# INSTRUÇÃO NORMATIVA Nº 15/SETI/UFFS/2024

Dispõe sobre a normatização da criação e administração de contas de acesso no âmbito da Universidade Federal da Fronteira Sul.

O SECRETÁRIO ESPECIAL DE TECNOLOGIA E INFORMAÇÃO, no uso de suas atribuições legais, e, considerando:

a. O Decreto nº 10.332, de 28 de abril de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências;
b. a Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet);
c. a Portaria nº 216/GR/UFFS/2018, de 9 de março de 2018, que estabelece a Política de Segurança da Informação e Comunicações da UFFS (POSIC UFFS);
d. o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional;
e. o Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;
f. a Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;
g. a norma ABNT NBR ISO/IEC 27002:2022 que trata de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade: Controles de Segurança da Informação; e
h. a Portaria GSI/PR nº 93, de 18 de outubro de 2021, que aprova o glossário de segurança da informação,

RESOLVE:

**Art. 1º** Estabelecer as normas para a Criação e Administração de contas de acesso, em complemento às diretrizes estabelecidas pelo Capítulo II, da Portaria nº 216/GR/UFFS/2018, de 9 de março de 2018, que estabelece a Política de Segurança da Informação e Comunicações da UFFS (POSIC UFFS).

## CAPÍTULO I
## DO 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 Secretaria Especial de Tecnologia e Informação (SETI), baseado nas responsabilidades e tarefas de cada usuário.

**Art. 3º** Para fins desta Instrução Normativa, considera-se usuário de recursos de tecnologia da informação:
I - Servidores efetivos, TAEs e Docentes, cedidos, substitutos, temporários e ocupantes de cargos em comissão;
II - Discentes devidamente matriculados;
III - Terceirizados que exerçam funções técnico-administrativas, respeitada a vigência do contrato;
IV - Bolsistas e estagiários;
V - Convidados, visitantes, participantes de eventos ou membros externos vinculados a atividades acadêmicas na instituição.

**Art. 4º** O padrão da nomenclatura utilizada para a criação das credenciais de acesso seguirá normas do Governo Federal ou padrões definidos pela Secretaria Especial de Tecnologia da Informação da UFFS.

**Art. 5º** É vedada a criação de credenciais de acesso para unidades organizacionais ou que caracterizem acesso anônimo ou coletivo.
§1º Entende-se como credenciais de acesso as informações utilizadas para acesso a sistemas administrativos, acadêmicos, em recursos de navegação na rede ou outras situações nas quais a identificação do autor é necessária.
§2° Este artigo não se aplica à criação de contas de e-mail institucional.

**Art. 6º** As credenciais de acesso serão criadas da seguinte forma:
I - Automaticamente, ao final do processamento do cadastro do usuário no Sistema Integrado de Gestão - SIG, credencial única, pessoal e intransferível com fins de acesso aos sistemas e serviços da UFFS, denominada idUFFS para usuários listados no art. 3º, incisos I, II e IV;
II - Por solicitação do gestor do contrato de prestação de serviço para usuários listados no art. 2º, inciso III;
III - Por solicitação de usuários listados no art. 2º, inciso V, com aprovação de servidor responsável da UFFS, através do sistema CAV para uso da Rede.

## CAPÍTULO II
## DA CONTA DE ACESSO LÓGICO E SENHA

**Art. 7º** Para a utilização das estações de trabalho da UFFS, será obrigatório o uso da identificação (login) e senha de acesso criados através do idUFFS. Acessos a repositórios, criação de e-mails e outros sistemas de uso institucional devem ser solicitados via sistema de Atendimento de Chamados de Tecnologia da Informação (ATI), mediante solicitação formal pelo titular da unidade do requisitante.
§1° Os privilégios de acesso dos usuários à Rede Local devem ser solicitados pela unidade

requisitante ao qual o usuário está vinculado, limitando-se às atividades estritamente necessárias à realização de suas tarefas em conformidade com o art. 12 da Política de Segurança da Informação e Comunicações da UFFS (Portaria nº 216/GR/UFFS/2018).
§2° Na necessidade de utilização de perfil diferente do disponibilizado a chefia da unidade do usuário deverá encaminhar solicitação, via abertura de chamado no ATI, para a SETI avaliar. A SETI poderá negar a solicitação caso entenda ser indevida.

**Art. 8º** O acesso remoto deve ser realizado por meio de VPN – Rede Virtual Privada, após as devidas autorizações.

**Art. 9º** O idUFFS e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação ou compartilhamento, sob pena de serem bloqueados pela SETI, ou setor responsável por manter e auxiliar nas tarefas relacionadas à segurança da informação, quando constatada qualquer irregularidade.
**Parágrafo único.** Para retomar o acesso à rede, uma nova requisição deverá ser formalizada pela chefia da unidade do requisitante.

**Art. 10.** O padrão adotado para o formato da conta de acesso do usuário é a sequência *nome+ponto+último nome do usuário*, como por exemplo joão.silva.
**Parágrafo único.** Nos casos de homônimos, a PROGESP ou setor responsável pela criação do usuário realizará outra combinação utilizando o nome completo da pessoa para a qual a conta está sendo criada.

**Art. 11.** O padrão adotado para o formato da senha é o definido pela SETI, ou setor responsável por manter e auxiliar nas tarefas relacionadas à segurança da informação, que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição das últimas 5 (cinco) senhas anteriores.
§1° A formação da senha de identificação (login) para acesso à Rede Local deverá seguir as seguintes regras:
I - Possuir tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras e números;
II - Utilizar letras maiúsculas, minúsculas 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, usuário, password ou system;
V - Não reutilizar as últimas 5 (cinco) senhas anteriores.
§2° O local de troca de senha é unicamente via sistema id.uffs.edu.br seguindo as recomendações da página ou o campo "Ajuda".
§3° As senhas de acesso, da conta única e pessoal criada em id.uffs.edu.br, serão renovadas a cada 180 (cento e oitenta) dias, devendo o usuário ser informado antecipadamente a fim de que o próprio efetue a mudança.
§4° Caso o usuário não efetue a troca de senha no prazo estabelecido, o seu acesso à Rede Local será bloqueado até que uma nova senha seja configurada automaticamente no portal

id.uffs.edu.br.

## CAPÍTULO III
## DO BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

**Art. 12.** 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 - Quando houver suspeita de mau uso dos serviços disponibilizados pela UFFS, identificação de usuário como possível vetor de distribuição de malware na rede ou descumprimento da Política de Segurança da Informação e normas correlatas em vigência;
IV - Após 180 (cento e oitenta) dias consecutivos sem movimentação pelo usuário.

**Art. 13.** O desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do superior imediato do usuário através de chamado para SETI ou setor responsável por manter e auxiliar nas tarefas relacionadas à segurança da informação.

**Art. 14.** Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato ou da PROGESP.

**Art. 15.** A conta de acesso não utilizada há mais de 180 (cento e oitenta) dias poderá ser cancelada.

## CAPÍTULO IV
## DA MOVIMENTAÇÃO INTERNA

**Art. 16.** Quando houver mudança do usuário para outro setor, os direitos de acesso à Rede Local devem ser readequados via solicitação formal do seu novo superior imediato através do Sistema de Atendimento de Chamados ou da PROGESP.
**Parágrafo único**. Em caso de mudança para outro setor, os direitos de acesso antigos do usuário devem ser imediatamente cancelados através de solicitação do antigo superior imediato ou da PROGESP.

## CAPÍTULO V
## DOS ADMINISTRADORES

**Art. 17.** A utilização de identificação (login) com acesso ao perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.
§1° Somente os servidores técnico-administrativos da Secretaria Especial de Tecnologia e Informação, devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede.

§2° Tendo a necessidade de utilização de login com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para a SETI que poderá negar se entender desnecessária a utilização.
§3° 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 da SETI.
§4° Se constatada irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão.
§5° A identificação (login) com privilégio de administrador nos equipamentos locais será fornecida em caráter provisório, podendo ser renovada por solicitação formal da chefia da unidade requisitante.
§6° 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 aos equipamentos servidores e aos dispositivos de rede.
§7° Excepcionalmente, poderão ser concedidas identificações (login) de acesso à rede de comunicação de dados a terceiros com função de suporte em caráter temporário após apreciação do setor responsável dentro da SETI.

## CAPÍTULO VI
## DAS RESPONSABILIDADES

**Art. 18.** É de responsabilidade do superior imediato do usuário comunicar formalmente à PROGESP e à SETI sobre o desligamento ou saída do usuário da UFFS para que as permissões de acesso à Rede Local sejam canceladas.

**Art. 19.** Caberá à PROGESP da UFFS a inativação/exclusão do usuário no sistema da UFFS quando houver desligamentos.

**Art. 20.** É responsabilidade do gestor ou fiscal do contrato com terceiros a comunicação imediata sobre desligamentos e licenças de funcionários de empresas prestadoras de serviços, para a SETI efetuar o bloqueio momentâneo ou revogação definitiva da permissão de acesso aos recursos.
§1° Os serviços serão filtrados por programas de antivírus, anti-phishing e anti-spam. Caso alguma regra de configuração seja violada, os acessos de terceiros serão bloqueados e excluídos automaticamente.
§2° Nenhum fornecedor da área de TI terá acesso ao conteúdo das informações armazenadas nos equipamentos servidores da UFFS.

**Art. 21.** É de responsabilidade da SETI 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/dispositivo 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 informação e

à infraestrutura tecnológica da UFFS.

**Art. 22.** O usuário é responsável por todos os acessos realizados através de sua conta e por possíveis danos causados à Rede Local e a recursos de tecnologia custodiados ou de propriedade da UFFS.
§1° 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.
§2° 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.
§3° O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à Rede Local.

**Art. 23.** O usuário deve informar à SETI qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança, inclusive de terceiros.

**Art. 24.** É dever do usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a instituição, tais como:
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, a partir do definido no art. 30.
X - É vedada a utilização de credenciais institucionais para propósitos que não sejam relacionados ao vínculo que o usuário mantém com a instituição.

## CAPÍTULO VII
## DO USO DE PIN

**Art. 25.** Em complemento às medidas de segurança estabelecidas nesta política, o uso de PIN (Número de Identificação Pessoal) é obrigatório para autenticação em determinados sistemas e serviços da UFFS.
§1° O PIN é um código pessoal e exclusivo, utilizado como uma camada adicional de proteção no acesso aos recursos de tecnologia da informação.
§2° O PIN deve ser mantido em sigilo pelo usuário e não deve ser compartilhado com terceiros. É responsabilidade do usuário manter a confidencialidade do seu PIN, não compartilhando ou armazenando-o em locais de acesso público ou de fácil acesso a terceiros.
§3° O PIN é gerado de forma segura e cada usuário pode consultar o seu através do sistema SCI (Sistema de Credenciamento Institucional) fornecido pela SETI.

**Art. 26.** Em caso de suspeita de comprometimento do PIN, o usuário deve informar imediatamente a SETI, via Sistema de Abertura de Chamados, para que as medidas adequadas possam ser tomadas, como a redefinição do PIN e a análise de eventuais incidentes de segurança.

**Art. 27.** O uso indevido ou negligente do PIN pode resultar em sanções disciplinares, conforme previsto na legislação e nas normas da UFFS.

## CAPÍTULO VIII
## DAS DISPOSIÇÕES FINAIS

**Art. 28.** 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 Secretaria Especial de Tecnologia e Informação (SETI).

**Art. 29.** Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a SETI fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.
§1° Nos casos em que o autor da quebra de segurança for um usuário, a SETI comunicará os resultados ao superior imediato desse para adoção de medidas cabíveis.
§2° Ações que violem a POSIC da UFFS 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.
§3° Deverá ser instaurado processo administrativo disciplinar específico para apurar as ações que constituem em quebra das diretrizes impostas por esta Instrução Normativa e pela POSIC.
§4° A resolução de casos de violação/transgressões omissas nas legislações correlatas será resolvida pelo Comitê de Segurança da Informação (CSI) da UFFS.

**Art. 30**. A SETI e os usuários com credenciais de acesso terão até o dia 31 de Março de 2025 para se adequarem ao disposto no Art. 11 desta Instrução Normativa, incluindo o §3° do referido artigo.

**Art. 31.** Esta Instrução Normativa entra em vigor no dia 1º de abril de 2024.

Chapecó-SC, 25 de março de 2024.

CASSIANO CARLOS ZANUZZO
Secretário Especial de Tecnologia e Informação