INSTRUÇÃO NORMATIVA 2/2025/REIT - CGAB/REIT

PROCESSO SEI Nº 23243.004192/2024-51

DOCUMENTO SEI Nº 2521036

Estabelece os controles de identificação, autenticação e autorização para salvaguardar as informações no âmbito do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO).

Instrução Normativa aprovada na 79ª Reunião Ordinária do Colégio de Dirigentes (CODIR) do Instituto Federal de Educação, Ciência e Tecnologia do Rondônia (IFRO), realizada nos dias 18 e 19 de dezembro de 2024, em formato híbrido. Processo SEI nº 23243.003768/2024-63.

DO OBJETO

A Política de Controle de Acesso objetiva estabelecer controles de identificação, autenticação e autorização para salvaguardar as informações no âmbito do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), 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.

Sem controles de autorização, identificação e autenticação, existe o risco potencial de que os sistemas de informação possam ser acessados ilicitamente e que a segurança desses sistemas de informação seja comprometida.

Considera-se, portanto, que as credenciais: crachá de identificação funcional e *logins* de acesso dos sistemas de informações, são pessoais e intransferíveis e são o único método legítimo pelo qual o direito de acesso físico e/ou lógico podem ser exercidos.

Os controles de autorização, identificação e autenticação garantem que apenas usuários autorizados tenham acesso físico ou façam uso dos sistemas de informação do IFRO.

DO ESCOPO

Esta Política se aplica a todas as informações tratadas pelo IFRO, ao meio utilizado para este tratamento, seja digital ou físico, e às dependências físicas desta organização, bem como a qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento.

Especificamente, inclui:

I. servidores

II. alunos

III. colaboradores

IV. estagiários

V. prestadores de serviço que exerçam atividades no âmbito da Instituição ou;

VI. qualquer cidadão que tenha acesso a dados ou informações no âmbito do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO).

DOS TERMOS E DEFINIÇÕES

CONTA DE ACESSO: conta de acesso para 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);*

SSO – *login* único *(single sign-on)*: esquema de autenticação que permite que os usuários façam *login* uma vez usando um único conjunto de credenciais e acessem várias aplicações durante a mesma sessão.

DAS REFERÊNCIAS LEGAIS E DE BOAS PRÁTICAS

ORIENTAÇÃO	SEÇÃO
Decreto nº 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, inciso XXIII
Instrução Normativa GSI/PR nº 1/2008	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 a 47
CIS Critical Security Controls Version 8 (CIS V8)	Capítulo 6
Guia do *Framework* de Privacidade e Segurança da Informação (PPSI)	Controles 5 e 6
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

DAS DECLARAÇÕES DA POLÍTICA

Dos princípios gerais:

I. a Política de Gestão de Controle de Acesso deve estar alinhada com a Política de Segurança da Informação (POSIC) do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO);

II. a Política de Gestão de Controle de Acesso deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

O PRESIDENTE DO COMITÊ DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RONDÔNIA (IFRO), no uso de suas atribuições e tendo em vista o disposto na Política de Segurança da Informação e

Comunicação (POSIC), aprovada pela Resolução nº 57/REIT - CONSUP/IFRO, de 15 de outubro de 2019,

R E S O L V E:

Art. 1º Fica aprovada, no âmbito do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), a Norma para criação e administração de contas de acesso, em complemento às diretrizes estabelecidas pelo inciso I do art. 15, Capítulo IX, da Política de Segurança da Informação e Comunicação (POSIC), aprovada pela Resolução nº 57/REIT - CONSUP/IFRO, de 15 de outubro de 2019.

CAPÍTULO I

ACESSO LÓGICO

Art. 2º 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 Gestão de Tecnologia da Informação (DGTI), baseado nas responsabilidades e tarefas de cada usuário.

I. terão direito a acesso lógico aos recursos da Rede Local os usuários de recursos de tecnologia da informação;

II. para fins desta Instrução Normativa, 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, alunos e demais usuários temporários em atividade no IFRO;

III. o acesso remoto deve ser realizado por meio de Rede Virtual Privada (VPN), após as devidas autorizações;

IV. deve ser utilizado o MFA para a autenticação de acesso remoto;

V. o acesso a todas as aplicações corporativas ou de terceiros que estejam hospedados em fornecedores deve utilizar MFA;

Art. 3º A DGTI deve estabelecer e manter um inventário de todas as contas gerenciadas, e neste 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. a DGTI é responsável por validar todas as contas ativas do órgão, a cada **90 (noventa) dias**.

Art. 4º A DGTI deve implementar a centralização da gestão de contas por meio de serviço de diretório e/ou identidade.

Art. 5º A DGTI deve estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, tal inventário deve ser revisado periodicamente.

Art.6º A DGTI deve centralizar o controle de acesso para todos os ativos de informação da organização por meio de um serviço de diretório ou provedor de SSO.

Art. 7º A DGTI deve 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. devem ser realizadas 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.

CAPÍTULO II

CONTA DE ACESSO LÓGICO E SENHA

Art. 8º Para utilização das estações de trabalho do IFRO, será obrigatório o uso de uma única identificação *(login)* e de senha de acesso, fornecidos pela DGTI, mediante solicitação formal pelo titular da unidade do requisitante.

I. a solicitação de acesso deve ser realizada através da Central de Serviços no Sistema Unificado de Administração Pública (SUAP);

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 titular da unidade do usuário deverá encaminhar solicitação, via Central de Serviços para a DGTI, que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Art. 9º O *login* e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pela DGTI quando constatada qualquer irregularidade.

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

Art. 10 O padrão adotado para o formato da conta de acesso do usuário são:

I. no caso de servidores: Matrícula SIAPE + senha;

II. no caso de alunos: Matrícula + senha;

III. terceirizados: CPF + senha;

Parágrafo único. Referente às contas relacionadas ao serviço de e-mail, esta deverá seguir o que está estabelecido no art. 20 da Instrução Normativa nº 2/2020/REIT - CGAB/REIT (SEI nº 1134430) e alterações da Instrução Normativa nº 4/2023/REIT - CGAB/REIT (SEI nº 1983895).

Art. 11 O padrão adotado para o formato da senha é o definido pela DGTI, 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 da identificação *(login)* de acesso à rede local deve seguir as regras de:

a) possuir tamanho mínimo de 8 (oito) caracteres, sendo obrigatório o uso de letras (maiúsculas e minúsculas), caracteres especiais ($, %, &,...) e números;

b) 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;

c) não utilizar termos óbvios, tais como: Brasil, senha, usuário, *password* ou *system*;

d) não reutilizar as últimas 3 (três) senhas.

II. a DGTI 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. 12 As senhas de acesso serão renovadas a cada 180 (cento e oitenta) 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.

CAPÍTULO III

BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

Art. 13 A conta de acesso 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. após desligamento do servidor, que deverá ser comunicado pelo setor de gestão de pessoas da unidade;

IV. quando da suspeita de mau uso dos serviços disponibilizados pelo IFRO ou descumprimento da Política de Segurança da Informação (POSIC) e normas correlatas em vigência.

V. após 50 (cinquenta) dias consecutivos sem movimentação pelo usuário.

Art. 14 O desbloqueio da conta de acesso à rede local será realizado apenas após solicitação formal do superior imediato do usuário ao setor da DGTI.

Art. 15 Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato ou do setor de Gestão de Pessoas.

Art. 16 A conta de acesso não utilizada pelo usuário há mais de 180 (cento e oitenta) dias poderá ser cancelada.

Art. 17 A DGTI 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. 18 O Setor responsável pela Tecnologia da Informação deve, sempre que possível, priorizar a revogação/desativação de contas com o objetivo de manter dados e *logs* para possíveis auditorias.

CAPÍTULO IV

MOVIMENTAÇÃO INTERNA

Art. 19 Quando houver mudança do usuário para outro setor ou o usuário ocupar uma nova função, os direitos de acesso à rede local referentes ao setor anterior devem ser revogados.

I. o novo superior imediato ou o setor responsável pela Gestão de Pessoas 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 ou do setor responsável pela Gestão de Pessoas.

CAPÍTULO V

CONTA DE ACESSO BIOMÉTRICO

Art. 20 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 IFRO deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO VI

ADMINISTRADORES

Art. 21 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 do setor responsável pela Tecnologia da Informação, devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede.

II. na necessidade de utilização de *login* com privilégios administrativos em determinado equipamento local, o pedido deverá ser realizado pelo superior imediato, que encaminhará a solicitação para o

setor responsável pela área de Tecnologia da Informação, o qual poderá negar os casos em que entender desnecessária a utilização.

III. se concedida a permissão ao usuário como administrador local na estação de trabalho, este 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 ou superior imediato;

VI. 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;

VII. excepcionalmente, poderão ser concedidas identificações *(login)* de acesso à rede de comunicação de dados a usuário externo em caráter temporário após apreciação do setor responsável pela Tecnologia da Informação;

VIII. o setor responsável pela Tecnologia da Informação deve implementar o MFA para todas as contas de administrador;

IX. o setor responsável pela Tecnologia da Informação 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.

CAPÍTULO VII

RESPONSABILIDADES

Art. 22 É de responsabilidade do superior imediato do usuário comunicar formalmente ao Setor responsável pela Gestão de Pessoas e o setor responsável pela Tecnologia da Informação o desligamento ou saída do usuário do IFRO para que as permissões de acesso à rede local sejam canceladas.

Art. 23 Caberá ao setor responsável pela Gestão de Pessoas do IFRO a comunicação imediata ao setor responsável pela Tecnologia da Informação sobre desligamentos, férias e licenças de servidores e estagiários, para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos.

Art. 24 Caberá ao setor responsável pela gestão de mão de obra terceirizada do IFRO a comunicação imediata ao setor responsável pela Tecnologia da Informação 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.

Art. 25 Caberá ao 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 IFRO.

Art. 26 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 IFRO.

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. 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;

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

Art. 27 É dever do 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 quanto a utilização da respectiva conta de acesso.

Art. 28 O usuário deve informar ao setor responsável pela Tecnologia da Informação qualquer situação da qual tenha conhecimento que configure violação dos termos desta política.

CAPÍTULO VIII

DISPOSIÇÕES GERAIS

Art. 29 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. 30 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, o setor responsável pela Tecnologia da Informação comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis;

II. o não cumprimento das determinações desta política sujeita o infrator às penalidades previstas na legislação e nos regulamentos internos do IFRO;

III. o descumprimento das disposições constantes nesta Política e nas Normas Complementares sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil;

IV. o usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos dessa política, fica sujeito à aplicação das penalidades previstas na Lei nº 8.112/1990, bem como na legislação pertinente ao assunto.

Art. 31 Esta Instrução Normativa entra em vigor na data de sua assinatura.

MOISÉS JOSÉ ROSA SOUZA
Reitor
Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO)

Documento assinado eletronicamente por **Moisés José Rosa Souza**, **Reitor(a)**, em 25/02/2025, às 18:54, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ifro.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2521036** e o código CRC **975F507C**.

Referência: Processo nº 23243.004192/2024-51 SEI nº 2521036