, que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos, à rede interna e à *internet*;

III - AUTENTICAÇÃO: processo que busca verificar a identidade digital de uma entidade de um sistema, no momento em que ela requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pela entidade com outras já pré-definidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo;

IV - AUTORIZAÇÃO: direito ou a permissão de acesso a um recurso de um sistema;

V - 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;

VI - BLOQUEIO DE ACESSO: processo que tem por finalidade suspender temporariamente o acesso;

VII - 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;

VIII - ESTAÇÃO DE TRABALHO: recurso estratégico em ambientes profissionais, combinando poder de processamento, *software* especializado e confiabilidade para atender a demandas técnicas ou criativas complexas;

IX - MFA: sigla de Autenticação de Multifatores (Multifactor Authentication);

X - NÍVEIS DE ACESSO: especificam quanto de cada recurso ou sistema o usuário pode utilizar;

XI - USUÁRIO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO: pessoa física ou jurídica que opera algum sistema informatizado a serviço da UFOB; e

XII - AGENTE PÚBLICO: pessoa legalmente investida em cargo público ou emprego público na administração direta, nas autarquias ou nas fundações públicas que fará uso de sistemas específicos para a realização de atividades administrativas e acadêmicas.

CAPÍTULO II
DO ACESSO LÓGICO

Art. 4º O acesso lógico aos recursos da Rede Local deve ser realizado por meio de sistema de controle de acesso.

§1º O acesso deve ser concedido e mantido pelo órgão gestor de Tecnologia da Informação e Comunicação da UFOB, baseado nas responsabilidades e tarefas de cada usuário.

§2º O Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB deve implementar protocolos de comunicação e redes seguros.

§3º Terão direito a acesso lógico aos recursos da Rede Local os usuários de recursos de tecnologia da informação.

§4º Para fins desta Resolução, 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 na UFOB.

§5º Deve ser utilizado o MFA para a autenticação de acesso remoto.

§6º O acesso a todas as aplicações corporativas ou de terceiros que estejam hospedados em fornecedores deve utilizar MFA.

§7º O Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB deve centralizar a Autenticação, Autorização e Auditoria - AAA dos ativos de informação da sua infraestrutura de rede.

§8º O Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB 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. 5º O acesso remoto para serviços que estão hospedados na rede interna da UFOB deve ser realizado por meio de Rede Virtual Privada - VPN, com *login* e senha padrão da conta institucional.

§1º Os acessos poderão ser concedidos de forma temporária aos usuários de recursos de tecnologia da informação mediante justificativa do setor responsável que deverá ser analisada pelo Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB.

§2º Técnico-Administrativos em Educação deverão encaminhar a solicitação com a anuência da chefia imediata.

§3º Docentes deverão encaminhar a solicitação com a anuência de seu respectivo Centro.

§4º O acesso a Terceirizados somente poderá ser concedido com solicitação do setor diretamente responsável pela execução do serviço ou tarefa que se pretenda realizar.

§5º O acesso a Estudantes que se façam necessários, deverá ser encaminhado diretamente pela Direção do Centro vinculado.

§6º As solicitações deverão ser encaminhadas conforme Catálogo de Serviços do Órgão Gestor de Tecnologia da Informação da UFOB.

§7º Os acessos devem ser revisados pelo Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB com periodicidade máxima de seis meses, podendo ser desativados em caso de observado o fim da necessidade justificada ou não utilização superior a 45 (quarenta e cinco) dias.

Art. 6º O Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB deve estabelecer e manter um inventário de todas as contas gerenciadas, incluindo contas de usuário, administrativas, testes e serviços. Em caso de contas de serviço, o inventário deve conter, no mínimo, informações de:

I - Unidade proprietária;

II - data de criação/última autorização de renovação de acesso; e

III - validação expressa do Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB, responsável por confirmar a regularidade e a legitimidade de todas as contas ativas.

Art. 7º O Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB deve implementar a centralização da gestão de contas por meio de serviço de diretório ou identidade.

Art. 8º O Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB deve estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, sendo que tal inventário deve ser revisado periodicamente.

Art. 9º O Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB deve centralizar o controle de acesso para todos os ativos de informação da organização por meio de um serviço de diretório ou provedor de *login* único.

Art. 10. O Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB deve definir e manter o controle de acesso dos usuários baseado em funções.

§1º Nos casos em que a administração de funções de um sistema seja gerenciada por outro setor, cabe a este delegar as funções observando as necessidades mínimas de concessão de privilégios.

§2º Deve ser elaborada a documentação dos direitos dos acessos para cada função dentro da organização.

§3º O Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB deve 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, sendo que esse processo deve ser repetido de forma periódica ou quando novas funções e ativos de informação forem inseridos na organização.

§4º 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:

I - 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;

II - garantia de que os direitos de acesso não estão ativados antes que o procedimento de autorização esteja completo;

III - 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;

IV - 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 de possuir qualquer vínculo com a UFOB; e

V - analisar criticamente os direitos de acesso em intervalos regulares.

Art. 11. O Órgão Gestor de Tecnologia da Informação e Comunicação, em conjunto com os demais órgãos da UFOB, no âmbito de suas competências, deverá implementar processo formal de registro de usuários que realizem tratamento de dados pessoais, visando à adequada atribuição de direitos de acesso e à adoção de medidas para resposta a incidentes envolvendo comprometimento de credenciais, tais como corrupção ou vazamento de senhas e demais dados de autenticação. Para esse fim, deverão ser observadas, no mínimo, as seguintes disposições:

I - utilizar identificador de usuário único, de modo a possibilitar a rastreabilidade das ações e a vinculação das responsabilidades de cada usuário;

II - admitir o uso compartilhado de identificador de usuário apenas quando estritamente requerido por razões operacionais ou de negócio, mediante aprovação prévia, justificativa formal e registro documental; e

III - assegurar que um identificador de usuário emitido não seja reutilizado ou atribuído a outra pessoa, ainda que após o desligamento, afastamento ou mudança de função do usuário anterior.

CAPÍTULO III
DA CONTA DE ACESSO LÓGICO E SENHA

Art. 12. Para utilização das estações de trabalho da UFOB será obrigatório o uso de uma única identificação (*login*) e de senha de acesso, fornecidos pelo órgão gestor de Tecnologia da Informação e Comunicação da UFOB.

§1º Os privilégios de acesso à Rede Local devem ser solicitados pela chefia imediata do usuário ao Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB ou demais órgão da UFOB, no âmbito das suas respectivas competências, limitando-se a atividades estritamente necessárias à realização de suas tarefas, conforme comprovação de designação emitida por sua chefia imediata.

§2º Na necessidade de utilização de perfil diferente do disponibilizado, o titular da unidade do usuário deverá encaminhar solicitação para o Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB, que a examinará, devendo analisar a necessidade e pertinência do pedido.

§3º Será possibilitado o registro de *e-mail* secundário com a finalidade de recuperação de conta ou comunicação em casos de perda de acesso ao *e-mail* institucional.

Art. 13. O *login* e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação ou compartilhamento, sob pena de serem bloqueados pelo Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB, inclusive de forma preventiva, quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo chefe da unidade do requisitante, mediante justificativa, que será analisada pelo Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB.

Art. 14. O padrão adotado para o formato da conta de acesso dos usuários em sistema de gestão de processos e documentos eletrônicos, é a sequência “primeiro nome + ponto + último nome do usuário”, como por exemplo: mateus.silva.

§1º Nos casos de já existência de conta de acesso para outro usuário, o Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB realizará outra combinação utilizando o nome completo do usuário ou matrícula para o qual a conta está sendo criada.

§2º O padrão adotado para o formato da conta de acesso dos estudantes da UFOB é a sequência “nome + ponto + primeira letra do último nome conjuntamente com os quatro últimos dígitos da matrícula”, como por exemplo: mateus.a1234.

Art. 15. O padrão adotado para o formato da senha é o definido pelo Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB, que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores.

§1º A formação da senha da identificação (*login*) de acesso à Rede Local deve seguir as regras de:

I - possuir tamanho mínimo de oito caracteres;

II - obrigatoriedade da utilização de letras maiúsculas, minúsculas, números e caracteres especiais ($, %, &,...);

III - 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;

IV - não utilizar termos óbvios, tais como: Brasil, senha, *admin*, usuário, *password* ou *system*; e

V - não reutilizar as últimas 03 (três) senhas.

§2º O Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB fornecerá uma senha temporária para cada conta de acesso criada no momento da liberação dessa conta e a mesma deverá ser alterada pelo usuário quando do primeiro acesso à Rede Local.

Art. 16. As senhas de acesso serão renovadas a cada 90 (noventa) 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.

Art. 17. Os sistemas institucionais da UFOB devem assegurar o respeito e a inclusão do nome social de todos os usuários, conforme previsto na legislação vigente.

§1º O nome social será exibido como identificação principal em interfaces de sistemas, quando solicitado pelo usuário.

§2º O registro do nome social será facultativo e realizado por meio de processo formalizado pelo Órgão Gestor de Tecnologia da Informação e Comunicação ou pelo Órgão de Gestão de Pessoas da UFOB.

§3º O tratamento do nome social deve prevalecer sobre o nome civil em comunicações internas e externas, exceto em situações onde a legislação exija o uso do nome registral.

CAPÍTULO IV
DO BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

Art. 18. A conta de acesso será bloqueada nos seguintes casos:

I - após 05 (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 pela UFOB ou descumprimento da Política de Segurança da Informação – PSI e normas correlatas em vigência; e

IV - após 45 (quarenta e cinco) dias consecutivos sem movimentação pelo usuário.

Art. 19. O desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do superior imediato do usuário ao Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB ou pelo próprio usuário, mediante justificativa formal.

Art. 20. Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato ou do Órgão responsável pela Gestão de Pessoas da UFOB.

Art. 21. A conta de acesso não utilizada há mais de 180 (cento e oitenta) dias poderá ser cancelada.

Art. 22. O Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB e os demais órgãos da UFOB, no âmbito das suas respectivas competências, devem garantir a implementação de um processo formal de cancelamento de usuários que administrem ou operem sistemas e serviços que tratem de dados pessoais. Tal processo deverá incluir:

I - a imediata remoção ou desabilitação de usuário que tenha encerrado as suas atividades na UFOB; e

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

Art. 23. O Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB deve 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. 24. O Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB e os demais órgãos da UFOB, devem, sempre que possível, priorizar a revogação/desativação de contas com o objetivo de manter dados e *logs* para possíveis auditorias.

CAPÍTULO V
DO ACESSO FÍSICO

Art. 25. O Comitê de Segurança Permanente da UFOB 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, sendo observado que:

a) deve-se executar testes nos Mecanismos de Controle de Acesso em períodos pré-definidos para assegurar a funcionalidade total do equipamento; e

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. 26. O acesso físico a ambientes seguros ou ativos de tratamento e armazenamento de dados da UFOB é destinado apenas a pessoal autorizado.

Art. 27. O Comitê de Segurança Permanente da UFOB deve manter um processo de gestão de acessos para fornecimento, revisão periódica, atualização e revogação das autorizações.

Art. 28. O Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB deve implementar e manter seguros *logs* ou registros físicos de todos os acessos aos ativos de informação.

Art. 29. 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 - autorização concedida pelo setor responsável pela gestão de acesso ou responsável pelo ativo; e

III - supervisionado e monitorado.

Art. 30. Os ativos de armazenamento e tratamento de dados que se encontrem fora da UFOB devem ser protegidos contra perda, roubo, danos e acesso físico não autorizado, 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; e

III - implementar as funcionalidades de rastreamento e limpeza remota.

Art. 31. A UFOB deve elaborar uma política ou normativo equivalente que defina condições e restrições pertinentes ao acesso físico nos dispositivos de trabalho remoto, levando em consideração as seguintes diretrizes:

I - segurança física do local de trabalho remoto; e

II - regras e orientações quanto ao acesso de familiares e visitantes ao dispositivo.

CAPÍTULO VI
DA MOVIMENTAÇÃO INTERNA

Art. 32. Quando houver mudança do agente público para outro setor ou este ocupar uma nova função, os direitos de acesso à Rede Local devem ser revogados.

§1º O novo superior imediato ou o Órgão responsável pela Gestão de Pessoas deve realizar a solicitação de novos acessos de acordo com o novo setor/função do usuário.

§2º Os direitos de acesso antigos devem ser imediatamente cancelados conforme solicitação do antigo superior imediato ou do Órgão responsável pela Gestão de Pessoas.

CAPÍTULO VII
DA CONTA DE ACESSO BIOMÉTRICO

Art. 33. 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. A UFOB deverá tratar seus respectivos dados biométricos como dados sigilosos, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO VIII
DOS ADMINISTRADORES

Art. 34. 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.

§1º Somente os técnicos do Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB, devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede.

§2º Na necessidade de utilização de *login* com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para o Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB, que poderá negar os casos em que entender desnecessária a utilização.

§3º 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 órgão gestor de Tecnologia da Informação e Comunicação da UFOB.

§4º Caso constatada a irregularidade o usuário perderá o acesso como administrador e a ocorrência será registrada como “Incidente de Segurança da Informação” junto à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais da UFOB.

§5º 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.

§6º Salvo para atividades específicas da área responsável pela gestão da tecnologia da informação do órgão, não será concedida, para um mesmo usuário, identificação (*login*) com privilégio de administrador para mais de uma estação de trabalho, ou para acesso a equipamentos servidores e a dispositivos de rede.

§7º As identificações (*login*) de acesso à rede de comunicação de dados a visitante em caráter temporário serão implementadas pelo Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB.

§8º O Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB deve implementar o MFA para todas as contas de administrador.

§9º O Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB deve restringir os privilégios de administrador a contas de administrador dedicados nos ativos de informação, para que o usuário com privilégio de administrador 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.

§10. Ao tratar dados pessoais, o Órgão Gestor de Tecnologia da Informação e Comunicação e os demais órgãos da UFOB, devem, no âmbito das suas respectivas competências, observar o princípio do privilégio mínimo como regra, para garantir que o usuário receba apenas os níveis de acessos mínimos necessários para executar suas atividades, para tanto podem ser realizadas as seguintes ações:

I - remover os direitos de administrador nos dispositivos finais;

II - 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;

III - eliminar privilégios permanentes, privilégios que estão “sempre ativos”, sempre que possível;

IV - limitar a associação de uma conta privilegiada ao menor número possível de pessoas; e

V - minimizar o número de direitos para cada conta privilegiada.

CAPÍTULO IX
DAS RESPONSABILIDADES

Art. 35. Caberá ao Órgão de Gestão de Pessoas a comunicação imediata ao Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB sobre desligamentos de servidores e estagiários, para que seja efetuada a revogação definitiva da permissão de acesso aos recursos.

Art. 36. É responsabilidade do setor responsável pela gestão de mão-de-obra terceirizada a comunicação imediata ao Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB sobre desligamentos de funcionários de empresas prestadoras de serviços, para que seja efetuado o bloqueio momentâneo ou revogação definitiva da permissão de acesso aos recursos.

§1º Os serviços serão filtrados por programas de antivírus, *anti-phishing* e *anti-spam* e, caso violem alguma regra de configuração, serão bloqueados ou excluídos automaticamente.

§2º Nenhum técnico terceirizado, salvo a autorização e acompanhamento do Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB, terá acesso ao conteúdo das informações armazenadas nos equipamentos servidores da UFOB.

Art. 37. É de responsabilidade do Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB 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 da UFOB.

Art. 38. O Órgão Responsável pelos Registros Acadêmicos comunicará ao Órgão Gestor de Tecnologia da Informação e Comunicação da UFOB acerca da vinculação dos estudantes.

Art. 39. 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 da UFOB.

§1º 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.

§2º A utilização simultânea da conta de acesso à rede local em mais de uma estação de trabalho ou *notebook* deve ser evitada, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica.

§3º O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à rede local.

Art. 40. O usuário deve informar ao Comitê Permanente de Segurança da Informação da UFOB qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 41. É dever do usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a UFOB, 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 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; e

VIII - conhecer as normas e políticas de segurança da UFOB.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 42. 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 à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR da UFOB.

Art. 43. Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR da UFOB fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

§1º Nos casos em que o autor da quebra de segurança for um usuário, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR da UFOB comunicará os resultados ao Órgão Gestor de Tecnologia da Informação e Comunicação para adoção de medidas cabíveis.

§2º Ações que violem a Política de Controle de Acesso 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.

§3º Processo administrativo disciplinar específico deverá ser instaurado para apurar as ações que constituem a quebra das diretrizes impostas por esta Resolução.

Art. 44. Os casos omissos serão dirimidos pela Câmara de Gestão Administrativa e Governança - CGAG.

Art. 45. Esta Resolução entra em vigor em 2 de março de 2026.

gov.br Documento assinado digitalmente
UILIAM RANGEL AMORIM SOUZA
Data: 19/02/2026 21:28:40-0300
Verifique em https://validar.iti.gov.br

UILIAM RANGEL AMORIM SOUZA
Presidente da Câmara de Gestão Administrativa e Governança

gov.br Documento assinado digitalmente
JACQUES ANTONIO DE MIRANDA
Data: 27/02/2026 10:32:06-0300
Verifique em https://validar.iti.gov.br

JACQUES ANTONIO DE MIRANDA
Presidente do Conselho Universitário