Art. 20. Durante o Período Especial Emergencial ficam mantidas as garantias de atendimento e normas especiais para a acessibilidade e inclusão de pessoas com deficiência, em especial o disposto na Resolução nº 11/2014/Cosuen.

Art. 21. As regras para o aproveitamento da carga horária Docente dedicada as aulas durante o Período Especial Emergencial, para a distribuição de atividades no Plano Individual de Trabalho Docente e para os relatórios de estágio funcional e progressão Docente serão tratadas em regulamentação própria emanada pela Comissão Permanente de Pessoal Docente (CPPD), a ser apresentada em até 30 (trinta) dias ao Conselho Universitário, após aprovação desta Resolução.
Parágrafo único. A carga horária Docente durante o Período Especial Emergencial deverá obrigatoriamente ser considerada nos processos de progressão funcional, sem prejuízo aos(às) Docentes que não puderem aderir.

Art. 22. Caso o Período Especial Emergencial seja suspenso, as turmas em andamento terão asseguradas sua continuidade no formato remoto ou a transferência para a forma presencial, a critério do(a) Docente, consultada a turma, com apresentação de novo cronograma e ajustes do Plano de Ensino, a serem devidamente aprovados pelos Colegiados dos Cursos de Pós-Graduação.
Parágrafo único. A consulta de que trata o caput deste Artigo deve ser realizada pelo(a) Docente e registrada, sendo que para fins de alteração de formato de oferta, deverá haver concordância, da maioria simples dos alunos regulares da turma.

Art. 23. O Calendário Acadêmico de 2020 será rediscutido e retomado no momento e nas condições necessárias para garantir a segurança sanitária da comunidade universitária na retomada das atividades presenciais diante do cenário epidemiológico da pandemia da Covid-19.
§ 1º Nos casos em que todo(a)s os(as) Discentes matriculados(as) em um componente curricular no semestre 2020.1 integralizaram tal componente durante o Período Especial Emergencial, as turmas abertas do período letivo 2020.1 poderão ser finalizadas/encerradas quando o calendário for retomado.
§ 2º Na retomada do Calendário Acadêmico do período letivo 2020.1, ficará assegurado novo período de ajuste de matrícula a todos(as) os(as) Discentes, mantidos, preferencialmente, os horários já registrados.

Art. 24. Será considerado o prazo de até 180 (cento e oitenta) dias após a publicação desta Resolução para todas as adequações que se fizerem necessárias no Sigaa.

Art. 25. A presente Resolução não suprime as normas vigentes, exceto pelas disposições em contrário a esta.

Art. 26. Os casos omissos serão resolvidos pela PRPPG, em diálogo com a respectiva Coordenação dos Programas de Pós-graduação e em grau de recurso na Comissão Superior de Ensino - Cosuen.

Art. 27. Esta Resolução entra em vigor na data de sua publicação no Boletim de Serviço, considerada a urgência justificada no presente expediente, nos termos do Art. 4º do Decreto nº 10.139, de 28 de novembro de 2019.

PABLO HENRIQUE NUNES
26 de agosto de 2020

COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES

RESOLUÇÃO Nº 3/2020/CGTIC

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 a Lei nº 12.527, de 18 de novembro de 2011 (Lei e Acesso à Informação);
CONSIDERANDO o Decreto nº 7.724, de 16 de maio de 2012 (Regulamenta a Lei nº 12.527, de 18 de novembro de 2011);
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 NC 14/IN01/DSIC/SCS/GSIPR, que estabelece princípios, diretrizes e responsabilidades no tratamento da informação em ambiente de computação em nuvem;
CONSIDERANDO a Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação;
CONSIDERANDO o objetivo estratégico OE3 de aperfeiçoar a governança de TIC, identificado no PETIC 2019-2021; e
CONSIDERANDO a iniciativa 5.2 de aperfeiçoar a gestão de segurança da informação da instituição, identificada no PETIC 2019-2021, resolve:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Aprovar a presente normativa, com a finalidade de estabelecer diretrizes, normas e regulamentos para a utilização dos serviços de armazenamento e compartilhamento de arquivos na UNILA.

Art. 2º Esta norma deverá ser observada em conjunto aos demais termos de uso de cada serviço de armazenamento e compartilhamento de arquivos utilizados pela UNILA.

Art. 3º Para efeitos desta normativa, considera-se:
I - serviços de armazenamento e compartilhamento de arquivos: doravante denominado serviços, conjunto de equipamentos e softwares que permitem que usuários possam armazenar e compartilhar arquivos, entre si e/ou entre grupos de usuários.
II - Central de Serviços: o canal de comunicação da área de TIC com os usuários que utilizam os serviços e produtos de TIC da UNILA.
III - credencial de acesso: mecanismo de segurança que identifica univocamente a pessoa vinculada à UNILA, com a finalidade de proporcionar acesso à recursos e serviços de TIC.
IV - unidade requisitante: macrounidade da UNILA demandante para a área de TIC.
V - requisitante: servidor representante da unidade requisitante, indicado pela autoridade competente.
VI - área privativa do usuário: local onde ficam armazenados arquivos e pastas do usuário.
VII - área privativa da unidade: local de armazenamento de arquivos e pastas que são compartilhados entre os usuários da unidade.
VIII - computação em nuvem: modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), doravante denominado nuvem.

Art. 4º Para fins desta normativa, a terminologia de Segurança da Informação utilizada pode ser consultada no Glossário de Segurança da Informação.

Art. 5º Este documento passa a compor a Política de Segurança da Informação - POSIN - e alcança toda a UNILA.

Art. 6º É vedado o armazenamento e compartilhamento de informações em desacordo com as leis, políticas e normas vigentes, inclusive as relacionadas ao sigilo de informações, direitos de propriedade intelectual e industrial e informação pessoal relativa à intimidade, vida privada honra e imagem.

Art. 7º Cabe a quem produz, coleta, recepciona, distribui, transfere, modifica ou armazena a informação, assegurar que ela passe por processo de classificação e gestão de risco de segurança da informação, atendendo a legislação vigente.

Art. 8º Arquivos e documentos classificados como sigilosos ou documentos preparatórios que possam originar informação sigilosa, de acordo com a legislação vigente e normativos internos, deverão ser mantidos na infraestrutura de armazenamento de dados da própria instituição, vedado o armazenamento em nuvem.
§ 1º É responsabilidade do usuário conhecer previamente a classificação e o tratamento da informação utilizada no desempenho de suas atividades.
§ 2º Compete ao usuário do serviço, a proteção da informação sigilosa e da informação pessoal.
§ 3º Cabe ao setor de Protocolo e Arquivo, fornecer orientações aos usuários acerca do procedimento de classificação de informação no âmbito da UNILA.

Art. 9º Ficam proibidos o armazenamento de arquivos de fotos, vídeos, músicas e/ou quaisquer outros tipos de arquivos, que não estiverem relacionados à administração pública e atividades de educação, pesquisa e extensão na UNILA.

Art. 10 Esta normativa observará as seguintes diretrizes:
I - a utilização dos serviços somente em atividades relacionadas à administração pública e atividades de educação, pesquisa e extensão na UNILA;
II - o uso racional dos recursos de tecnologia da informação utilizados para prover os serviços à instituição e aos usuários;
III - confiabilidade, integridade, disponibilidade, autenticidade e não repúdio das informações armazenadas;
IV - a proibição do uso dos serviços, mesmo que por prazo determinado, por pessoas que não tenham vínculo direto ou por unidades que não façam parte do organograma da UNILA;
V - o uso preferencial dos serviços de armazenamento e compartilhamento em nuvem.
Parágrafo único. As diretrizes estabelecidas nesta normativa deverão ser observadas em caráter permanente no âmbito da UNILA.

CAPÍTULO II
DOS SERVIÇOS DE ARMAZENAMENTO EM NUVEM

Seção I
Das áreas privativas das unidades

Art. 11 Cada unidade administrativa da instituição poderá ter uma ou mais áreas privativas, as quais não serão acessíveis por outras unidades, salvo quando criadas para este fim.

Art. 12 A solicitação de criação ou exclusão de áreas privativas deverá ser realizada pela chefia da unidade requisitante, por meio da Central de Serviços.

Art. 13 É responsabilidade da chefia da unidade ou de servidor indicado e pertencente à unidade, realizar e revogar os compartilhamentos de arquivos e pastas com outros usuários ou unidades e os efeitos decorrentes deste.

Seção II
Das áreas privativas dos usuários

Art. 14 Terão direito a uma área privativa de compartilhamento e armazenamento:
I - servidores efetivos, cedidos, substitutos, temporários e ocupantes de cargos em comissão;
II - discentes devidamente matriculados.

Art. 15 O usuário é o único responsável por todo o conteúdo armazenado em sua área privativa.

Art. 16 É responsabilidade do usuário o compartilhamento de conteúdo privativo com outros usuários e os efeitos decorrentes deste.

CAPÍTULO III
DOS SERVIÇOS DE ARMAZENAMENTO INTERNO

Seção I
Da área compartilhada da unidade

Art. 17 Os serviços internos estão disponíveis somente às unidades administrativas, vedado a sua criação para usuários individuais.

Art. 18 A solicitação da criação de áreas compartilhadas deverá ser realizada pela chefia da área requisitante, por meio da Central de Serviços.

Art. 19 Compete à chefia da unidade requisitante manter atualizada a relação dos usuários e/ou grupos de usuários que poderão acessar as áreas compartilhadas da unidade.
Parágrafo único. Solicitações de informação, inclusão, alteração ou exclusão das permissões de acesso dos usuários à área compartilhada, deverão ser realizadas pelo chefe da unidade por meio da Central de Serviços.

Art. 20 Os serviços são acessíveis somente através da intranet ou VPN (Virtual Private Network).

CAPÍTULO IV
DA FISCALIZAÇÃO E DO USO DOS SERVIÇOS

Seção I
Da fiscalização do uso dos serviços

Art. 21 Poderão ser realizadas varreduras automatizadas nos serviços, com finalidade única e exclusiva de encontrar conteúdos que violem direitos autorais, normas e a legislação vigente.

Art. 22 Serão mantidos para fins de auditoria e/ou para subsidiar investigações administrativas, penais ou civis, a identificação do usuário, as operações realizadas e o endereço IP ou nome do equipamento que originou o acesso.

Art. 23 Na ocorrência de infração, o usuário terá o acesso temporariamente bloqueado, sendo notificado por e-mail para que realize os ajustes necessários.
§ 1ºO acesso será restabelecido somente após sanada a infração que deu causa ao bloqueio temporário.
§ 2ºA depender da criticidade da infração cometida pelo usuário, a equipe de TIC poderá realizar as ações necessárias para a solução imediata da infração cometida, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.

Seção II
Do término do uso dos serviços

Art. 24 A partir do encerramento do vínculo do usuário com a instituição, o acesso aos serviços será interrompido conforme os critérios e prazos estabelecidos na normativa de credencial de acesso.
Parágrafo único. É responsabilidade do usuário retirar os materiais da sua área privativa antes do término do vínculo com a instituição.

CAPÍTULO V
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 25 É responsabilidade da chefia da unidade administrativa solicitar por meio da Central de Serviços a migração do conteúdo armazenado no serviço interno para o serviço de armazenamento em nuvem, respeitado o disposto nos Art. 6º, 7º e 8º.

Art. 26 As situações não previstas nesta normativa de uso poderão ser levadas ao Comitê de Segurança da Informação - CSI, que indicará as medidas a serem tomadas.

Art. 27 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
25 de agosto de 2020

RESOLUÇÃO Nº 4/2020/CGTIC

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: