**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**

**SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO**

# INSTRUÇÃO NORMATIVA POSIN/STI Nº 06, DE 24 DE NOVEMBRO DE 2025

Estabelece diretrizes e procedimentos para o controle de acesso no âmbito da Universidade Federal do Espírito Santo.

O SUPERINTENDENTE DE TECNOLOGIA DA INFORMAÇÃO DA UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO no uso das suas atribuições e considerando o disposto na Lei nº 13.709 (Lei Geral de Proteção de Dados Pessoais - LGPD), de 14 de agosto de 2018, no Programa de Privacidade e Segurança da Informação (PPSI) do Governo Federal e na Política de Segurança da Informação desta Universidade, resolve:

## CAPÍTULO I

## DISPOSIÇÕES PRELIMINARES

**Art. 1º** Esta Instrução Normativa estabelece diretrizes e procedimentos para o controle de acesso no âmbito da Universidade Federal do Espírito Santo (Ufes).

**Art. 2º** Para os fins desta Instrução Normativa, considera-se:

I. Controle de acesso: conjunto de procedimentos, recursos e meios utilizados para conceder ou bloquear o acesso a sistemas, aplicações, informações e ambientes;

II. Autenticação: processo de verificação da identidade digital do usuário;

III. Autorização: processo de verificação das permissões do usuário para execução de determinada ação;

IV. Credenciais de acesso: conjunto de informações utilizadas para autenticação do usuário, tipicamente composto por identificador de usuário e senha;

V. *Login* Único: sistema centralizado de gestão de identidades e acessos da Ufes.

VI. Múltiplo fator de autenticação: sistema de segurança que exige múltiplas formas de verificação para confirmar a identidade de um usuário, fortalecendo a proteção contra acessos não autorizados.

## CAPÍTULO II

## DOS PRINCÍPIOS E DIRETRIZES GERAIS

**Art. 3º** Conforme estabelecido na Política de Uso da Rede Ipê, a Ufes pode utilizar os Serviços de Redes disponíveis, suas facilidades de trânsito nacional e internacional, bem como usufruir dos

acordos de interconexão existentes entre a RNP e outras redes estaduais, regionais e internacionais para promoção de suas atividades de ensino, pesquisa e extensão.

**Art. 4º** Devido à natureza da Universidade, deve haver um livre fluxo de informação e intercâmbio de ideias nos ambientes acadêmicos. Por outro lado, existem impedimentos legais e éticos a determinadas ações, que implicam em responsabilidades atribuídas tanto à Ufes quanto ao usuário. Por isso, a Ufes deverá usar instrumentos para o rastreamento de tais ações, para ser possível a determinação do responsável por um ato ilícito.

**Art. 5º** As informações para autenticação são consideradas pessoais e intransferíveis, não podendo a Ufes armazená-las de forma que permita a sua recuperação, nem o usuário divulgá-las sob qualquer pretexto.

**Parágrafo único.** A autenticação é de caráter pessoal, não sendo possível a vinculação de autenticação ao cargo ocupado.

**Art. 6º** O acesso aos sistemas corporativos da Ufes utilizará, pelo menos, o *login* como forma de estabelecer permissões e gerenciar o que cada perfil do usuário poderá acessar, podendo ser exigidas etapas adicionais no processo de autenticação, como, por exemplo, o uso de múltiplo fator de autenticação.

**Parágrafo único.** Poderão ser estabelecidas exigências adicionais quanto às características do equipamento utilizado no acesso, incluindo o seu registro no domínio ou em um sistema de inventário.

## CAPÍTULO III

## DA POLÍTICA DE SENHA

**Art. 7º** A Ufes adotará uma gestão centralizada de credenciais de acesso cujo intuito é garantir um acesso facilitado aos portais corporativos da instituição.

**Parágrafo único.** A gestão do *Login* Único será feita através do sítio https://senha.ufes.br.

**Art. 8º** A senha deverá ter o tamanho mínimo de 8 (oito) caracteres e obedecerá aos seguintes critérios:

I. Utilizar ao menos uma letra maiúscula;

II. Utilizar ao menos uma letra minúscula;

III. Utilizar ao menos um caractere especial;

IV. Utilizar ao menos um número.

**Art. 9º** A Superintendência de Tecnologia da Informação (STI) se reserva no direito de proibir o uso de certas combinações como, por exemplo, data de nascimento, nome e outras informações pessoais que tornem a senha mais suscetível a ataques de engenharia social.

**Art. 10.** O usuário deverá trocar a senha periodicamente a cada 12 (doze) meses.

**Art. 11.** Deve-se evitar o acesso aos sistemas corporativos da Ufes a partir de computadores que possam estar com a segurança comprometida, assim como a partir de redes públicas ou redes privadas não confiáveis.

## CAPÍTULO IV

## DAS RESPONSABILIDADES DOS USUÁRIOS

**Art. 12.** São responsabilidades dos usuários:

I. Memorizar a sua senha, sendo essa de uso pessoal e intransferível;

II. Assumir total responsabilidade pelo seu uso das suas credenciais de acesso;

III. Jamais solicitar ou compartilhar as suas credenciais de acesso com outras pessoas;

IV. Cuidar para que ninguém observe o momento da digitação da senha;

V. Nunca aceitar ou solicitar ajuda de estranhos na digitação de senha;

VI. Comunicar imediatamente ao superior imediato e/ou a Superintendência de Tecnologia da Informação (STI) os casos de violação das credenciais, acidental ou não, e providenciar a sua substituição.

## CAPÍTULO V

## DAS RESPONSABILIDADES DA STI

**Art. 13.** São responsabilidades da Superintendência de Tecnologia da Informação (STI):

I. Prover e manter sistema de guarda, criação e alteração das credenciais de acesso dos usuários;

II. Garantir que a senha do usuário sempre trafegue por canal seguro (criptografada);

III. Bloquear ou desabilitar as credenciais em casos de suspeitas de fraudes, de mal-uso ou de determinação administrativa ou judicial;

IV. Armazenar as senhas em sistema seguro, de forma criptografada e irreversível;

V. Implementar mecanismos adicionais de segurança, podendo solicitar a colaboração do usuário.

## CAPÍTULO VI

## DO MONITORAMENTO

**Art. 14.** Os sistemas devem ser monitorados e eventos de segurança da informação devem ser registrados.

**Art. 15.** Os controles de acesso devem ser aplicados nos seguintes âmbitos:

I. Controle de Acesso Lógico: Os sistemas de TIC devem verificar a identidade dos usuários que tentam utilizar seus serviços. Podem ainda ser adotadas medidas adicionais para a concessão de acesso às informações sigilosas e para o acesso remoto, no âmbito da rede corporativa, por meio de canal seguro.

II. Controle de Acesso Físico: Os ativos de informação sensíveis devem ser protegidos fisicamente e acessíveis somente às pessoas autorizadas.

**Art. 16.** As credenciais utilizadas para o acesso aos ativos de informação e as instalações físicas da Ufes deverão ser revogadas ou suspensas quando não mais necessárias.

**Art. 17.** Dispositivos usados para autenticação, tais como cartões, *tokens* e afins, devem ser guardados com zelo e o seu extravio imediatamente comunicado à Superintendência de Tecnologia da Informação (STI) ou ao órgão emissor.

**Art 18.** Os registros de auditoria, que documentam as atividades de todos os usuários, exceções e outros eventos relacionados à segurança da informação, devem ser gerados e preservados por um período previamente acordado, visando apoiar investigações futuras e o monitoramento do controle de acesso. Esses registros (logs) de auditoria devem conter, sempre que aplicável, as seguintes informações:

I. Identificação dos usuários;

II. Datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (*logon*) e saída (*logoff*) no sistema;

III. Identidade do terminal ou, quando possível, a sua localização;

IV. Registros das tentativas de acesso ao sistema aceitas e rejeitadas;

V. Registros das tentativas de acesso a outros recursos e dados aceitos e rejeitados;

VI. Alterações na configuração do sistema;

VII. Uso de privilégios;

VIII. Uso de aplicações e utilitários do sistema;

IX. Arquivos acessados e tipo de acesso;

X. Endereços e protocolos de rede.

**Art 19.** Os registros (*logs*) de auditoria podem incluir dados pessoais e informações relacionadas a acessos não autorizados. É recomendável que medidas adequadas de proteção à privacidade sejam implementadas.

**Parágrafo único.** É recomendável, sempre que possível, que os administradores de sistemas e redes não possuam permissões para excluir ou desativar os registros (*logs*) referentes às suas próprias atividades.

**Art 20.** As falhas ocorridas devem ser registradas e analisadas sob demanda, e devem ser adotadas ações apropriadas. É importante existirem regras claras para o tratamento das falhas, incluindo:

I. Análise crítica dos registros (*log*) de falha para assegurar que as falhas foram satisfatoriamente resolvidas; e

II. Análise crítica das medidas corretivas para assegurar que os controles não foram comprometidos e que a ação tomada é autorizada.

**Art 21.** A coleta dos registros de erros e alertas deverá ser realizada, caso essa função esteja disponível no sistema.

**Art 22.** Os registros (*log*) de atividades dos operadores e administradores dos sistemas devem ser analisados criticamente caso ocorra algum incidente.

**Art 23.** Um sistema de detecção de intrusos poderá ser utilizado para monitorar a conformidade das atividades dos usuários na rede.

**Art 24.** Os recursos e informações de registros (*log*) poderão ser protegidos contra falsificação e acesso não autorizado. Estas medidas objetivam a proteção contra modificações não autorizadas e problemas operacionais com os recursos dos registros (*log*).

**Art 25.** Os registros (*log*) de auditoria deverão ser guardados como parte da política de retenção de registros ou devido à solicitação fundamentada para instrução de ação administrativa e/ou disciplinar.

**Art 26.** Devem ser estabelecidos procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento devem ser analisados regularmente.

**Art 27.** O nível de monitoramento requerido para os recursos individuais deve ser determinado por meio de uma análise/avaliação de riscos. As seguintes áreas devem ser consideradas:

I. Acessos autorizados, incluindo detalhes como o identificador do usuário (ID de usuário), a data e o horário dos eventos-chave, tipo do evento, os arquivos acessados e os programas ou utilitários utilizados;

II. Todas as operações privilegiadas, tais como o uso de contas privilegiadas (por exemplo: supervisor, *root*, administrador), a inicialização e finalização do sistema, e a conexão e desconexão de dispositivos de entrada e saída;

III. Tentativas de acesso não autorizadas, tais como ações de usuários com falhas ou rejeitados, ações envolvendo dados ou outros recursos com falhas ou rejeitadas, violação de políticas de acesso e notificações para *gateways* de rede e *firewalls* e alertas dos sistemas proprietários de detecção de intrusos;

IV. Alertas e falhas do sistema, tais como alertas ou mensagens do console, registro das exceções do sistema, alarmes do gerenciamento da rede e alarmes disparados pelo sistema de controle de acesso; e

V. Alterações ou tentativas de alterações nos controles e parâmetros dos sistemas de segurança.

**Art 28.** O uso de procedimentos de monitoramento é necessário para assegurar que os usuários estão executando somente as atividades que foram explicitamente autorizadas. A análise crítica dos registros (*log*) envolve a compreensão das ameaças encontradas no sistema e a maneira pela qual isso pode acontecer.

## CAPÍTULO VII

## DA SINCRONIZAÇÃO DOS RELÓGIOS

**Art 29.** Os relógios de todos os equipamentos e sistemas, na organização ou do domínio de segurança, devem ser sincronizados segundo a hora oficial.

**Art 30.** Sempre que um computador ou dispositivo de comunicação dispuser de um relógio de tempo real, é recomendável que o ajuste seja feito segundo o padrão acordado, como o Tempo Coordenado Universal (UTC) ou um padrão de tempo local.

**Art 31.** A interpretação correta do formato data/hora é importante para assegurar que o *timestamp* reflita a data/hora real.

**Parágrafo único.** Deve-se considerar as especificações locais, como, por exemplo, horário de verão.

**Art 32.** A configuração adequada dos relógios dos computadores é fundamental para garantir a precisão dos registros (*logs*) de auditoria, os quais podem ser necessários em investigações ou como evidências em processos legais ou disciplinares.

## CAPÍTULO VIII

## DA REDE SEM FIO (WI-FI)

**Art. 33.** A Ufes deverá oferecer uma solução de cobertura de rede sem fio.

**Parágrafo único.** Todos os equipamentos que forneçam acesso à rede Wi-Fi (*Access Points* – AP) deverão exigir a autenticação do usuário, não sendo permitido o uso de senhas compartilhadas.

**Art. 34.** Não serão permitidos equipamentos que forneçam acesso à rede Ufes, inclusive Wi-Fi (*Access Points* – AP), que não sejam os providos oficialmente pela Ufes ou que possuam autorização expressa da Superintendência de Tecnologia da Informação (STI).

**Parágrafo único.** A autorização considerará os mecanismos de segurança existentes no equipamento e os riscos à segurança de dados na infraestrutura de TIC da Ufes.

## CAPÍTULO IX

## DISPOSIÇÕES FINAIS

**Art. 35.** Compete à Superintendência de Tecnologia da Informação (STI) orientar e fiscalizar o cumprimento desta Instrução Normativa.

**Art. 36.** Os casos omissos serão resolvidos pelo Comitê de Governança Digital da Ufes.

**Art. 37.** Esta Instrução Normativa entra em vigor na data de sua publicação.

**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**

**SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO**

gov.br
Documento assinado digitalmente
PAULO ALEXANDRE LOBATO
Data: 08/12/2025 16:49:57-0300
Verifique em https://validar.iti.gov.br

**PAULO ALEXANDRE LOBATO**

Superintendente de Tecnologia da Informação