MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DA INTEGRAÇÃO LATINO-AMERICANA

COMITÊ DE GOVERNANÇA, INTEGRIDADE, RISCOS E CONTROLES INTERNOS

RESOLUÇÃO Nº 3, DE 25 DE JULHO DE 2022

Estabelece a Política de Segurança da Informação - POSIN, da Universidade Federal da Integração Latino-Americana - UNILA

O PRESIDENTE DO COMITÊ PERMANENTE DE GOVERNANÇA, INTEGRIDADE, RISCOS E CONTROLES (CGIRC), designado pela Portaria nº 376/2020/GR/UNILA, no exercício de suas atribuições, e considerando o que consta nos autos de nº 23422.020849/2021-95, resolve:

Art. 1º Instituir a Política de Segurança da Informação (POSIN) da UNILA.

CAPÍTULO I
DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para os efeitos desta resolução e de suas regulamentações, aplicam-se as seguintes definições:
I - agente público: o agente político, o servidor público e todo aquele que exerça, ainda que transitoriamente ou sem remuneração, por eleição, por nomeação, por designação, por contratação ou por qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função no Poder Executivo Federal;
II - ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
III - atividades precípuas: conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade-fim da UNILA;
IV - atividades críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;
V - ativo: qualquer coisa que tenha valor para a organização;
VI - ativos de informação: os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;
VII - (princípio da) auditabilidade: todos os eventos significativos dos processos e sistemas devem ser rastreáveis até o evento inicial, identificando, inclusive, o responsável pelo seu acontecimento;
VIII - autenticidade: propriedade que garante que uma determinada informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
IX - ciclo de vida da informação: ciclo formado pelas fases de produção, recepção, organização, uso, disseminação e destinação;
X - cifração: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro por outros ininteligíveis a pessoas não autorizadas a conhecê-los;
XI - confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;
XII - continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;
XIII - (princípio dos) controles automáticos: deverão ser utilizados, sempre que possível, controles de segurança automáticos, especialmente aqueles controles que dependem da vigilância humana e do comportamento humano;
XIV - credencial de acesso: mecanismo de segurança que identifica univocamente uma pessoa, podendo ser a combinação de nome de usuário e senha, PIN, crachá, certificado digital ou atributo biométrico, com a finalidade de proporcionar acesso físico às instalações ou aos recursos e serviços de tecnologia da informação, de acordo com seu perfil de usuário;
XV - decifração: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;
XVI - (princípio da) defesa em camadas: controles devem ser desenhados em camadas ou níveis, de tal forma que, se uma camada de controle falhar, exista um tipo diferente de controle em outra camada ou nível para prevenir a vulnerabilidade de segurança;
XVII - disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;
XVIII - gestão de segurança da informação: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade de negócios, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando à tecnologia da informação e comunicações;
XIX - incidente: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;
XX - incidente cibernético: ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de norma, política de segurança,

procedimento de segurança ou política de uso. De maneira geral, os tipos de atividade comumente reconhecidas como incidentes cibernéticos são: a) tentativas de obter acesso não-autorizado a um sistema ou a dados armazenados; b) tentativa de utilização não-autorizada de sistemas para a realização de atividades de processamento ou armazenamento de dados; c) mudanças não-autorizadas de firmware, hardware ou software em um ambiente computacional; d) ataques de negação de serviço (DoS); e e) demais ações que visem afetar a disponibilidade ou integridade dos dados. Um incidente de segurança cibernética não significa necessariamente que as informações já estão comprometidas; significa apenas que a informação está ameaçada;
XXI - incidente de segurança - qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
XXII - informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
XXIII - integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
XXIV - irretratabilidade (ou não repúdio): garantia de que o emissor se responsabilize e não possa negar a autoria da mensagem ou transação, permitindo sua identificação;
XXV - macrounidades: as unidades que compõem a Reitoria, de acordo com o Regimento Geral da Universidade.
XXVI - (princípio do) menor privilégio: pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma determinada tarefa;
XXVII - norma regulamentadora: definem procedimentos e responsabilidades em nível tático, em conformidade com as diretrizes da POSIN;
XXVIII - (princípio da) privacidade: a utilização dos ativos de informação deve ocorrer em conformidade com a preservação da intimidade, da vida privada e da honra dos seus usuários, sem prejuízo das auditorias de acesso aos sistemas que se fizerem necessárias para a condução de investigações de violações de segurança;
XXIX - procedimentos operacionais: instrumentalizam os dispositivos operacionais, permitindo a direta aplicação nas atividades da instituição, cabendo a cada macro gestor a responsabilidade de elaborá-los;
XXX - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;
XXXI - recurso: além da própria informação, é todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;
XXXII - recurso criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;
XXXIII - (princípio da) resiliência - os processos, sistemas e controles devem ser projetados para que possam resistir ou se recuperar dos efeitos de um desastre;
XXXIV - risco: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;
XXXV - (princípio da) segregação de função - funções de planejamento, execução e controle devem ser segregadas a fim de reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos de informação;
XXXVI - segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
XXXVII - (princípio da) substituição da segurança em emergências: controles de segurança devem ser desconsiderados somente de formas pré-determinadas e seguras, devendo existir procedimentos e controles alternativos previamente elencados para minimizar o nível de risco em uma emergência.
XXXVIII - unidade - faz referência a qualquer unidade organizacional, seja ela administrativa ou acadêmica;
XXXIX - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;
XXXX - usuário: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da APF, formalizada por meio da assinatura de Termo de Responsabilidade;
XXXXI - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou para uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

Art. 3º Aplica-se supletivamente o glossário de que trata o art. 19 do Decreto n. 9637, de 26 de dezembro de 2018.

CAPÍTULO II
DOS PRINCÍPIOS

Art. 4º O conjunto de documentos que compõem esta POSIN deverá guiar-se pelos seguintes princípios:
I - segregação de função;
II - menor privilégio;
III - auditabilidade;
IV - controles automáticos;
V - resiliência;
VI - defesa em camadas;
VII - privacidade; e
VIII - substituição da segurança em emergências.

CAPÍTULO III
DO ESCOPO

Art. 5º São objetivos da POSIN da UNILA:
I - garantir a integridade, autenticidade, confidencialidade, disponibilidade e irretratabilidade das informações pertencentes a UNILA ou sob sua responsabilidade;
II - instituir diretrizes estratégicas, responsabilidades e competências visando à estruturação da segurança da informação;
III - promover ações necessárias à implementação e à manutenção da segurança da informação;
IV - coibir atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação e a imagem da instituição;
V - promover a conscientização e a capacitação de recursos humanos em segurança da informação.

Art. 6º A presente política aplica-se a todas as pessoas que utilizam ativos de informação no âmbito da UNILA.

CAPÍTULO IV
DAS DIRETRIZES GERAIS

Art. 7º A estrutura normativa decorrente desta Política de Segurança da Informação deverá ser estabelecida de acordo com o seguinte nível hierárquico:

I - normas regulamentadoras; e
II - procedimentos operacionais.

Seção I
Da Gestão de Ativos

Art. 8º Medidas de segurança deverão garantir a proteção lógica e física dos ativos de informação da UNILA em níveis compatíveis ao seu grau de relevância para a consecução das atividades e objetivos estratégicos.

Art. 9º Os ativos de informação, de acordo com sua criticidade, devem ser identificados, inventariados, mantidos atualizados, possuírem um responsável e serem protegidos contra acessos indevidos.
Parágrafo único. Ativos de informação não inventariados, não gerenciados, ou de uso particular, não poderão acessar a rede administrativa da instituição, exceto em condições excepcionais tratadas em norma complementar específica.

Art. 10. Apenas software homologado poderá ser instalado e utilizado nas estações de trabalho e em servidores de rede institucionais.

Art. 11. A informação armazenada em estações de trabalho, dispositivos móveis ou mídias externas é de responsabilidade do usuário, cabendo ao mesmo adotar as medidas necessárias para evitar a perda de dados.

Seção II
Do Controle de Acesso, Segurança Física e do Ambiente

Art. 12. O acesso às redes de dados institucionais e aos ativos de informação será normatizado em instrumento específico.

Art. 13. A credencial de acesso aos ativos de informação da UNILA é de uso exclusivo para fins profissionais e acadêmicos.
§ 1º A credencial de acesso de que trata o caput é pessoal e intransferível, devendo o seu portador adotar medidas para sua proteção e preservação do sigilo.
§ 2º A concessão de credencial de acesso será condicionada ao aceite dos termos e condições contidas nesta política e em normas complementares de segurança da informação.
§ 3º A gestão de credenciais de acesso deverá ser feita preferencialmente de forma centralizada e, quando possível, automatizada.
§ 4º Os procedimentos de concessão de acesso aos ativos de informação deverão observar:
I - o critério do menor privilégio necessário;
II - a segregação de funções;
III - a identificação individual e inequívoca do portador da credencial;
IV - o uso de credencial secundária para atividades de privilégio elevado;
V - a concessão mediante processo formal e regulamentado.

Art. 14 Devem ser adotados procedimentos para que nenhuma informação sensível seja deixada à vista, como forma de minimizar os riscos de acesso não autorizado, perda ou corrompimento de informações, durante e fora do horário de expediente.

Art. 15 Os acessos às informações devem ser controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente e cancelados ao término do vínculo, mudança de atribuição ou responsabilidade.

Art. 16 As normas aplicáveis à segurança física e do ambiente deverão contemplar procedimentos de acesso físico a áreas e instalações, gestão de acessos e delimitação de perímetros de segurança.
Parágrafo único. O planejamento da segurança de equipamentos e instalações de processamento de informações críticas ou sensíveis, deverá prever a proteção contra ameaças físicas e ambientais.

Seção III
Da Gestão de Riscos e da Continuidade de Negócios

Art. 17. Deverão ser estabelecidos processos e procedimentos de gestão de riscos de ativos de informação, visando à identificação, avaliação e posterior tratamento e monitoramento dos riscos considerados críticos para a segurança da informação.
Parágrafo único. O conjunto de processos e procedimentos de gestão de riscos de ativos de informação serão organizados em documento específico e publicados no site da UNILA.

Art. 18. A gestão de continuidade de negócio deve ser implementada de modo a garantir o fluxo das informações críticas em momento de crise e salvaguardar as informações, o interesse das partes interessadas, a reputação e a imagem da UNILA.

Art. 19. Ativos de informação considerados críticos, devem possuir cópias de segurança suficientes para restaurar o funcionamento dos sistemas em caso de uma perda de dados ou interrupção de serviço.

Seção IV
Da Gestão de Incidentes de Segurança da Informação

Art. 20. A UNILA manterá permanentemente uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR.
§ 1º A ETIR tem como missão atuar na prevenção, tratamento e resposta a incidentes cibernéticos ocorridos nas redes de dados da UNILA.
§ 2º Sem prejuízo às demais atribuições, a ETIR deverá estabelecer e dar publicidade a processos e procedimentos de gerenciamento e tratamento adequado de incidentes cibernéticos.

Seção V
Da Auditoria e Conformidade

Art. 21. Deverá ser mantido o registro de logs e trilhas de auditoria no ambiente computacional, protegidos de acessos e alterações não autorizados, que permitam identificar os acessos e modificações nos ativos de informação.

Art. 22. O setor de tecnologia da informação, com a finalidade de assegurar o funcionamento dos serviços e a segurança do ambiente computacional,

poderá auditar e inspecionar os recursos de TIC que interagem com seus ambientes lógicos, físicos ou com suas informações.

Art. 23. A ETIR poderá monitorar, auditar, coletar evidências e realizar análise do uso dos serviços e recursos de TIC, para fins de apuração de transgressão disciplinar ou violação desta política, atendendo a ordem judicial ou solicitação policial.
Parágrafo único. O disposto no caput também se aplica para o atendimento à solicitações de disponibilização de informações encaminhadas por unidades administrativas internas responsáveis pela análise preliminar ou pela apuração de denúncias.

Art. 24. A ETIR deverá adotar boas práticas para preservação da cadeia de custódia dos dados coletados.

Art. 25. Devem ser adotados mecanismos de gestão de mudança de forma que alterações significativas no ambiente computacional da UNILA sejam documentadas e possam identificar o requisitante e a necessidade que deu causa a ela.

Seção VI
Gestão do Uso dos Recursos de Comunicações

Art. 26. O acesso à Internet no âmbito da UNILA é fornecido para fins diretos e complementares às atividades da instituição, sendo, portanto, passível de registro e auditoria nos termos da lei.

Art. 27. Perfis em mídias sociais, sites ou portais externos, pertencentes a alguma das unidades organizacionais da instituição, devem ser criados, atualizados e descontinuados de acordo com normas complementares específicas.

Art. 28. O serviço de internet, correio eletrônico institucional, bem como listas de transmissão de correio eletrônico, mensagens instantâneas, telefonia e demais serviços de comunicação, são destinados para atividades acadêmicas e administrativas e seus termos de uso serão regulamentados por normas complementares.

Seção VII
Do Desenvolvimento de Sistemas Seguros

Art. 29. Os processos e procedimentos de desenvolvimento de software contemplarão controles específicos para a garantia da segurança dos sistemas utilizados, a preservação do ambiente tecnológico e a prevenção de incidentes cibernéticos, devendo observar:
I - as orientações do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) e boas práticas de mercado, para desenvolvimento de software seguro, apropriadas para a linguagem de programação e o ambiente de desenvolvimento utilizado na UNILA;
II - a busca permanente por capacitação e desenvolvimento dos servidores envolvidos em desenvolvimento e manutenção dos sistemas institucionais;
III - a separação de ambientes para sistemas de produção e de não produção;
IV - a segregação de funções em todo ciclo de vida do processo de desenvolvimento, implantação e manutenção de software;
V - a manutenção do código-fonte dos sistemas em repositório gerenciado de modo a preservar o histórico das modificações realizadas.

Seção VIII
Do Uso de Recursos Criptográficos

Art. 30. A informação classificada ou restrita, produzida, armazenada ou transmitida pela instituição, em parte ou totalmente, por qualquer meio eletrônico, deverá ser protegida com recurso criptográfico.
§1. A proteção criptográfica poderá ser dispensada em razão de justificativa técnica, ou do custodiante da informação, considerados os riscos envolvidos.
§2. A informação de que trata o caput, se armazenada em dispositivos de mídia removível, deve estar obrigatoriamente protegida por criptografia.

Seção IX
Do Processo de Tratamento da Informação

Art. 31. O(A) agente público(a) responsável pela produção ou pelo recebimento da informação deverá prover sua classificação, sob os critérios legalmente estabelecidos de confidencialidade, disponibilidade e integridade.

Art. 32. As informações produzidas por usuários, no exercício de suas funções, são patrimônio da UNILA, protegidas pelos direitos de propriedade intelectual, de acordo com a lei.

Art. 33. A utilização de conteúdos de terceiros, em qualquer tipo de produção on-line pertencente à UNILA, deverá conter a respectiva indicação de autoria e respeitar a legislação de propriedade intelectual vigente.

Art. 34. É vedado o uso de aplicações e repositórios não homologados para processar, armazenar ou publicar informações de propriedade da UNILA ou sob sua responsabilidade, salvo casos de informação sem restrição de acesso e que tenham sido adotadas medidas de preservação contra perda de dados e aprisionamento tecnológico.

Art. 35. No processo de tratamento da informação, deve ser garantida a privacidade, a disponibilidade, a integridade e a confidencialidade dos dados pessoais em todo o seu ciclo de vida, em qualquer formato de armazenamento e suporte.

Art. 36. Deverão ser estabelecidos controles e normas relacionados à confidencialidade, disponibilidade e integridade no armazenamento e compartilhamento de arquivos em serviços disponibilizados na rede da instituição ou em nuvem.

Seção X
Da Segurança em Recursos Humanos

Art. 37. Os agentes públicos e discentes deverão ser continuamente capacitados para o desenvolvimento de competências em Segurança da Informação.

Art. 38. Compete a cada unidade, divulgar aos agentes públicos ou discentes a ela vinculados, suas atribuições e responsabilidades em relação à Segurança da Informação.

CAPÍTULO V

DAS VIOLAÇÕES, SANÇÕES E PENALIDADES

Art. 39. A violação ao disposto na POSIN, ou em qualquer de suas normas complementares, assim como comprometer a integridade dos controles de segurança da informação, sujeita à responsabilização disciplinar, penal e civil, nos termos da lei.

CAPÍTULO VI
DA ESTRUTURA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 40. Compõem a estrutura de Segurança da Informação da UNILA:
I - Comitê Permanente de Governança Integridade, Riscos e Controles (CGIRC);
II - Comitê de Governança Digital - CGD;
III - Gestor de Segurança da Informação; e
IV - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR.

CAPÍTULO VII
DAS COMPETÊNCIAS, DEVERES E RESPONSABILIDADES

Art. 41. Compete às macrounidades, dentro de suas responsabilidades:
I - elaborar e submeter ao CGD, normas de segurança da informação, que visem regulamentar procedimentos vinculados às suas atividades e competências;
II - estabelecer e publicar os procedimentos de segurança da informação, necessários à execução dos processos e subprocessos sob sua gestão, alinhados às diretrizes aqui estabelecidas.

Art. 42. Compete à Pró-reitoria de Gestão de Pessoas:
I - viabilizar as capacitações sobre segurança da informação e proteção de dados presentes no Plano de Desenvolvimento de Pessoas.

Art. 43. Compete à Secretaria de Comunicação Social:
I - Adotar medidas de conscientização junto à comunidade acadêmica da UNILA, para que seja fortalecida a cultura de segurança da informação na instituição.

Art. 44. Compete aos titulares das unidades organizacionais da UNILA:
I - fazer cumprir as diretrizes, normas e procedimentos de segurança da informação na unidade sob sua responsabilidade;
II - incorporar aos processos de trabalho da unidade, práticas inerentes à segurança da informação;
III - promover a divulgação dessa política, e demais normas e procedimentos de segurança da informação, aos servidores, estagiários e terceirizados que atuam em sua unidade;
IV - tomar as medidas administrativas necessárias para que sejam apurados os casos de descumprimento desta política por parte dos usuários sob sua supervisão.

Art. 45. São deveres, dos destinatários dessa política, relacionados no art. 6º, como corresponsáveis pela segurança da informação:
I - ter pleno conhecimento desta política e zelar por seu cumprimento;
II - responder por toda atividade executada com o uso de sua credencial de acesso;
III - reportar tempestivamente a ETIR quaisquer falhas ou indícios de falhas de segurança cibernética de que tenha conhecimento ou suspeita;
IV - colaborar, em suas áreas de competência, na identificação e no tratamento de incidentes de segurança da informação;
V - proteger as informações restritas ou sigilosas obtidas em decorrência do exercício de suas atividades;
VI - utilizar os ativos sob sua responsabilidade de forma segura, em observância ao disposto nesta política e em eventuais normativos a ela subordinados.

Art. 46. As competências, deveres e responsabilidades relacionadas à estrutura de Gestão de Segurança da Informação serão tratados em documento próprio.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Art. 47. Os casos omissos desta POSIN serão resolvidos pelo CGD.

Art. 48. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pela UNILA devem observar, no que couber, o constante desta POSIN.

Art. 49. Os instrumentos normativos de segurança da informação deverão ser revisados no período máximo de 4 (quatro) anos de sua publicação.

GLEISSON ALISSON PEREIRA DE BRITO

Resolução nº 3/2022/CGirc, com publicação no Boletim de Serviço nº 133, de 25 de Julho de 2022.