MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DA INTEGRAÇÃO LATINO-AMERICANA

COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

RESOLUÇÃO Nº 4, DE 03 DE MARÇO DE 2020

Aprova a presente normativa com o propósito de normatizar o uso de credenciais de acesso aos recursos de Tecnologia da Informação e Comunicação da UNILA

O PRESIDENTE DO COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - CGTIC, designado pela Portaria nº 29/2019/GR/UNILA, no exercício de suas atribuições, e
CONSIDERANDO os princípios da governança de TIC, expressos na Portaria ME/SEDGGD/SGD 778, de 4 de abril de 2019, foco nas partes interessadas, TIC como ativo estratégico, gestão por resultados, transparência, prestação de contas e responsabilização e conformidade;
CONSIDERANDO a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);
CONSIDERANDO a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet);
CONSIDERANDO a iniciativa 3.2 de aperfeiçoar a governança de TIC, identificada no PETIC 2019-2021;
CONSIDERANDO a iniciativa 5.2 de aperfeiçoar a gestão de segurança da informação da instituição, identificada no PETIC 2019-2021;
CONSIDERANDO o Glossário de Segurança da Informação aprovado na Portaria GSI/PR nº 93, de 26 de setembro de 2019; e
CONSIDERANDO a ABNT NBR ISO/IEC 27002:2013, norma de boas práticas para Política de controle de acesso, resolve:

DAS DISPOSIÇÕES GERAIS

Art. 1º Aprovar a presente normativa com o propósito de normatizar o uso de credenciais de acesso aos recursos de Tecnologia da Informação e Comunicação da UNILA.

Art. 2º Este documento passa a compor a Política de Segurança da Informação - POSIN e alcança toda a UNILA.

Art. 3º Para fins desta normativa, entende-se por:
I - Credencial de acesso: também conhecida como “conta de acesso”, é um mecanismo de segurança que identifica univocamente a pessoa vinculada à UNILA, acessada por meio de um “nome de usuário” e uma senha ou pelo PIN correspondente, com a finalidade de proporcionar acesso aos recursos e serviços, de acordo com seu perfil de usuário;
II - Número de Identificação Pessoal - PIN: é uma forma de acesso simplificado da credencial de acesso, que substitui a necessidade de usar um nome de usuário e senha por um código numérico, portanto, são recursos análogos representados neste documento simplesmente por “credencial de acesso”;
III - Comitê de Segurança da Informação - CSI: órgão responsável pelo assessoramento nos assuntos relativos à gestão da segurança da informação;
IV - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - Etir: também conhecida como CSIRT (Computer Security Incident Response Team) é a equipe que centraliza as atividades de tratamento e resposta de incidentes de segurança da informação no âmbito da instituição.
TÍTULO I
DAS CREDENCIAIS DE ACESSO

Art. 4º A credencial de acesso permite a utilização de serviços fornecidos pela instituição, listados no catálogo de serviços da área de TIC, a exemplo de:
I - internet;
II - correio eletrônico;
III - acesso às estações de trabalho administrativas e de laboratórios de informática;
IV - impressoras;
V - sistemas institucionais;
VI - conexão a rede wireless da universidade e de instituições públicas e particulares aderentes ao serviço eduroam;
VII - acesso a Comunidade Acadêmica Federada (CAFe).

Art. 5º Todo o acesso a recursos de tecnologia da informação utilizados na UNILA deve estar associado a uma pessoa física e atrelado inequivocamente a um documento de identificação civil.
Parágrafo único. Poderão ser armazenados os registros de acesso de aplicação e registros de conexão, nos termos da legislação vigente.

Art. 6º A credencial de acesso é pessoal e intransferível, vedado o seu compartilhamento, sob pena de responsabilização pelos atos decorrentes do uso indevido.

Art. 7º A existência de credencial de acesso não pressupõe o acesso à todos os sistemas e recursos de tecnologia da informação.
Parágrafo único. Os perfis de acesso aos recursos serão concedidos conforme o vínculo institucional, competências e atribuições e/ou política de uso específica do serviço.

Art. 8º Credenciais poderão ser criadas para:
I - servidores efetivos, 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 - pós-doutorandos devidamente registrados na Pró-reitoria de Pesquisa e Pós-Graduação (PRPPG);
V - convidados, visitantes, participantes de eventos ou membros externos vinculados a atividades acadêmicas na instituição.
Parágrafo único. O padrão da nomenclatura utilizada para a criação das credenciais de acesso seguirá normas de governo ou padrões definidos pela área de Tecnologia da Informação.

Art. 9º É vedada a criação de credenciais de acesso para unidades organizacionais ou, que caracterizem acesso anônimo ou coletivo.

Art. 10 As credenciais de acesso serão criadas da seguinte maneira:
I - automaticamente, ao final do processamento do cadastro do usuário no Sistema Integrado de Gestão - SIG, para usuários relacionados no Art. 8º, Incisos I e II;
II - por solicitação do gestor do contrato de prestação de serviço, para usuários relacionados no Art. 8º, Inciso III;
III - por solicitação do servidor responsável pela atividade, para usuários relacionados no Art. 8º, Inciso IV e V.
§ 1º As solicitações tratadas no Art. 10, Incisos II e III devem ser feitas por meio da Central de Serviços, com antecedência mínima de 24 horas, informando nome completo, número do documento de identificação, endereço de e-mail de quem utilizará a credencial de acesso, além do prazo necessário.
§ 2º Compete ao servidor responsável pela requisição fazer a conferência da veracidade dos dados cadastrais contidos na solicitação de criação das credenciais.
§ 3º No momento do cadastro do usuário, será gerada automaticamente uma senha aleatória e temporária, que será enviada para o endereço de e-mail pessoal registrado no Sistema Integrado de Gestão - SIG. A senha temporária deverá ser trocada no primeiro acesso do usuário.

Art. 11 A credencial de acesso poderá ser suspensa quando:
I - for detectado uso com finalidade diversa às atividades institucionais;
II - identificado o uso compartilhado;
III - em casos de determinação judicial ou administrativa, pelos respectivos órgãos de controle;
IV - identificadas sucessivas tentativas de acesso mal sucedidas a recursos de tecnologia da informação.
Parágrafo único. A equipe de TIC poderá suspender a credencial de acesso de maneira preventiva, quando for identificado o seu comprometimento ou uso diverso ao disposto nesta normativa.

Art. 12 O desbloqueio da credencial de acesso ocorrerá:
I - ao final de procedimento de verificação de responsabilidade, de acordo com regimento disciplinar ou por solicitação de servidor ou unidade competente, para situação prevista no Art. 11, Incisos I e II;
II - por solicitação da autoridade competente para a situação prevista no Art. 11, Inciso III;
III - mediante troca de senha para a situação prevista no Art. 11, Inciso IV.
Parágrafo único. O desbloqueio temporário, ainda que não concluído ou ensejado procedimento de verificação de responsabilidade, não encerra as obrigações do usuário por qualquer ato decorrente do uso indevido da sua credencial de acesso, nos casos de dolo ou culpa.

Art. 13 As credenciais de acesso serão desativadas:
I - automaticamente após processamento do cadastro pelo Sistema Integrado de Gestão - SIG, ou imediatamente a pedido da Pró-Reitoria de Gestão de Pessoas (PROGEPE), quando da exoneração, demissão ou desligamento de usuários com vínculo funcional;
II - após seis meses de desligamento ou da conclusão do curso dos usuários elencados no Art. 8°, Inciso II;
III - após três meses de inatividade da credencial de acesso;
IV - após o registro de final de contrato, para os usuários relacionados no Art. 8°, Inciso III;
V - ao fim do prazo de vigência da credencial de acesso para os usuários elencados no Art. 8°, Incisos IV e V.
§ 1º Não haverá aviso prévio ao usuário sobre a desativação da credencial de acesso.
§ 2º Após a desativação, a credencial de acesso somente poderá ser reativada se atender aos critérios de credenciamento inicial ou por solicitação justificada de unidade competente.

TÍTULO V
DOS DEVERES E RESPONSABILIDADES DO TITULAR

Art. 14 É dever do titular da credencial de acesso:
I - zelar pela confidencialidade da sua senha;
II - encerrar ou bloquear a sessão com sistemas, computadores e dispositivos sempre que se ausentar da estação de trabalho;
III - utilizar senhas fortes;
IV - alterar a senha sempre que existir qualquer indicação de possível comprometimento dos dados de qualquer serviço de TIC ou da própria senha;
V - utilizar suas credenciais somente para fins designados e para os quais estiver devidamente autorizado, de acordo com suas funções e responsabilidades;
VI - substituir a senha inicial gerada pelo sistema, assim que recebê-la;
VII - solicitar o cancelamento das credenciais ou perfis de acesso, suas ou de seus subordinados, quando elas não forem mais necessárias ou quando houver revogação de competência;
VIII - conhecer e seguir as regras estabelecidas nesta normativa, bem como os informativos submetidos pelos órgãos responsáveis pela segurança da informação na UNILA;
IX - verificar os registros de utilização do PIN, que são enviados para a sua conta de e-mail, e denunciar caso perceba o uso não autorizado;
X - denunciar os casos de violação das credenciais de acesso e mal uso dos recursos de tecnologia da informação;
XI - fazer uso ético e racional dos recursos de tecnologia da informação;
XII - manter seu endereço de e-mail pessoal atualizado no Sistema Integrado de Gestão - SIG, para os casos de recuperação de senha.
Parágrafo único. A recuperação de senha será disponibilizada por meio da opção i) “Recuperar Senha” presente nos serviços de TIC da UNILA, ou ii) pessoalmente junto à unidade de TIC local, munido de documento de identificação civil com foto, ou iii) por videoconferência, munido de documento de identificação civil com foto, assegurada a possibilidade de realizar a identificação pessoal.

Art. 15 Denúncias sobre mal uso ou ataques a credenciais de acesso poderão ser encaminhadas a Etir, pelo e-mail csirt@unila.edu.br.

TÍTULO IV
DISPOSIÇÕES FINAIS

Art. 16 Esta normativa aplica-se para as credenciais de acesso já existentes bem como para os novos credenciamentos a partir da sua publicação.

Art. 17 Casos omissos serão tratados pelo CSI.

Art. 18 Esta Resolução entra em vigor em 1º de outubro de 2020, nos termos do Art. 4º do Decreto nº 10.139/2019.

GLEISSON ALISSON PEREIRA DE BRITO

Observações:

Publicada no Boletim de Serviço nº 74, de 26 de agosto de 2020.