MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE LAVRAS
COMITÊ INTERNO DE GOVERNANÇA

RESOLUÇÃO NORMATIVA CIGOV Nº 2, DE 30 DE JUNHO DE 2022.

Dispõe sobre o controle de acesso lógico aos ativos de tecnologia da informação na Universidade Federal de Lavras (UFLA).

O COMITÊ INTERNO DE GOVERNANÇA DA UNIVERSIDADE FEDERAL DE LAVRAS, no uso de suas atribuições legais e regimentais, resolve:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Resolução Normativa define as normas relativas ao controle do acesso lógico aos ativos de tecnologia da informação da UFLA e não abrange o controle de acesso físico aos ativos de tecnologia da informação.

Art. 2º Esta Resolução Normativa se aplica a todos os usuários de serviços de tecnologia da informação institucionais, tais como: servidores do quadro permanente, comissionados, cedidos, requisitados, terceirizados, discentes, estagiários, prestadores de serviços, usuário de unidade/setor e pessoal de associação temporária que usam serviços de tecnologia da informação da UFLA com acesso restrito, ou acesso autenticado.

Art. 3º Esta Resolução Normativa tem o objetivo de estabelecer normas para minimizar riscos à gestão de credenciais de acesso lógico, tendo como objetivos específicos:

I- especificar um modelo mínimo de controle de acesso lógico para proteger os ativos de tecnologia da informação de acessos não autorizados;

II- legitimar o processo de definição de responsabilidades para usuários;

III- especificar procedimentos mínimos para o controle de acesso lógico aos ativos de tecnologia da informação.

Art. 4º O controle de acesso lógico a ativos de tecnologia da informação no âmbito da UFLA busca atender aos seguintes princípios:

I- privacidade: respeito à privacidade dos usuários e a finalidade de tratamento dos dados pessoais;

II- confidencialidade: garante que somente o usuário autorizado possa acessar o ativo de informação;

III- segurança: previne os riscos de acessos indesejáveis e vazamento de informações tratadas pela UFLA;

IV- autenticidade: garante que usuários anônimos acessem somente os ativos de tecnologia da informação considerados públicos;

V- interoperabilidade e otimização de recursos: uso de tecnologias ou processos que atendam o maior número de ativos de tecnologia da informação, quando for viável;

VI- não repúdio: acurácia e precisão na identificação das atividades do usuário.

Art. 5º Para os fins desta Resolução Normativa, considera-se:

I- acesso autenticado: acesso restrito que exige a identificação da pessoa, por meio do usuário e passe, para acessar um serviço de tecnologia da informação;

II- acesso lógico: direito de acesso na modalidade virtual a um ativo de tecnologia da informação;

III- acesso lógico privilegiado: acesso lógico privilegiado é um tipo específico de acesso à aplicação de infraestrutura computacional ou de configuração de serviços em ativos de tecnologia da informação sob responsabilidade da DGTI, incluindo, mas não se limitando a: sistema operacional, servidor, sistema gerenciador de banco de dados, acesso remoto a servidores, configuração de micro serviços e acesso à serviço que trata dados pessoais;

IV- aposentado: ex-servidor do quadro permanente que encerrou suas atividades funcionais na UFLA;

V- área de negócio: unidade ou setor que gerencia um processo de trabalho específico, de área meio ou finalística;

VI- ativo de tecnologia da informação: recurso digital que constitui um sistema de informação, tais como: dados, serviço de conectividade, aplicativo, informação e programas de computador;

VII- cancelamento de usuário: processo para desabilitar a credencial de um usuário para que o mesmo não possa mais se autenticar como usuário válido;

VIII- controle de acesso lógico: operação de conceder, alterar, analisar e revogar direito de acesso a um ativo de tecnologia da informação;

IX- egresso: pessoa que concluiu formação na UFLA;

X- gestão de usuário: operações de cadastro, alteração, análise ou cancelamento de usuário;

XI- passe: padrão de controle para confirmar a identidade do respectivo usuário ao ativo de tecnologia da informação, tais como: senha, biometria e criptografia;

XII- processo de negócio: conjunto de atividades ou tarefas estruturadas para produção de um resultado de valor para o cliente, por meio da entrega de um serviço ou produto, conduzidos por uma unidade ou setor;

XIII- regras de negócios: declarações sobre a forma de operar um processo de negócio ou uma rotina;

XIV- revogação de acesso: cancelamento do direito de acesso lógico do usuário a um ativo de tecnologia de informação;

XV- setor: unidade da estrutura organizacional da UFLA;

XVI- senha: conjunto de caracteres secretos utilizado como sinal de reconhecimento de uma pessoa;

XVII- usuário: identificação de uma pessoa na base de dados de um sistema por meio de um identificador único denominado “nome de usuário” para o qual pode ser associado direito de acesso lógico;

XVIII- vínculo: relação direta com a UFLA. Discentes egressos, servidores aposentados e pensionistas possuem vínculo, apesar desse vínculo representar o encerramento de um vínculo anterior que foi concluído. Funcionários terceirizados, servidores demitidos, transferidos ou exonerados não possuem vínculo. Discentes jubilados e que abandonaram o curso não são considerados egressos, pois não concluíram o vínculo anterior;

XIX- vínculo funcional: vínculo formal e legítimo de pessoa ativa no quadro permanente de servidores da UFLA.

CAPÍTULO II
DOS TRATAMENTOS DE INCIDENTES

Art. 6º O processo de tratamento de incidentes de segurança deve considerar eventual violação deste normativo de controle de acesso lógico.

Art. 7º A permissão de acesso lógico que não implementar padrão de controle a partir de um dispositivo criptográfico, biometria ou senha deve ser tratada como incidente de segurança.

Art. 8º Pedido de análise de operação de um comportamento de usuário deve ser registrado pela área de negócio responsável pelo serviço ou por um grupo de trabalho que foi formalmente designado para investigar um incidente envolvendo o respectivo usuário.

CAPÍTULO III
DAS RESPONSABILIDADES DOS ENVOLVIDOS

Art. 9º A Diretoria de Gestão de Tecnologia da Informação (DGTI) é a unidade responsável por assegurar a execução das normas do controle de acesso lógico aos ativos de tecnologia da informação.

Art. 10. A área de negócio deve definir o direito de acesso lógico dos usuários ao respectivo serviço de tecnologia da informação por ela gerenciado.

Art. 11. O acesso lógico é atribuído a um usuário em observância às regras de negócios especificadas pelo operador do processo de negócio.

Art. 12. Todo direito de acesso lógico está condicionado à aprovação, ou validação, da respectiva pessoa responsável pelo processo de negócio, tais como: chefia de unidade organizacional, operador de dados ou coordenador de projeto registrado na instituição.

Art. 13. O controle de acesso lógico a ativo de tecnologia da informação mantido pela DGTI é executado:

I- pela DGTI quando o direito de acesso lógico habilitar simultaneamente processos de negócio gerenciados por diferentes áreas de negócio; ou quando habilitar opções de configuração global do ativo de tecnologia da informação; ou habilitar recurso privilegiado para administração de ativo de tecnologia da informação, ou quando somente a DGTI possuir acesso à ferramenta de controle;

II- pela área de negócio responsável por determinado serviço quando o acesso lógico habilitar somente o processo de negócio ou serviço gerenciado pela respectiva área de negócio;

III- automático quando o direito de acesso lógico estiver bem definido para um grupo de usuários e legitimado institucionalmente, tais como: chefia de setor, servidor técnico administrativo, servidor docente, discente de graduação e discente de pós-graduação.

Art. 14. A gestão de usuário para pessoas com algum tipo de vínculo com a UFLA é executada:

I- pela DGTI quando o tratamento dos dados pessoais do usuário não é feito em um processo meio ou finalístico da instituição; ou quando somente a DGTI possuir acesso ao recurso para registrar o respectivo usuário;

II- pela área de negócio responsável pelo serviço quando uma pessoa não possui usuário registrado na base centralizada para autenticação de usuários e a respectiva área de negócio for responsável pelo processo no qual a pessoa estabelece sua primeira interação com um processo da instituição.

Art. 15. Em relação à gestão de usuários e o controle de acesso lógico, a DGTI é responsável por:

I- disponibilizar ferramentas para gestão de usuários e controle de acesso lógico dos usuários;

II- buscar melhoria contínua para os processos de autenticação e controle de acesso lógico;

III- auxiliar as áreas de negócio na gestão de usuários, bem como fornecer treinamentos quando necessário;

IV- analisar e auditar de forma crítica os direitos de acesso lógico dos usuários, em conformidade com legislação vigente, os normativos de segurança da informação e comunicação, proteção de dados pessoais da UFLA e às boas práticas de segurança da informação;

V- divulgar e sensibilizar o normativo de controle de acesso lógico aos usuários ativos da instituição.

Art. 16. Todo serviço de tecnologia da informação mantido pela UFLA, adquirido ou desenvolvido a partir da publicação deste normativo, deve priorizar o uso de controle de acesso lógico com o uso da base de dados centralizada para autenticação institucional, bem como definir as responsabilidades para execução do controle de acesso lógico e gestão de usuário.

Art. 17. As informações de direitos de acesso lógico a ativo de tecnologia da informação devem estar disponíveis para o gestor da área de negócio responsável pelo tratamento de dados do respectivo ativo e pela chefia imediata do usuário. As informações de direito de acesso lógico são, mas não se limita a, usuários com o acesso lógico e descrição do direito de acesso.

CAPÍTULO IV
DO ACESSO ÀS REDES E AOS SERVIÇOS DE REDE

Art. 18. O acesso lógico à rede e ao serviço de rede é concedido somente a usuário previamente autorizado.

Art. 19. A identificação do acesso lógico e atividades do usuário devem ser registradas para auxiliar na responsabilização das ações do usuário.

Art. 20. As regras de autorização do acesso às redes e aos serviços de rede devem ser complementadas em normativo específico, mantendo consonância com esta Resolução Normativa.

CAPÍTULO V
DO REGISTRO E CANCELAMENTO DE USUÁRIO

Art. 21. Uma pessoa deve ter somente uma identificação de usuário ativa no serviço de tecnologia da informação, exceto quando não for possível implementar tal recurso, porém a não implementação deve ser justificada.

Art. 22. Todo usuário deve atestar conhecimento sobre suas responsabilidades em relação aos normativos de segurança da informação e privacidade, no primeiro acesso, anualmente e sempre que houver alterações nestes normativos.

Art. 23. O uso compartilhado de usuário é permitido somente quando este é necessário por razões específicas de um processo de negócio, desde que:

I- gestão de risco do compartilhamento, em conformidade com o normativo de segurança da informação e privacidade de dados;

II- esteja formalmente documentado e com responsabilização do gestor do processo de negócio;

III- aprovado pelo gestor de segurança da informação ou gestor de infraestrutura computacional.

Art. 24. O cancelamento de todos os direitos de acesso vigentes do usuário deve ocorrer de forma imediata, e geral em todos os ativos de tecnologia da informação, quando a pessoa encerrar o vínculo institucional, salvo exceções previstas em normativo específico.

Art. 25. A gestão de usuário e passe para acesso a ativos de tecnologia da informação devem estar em conformidade com o normativo relativo à gestão de credenciais de acesso.

Art. 26. A gestão de usuário deve considerar que:

I- O usuário não pode ser excluído, ele deve ser inativado ou desabilitado, salvo exceções previstas em normativo ou procedimento específico para o respectivo ativo onde o usuário está registrado;

II- A inativação pode fundamentar-se, também, em análise crítica que apresenta o risco do usuário ativo à segurança da informação ou desconformidade com algum normativo vigente;

III- A inativação automatizada de usuário deve existir quando houver regras de negócio bem definidas e implementação viável em programa de computador.

Art. 27. O controle de acesso lógico deve utilizar uma base centralizada para autenticação dos usuários, exceto quanto o ativo não permitir a interoperabilidade com a base central de autenticação institucional.

Art. 28. O usuário que tiver algum dado da conta institucional envolvido em vazamento de dados terá a conta institucional suspensa até que seja feito troca das credenciais de acessos.

Art. 29. A concessão de acesso lógico deve ser efetivada mediante autorização ou consentimento do respectivo responsável pelo processo de negócio que gerencia o ativo de tecnologia de informação a ser acessado.

Art.30. A concessão de acesso lógico deve estar em conformidade com os normativos e procedimentos institucionais relativos à segurança da informação e privacidade de dados.

Art. 31. O processo de gestão e concessão de acesso lógico ao usuário deve ser padronizado e publicado de forma clara e objetiva pelo gestor de tecnologia da informação e pela área de negócio que opera o registro do usuário.

Art. 32. É dever da chefia imediata comunicar formalmente a mudança de lotação ou desligamento de usuário(a) aos responsáveis pela gestão do direito de acesso lógico, bem como os direitos de acesso lógico a serem cancelados em decorrência da respectiva mudança da pessoa na unidade;

Art. 33. As ações, listadas a seguir, devem ser tomadas em relação à concessão do acesso lógico do usuário que tiver a função, atividade ou lotação institucional alteradas:

I- O nível de acesso lógico deve ser revogado ou readequado à nova situação funcional;
II- Os direitos de acesso de um usuário devem ser revisados periodicamente pela chefia imediata e ajustados de acordo com mudanças.

Art. 34. A mudança para outro vínculo com a instituição acarretará na revogação do direito de acesso lógico aos ativos de tecnologia da informação, concedidos ao vínculo anterior, considerando que:

I- são consideradas mudanças de vínculo: discentes para egressos e servidores para aposentados;
II- os direitos de acesso lógico concedidos após mudança de vínculo serão tratados em procedimentos específicos pelos gestores dos respectivos processos de negócios.

Art. 35. Os direitos de acesso lógico aos ativos de tecnologia da informação devem ser analisados criticamente em intervalos de 12 meses, no máximo, pelos gestores dos respectivos processos de negócios e pelas chefias imediatas dos usuários para os quais há concessão de acesso lógico.

Art. 36. Usuário com vínculo ativo que não realizar autenticação por meio da central de autenticação em período superior a 180 dias pode ser inativado e ter seus direitos de acesso cancelados.

CAPÍTULO VI
DA GESTÃO DO DIREITO DE ACESSO LÓGICO PRIVILEGIADO

Art. 37. A gestão de direitos de acesso lógico privilegiado deve atender requisitos complementares, tais como:

I- o tempo para expirar os direitos de acesso lógico privilegiado a uma aplicação pode ser modificado, considerando o limite exposto neste normativo;

II- ter um processo de gestão de direito de acesso lógico divulgado no catálogo de serviços ou portal da área responsável pelo processo de gestão;

III- concedido somente ao usuário de pessoa com vínculo funcional vigente e legítimo com a instituição, ou para usuário de pessoa com vínculo institucional vigente que tenha autorização de pessoa com vínculo funcional vigente (autorizado formalmente) e que detenha responsabilidade sobre o respectivo processo de negócio;

IV- consentimento de responsabilidade e condição técnica para fazer uso do direito de acesso;

V- aprovação prévia pelo gestor de segurança da informação ou gestor de infraestrutura computacional;

VI- manter registro organizado das pessoas cujo usuário possui o direito de acesso lógico privilegiado e o tempo com a respectiva permissão;

VII- revisar a relação de usuários com acesso lógico privilegiado no período máximo de 12 meses após a última revisão e manter relatório das revisões de acesso lógico privilegiado;

VIII- não remover acessos lógicos privilegiados sem confirmar a necessidade de manter o respectivo acesso para o usuário;

IX- usar login único ou manter usuários com acesso privilegiado ao ambiente de infraestrutura computacional com o mesmo login de usuário aos sistemas institucionais.

Art. 38. Somente a área responsável por um processo de negócio pode ordenar ou ter acesso total para operar cadastro, exclusão, edição e alteração de dados no respectivo processo.

§ 1º A DGTI poderá realizar tais operações, com requisição formalizada pela chefia da respectiva área de negócio, quando não existir funcionalidade em sistema de informação para esse fim e a operação não representar violação de conformidade legal, segurança da informação ou privacidade.

§ 2º Os dados de identificação do usuário que realiza uma operação de tratamento de dados devem ser registrados no respectivo sistema de informação, bem como os dados tratados.

CAPÍTULO VII
DA GESTÃO DA INFORMAÇÃO DE AUTENTICAÇÃO SECRETA DE USUÁRIO

Art. 39. A complexidade mínima para as credenciais armazenadas e a temporalidade para a sua alteração devem seguir as diretrizes definidas pelo normativo institucional de gestão de credenciais de acesso.

Art. 40. Informações como senhas ou certificados digitais de acesso devem ser armazenadas de forma criptografada e medidas de segurança devem garantir que apenas usuários autorizados tenham acesso ao cadastro.

Art. 41. Estabelecer procedimento para analisar a identidade do usuário antes de fornecer qualquer informação associada à autenticação do usuário.

CAPÍTULO VIII
DA ANÁLISE CRÍTICA E AJUSTE DOS DIREITOS DE ACESSO DE USUÁRIO

Art. 42. O acesso lógico pode ser analisado criticamente pela DGTI e deve incluir os procedimentos para:

I- Catalogar os acessos lógicos privilegiados, bem como as modificações nestes;

II- Garantir que o direito de acesso lógico privilegiado esteja atribuído a um identificador de usuário igual ao identificador utilizado nas atividades normais de negócio;

III- Garantir que o direito de acesso lógico esteja em conformidade com a autorização que motivou o respectivo acesso;

IV- Revisar acesso lógico privilegiado em intervalos de tempo inferior ao limite determinado neste normativo.

CAPÍTULO IX
DAS VIOLAÇÕES, PENALIDADES E SANÇÕES

Art. 43. A desobediência ou violação desta norma implicará em sanções administrativas nos termos da lei, normas complementares, regimentos e resoluções internas, sem prejuízo de outras previstas nas esferas cível e penal.

Parágrafo Único. O procedimento para a aplicação das penalidades e/ou sanções seguirá o rito específico da legislação, norma, regimento ou resolução a que corresponder o caso concreto.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 44. A elaboração e a atualização deste documento são de responsabilidade da DGTI.

Art. 45. Os casos omissos e as dúvidas surgidas na aplicação do disposto no normativo de controle de acesso lógico deverão ser analisados pela DGTI.

Art. 46. A presente Resolução Normativa passa a vigorar a partir do dia 1º de setembro de 2022, revogando-se as disposições em contrário.

JOÃO CHRYSOSTOMO DE RESENDE JÚNIOR
Presidente