MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DA INTEGRAÇÃO LATINO-AMERICANA

COMITÊ DE GOVERNANÇA, INTEGRIDADE, RISCOS E CONTROLES INTERNOS

RESOLUÇÃO Nº 3, DE 03 DE JULHO DE 2026

Aprova a atualização da Política de Segurança da Informação e Comunicação (POSIN) da Universidade Federal da Integração Latino-Americana – UNILA.

A PRESIDENTE DO COMITÊ DE GOVERNANÇA, INTEGRIDADE, RISCOS E CONTROLES INTERNOS (CGIRC), no uso das competências e atribuições conferidas pela Portaria nº 186/2026/Gabinete, pelo Regimento Interno do Comitê de Governança, Integridade, Riscos e Controles Internos da Universidade Federal da Integração Latino-Americana (UNILA) e considerando o disposto na Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016; no Decreto nº 9.203, de 22 de novembro de 2017 (Política de Governança da Administração Pública Federal); no Decreto nº 11.529, de 16 de maio de 2023, que institui o Sistema de Integridade, Transparência e Acesso à Informação (Sitai); na Portaria Normativa CGU nº 234, de 6 de novembro de 2025; na Instrução Normativa GSI/PR nº 9, de 8 de janeiro de 2026, que dispõe sobre a Estrutura de Gestão da Segurança da Informação no âmbito da Administração Pública Federal e o que consta no processo nº 23422.020849/2021-77, RESOLVE:

Art. 1º. Aprovar a atualização da Política de Segurança da Informação e Comunicação (POSIN) da Universidade Federal da Integração Latino-Americana – UNILA.

Art. 2º. A POSIN passa a constituir instrumento de governança institucional, estabelecendo princípios, diretrizes, responsabilidades e controles para a proteção dos ativos de informação, em consonância com a legislação vigente, as normas federais aplicáveis e as boas práticas de segurança da informação.

Art. 3º. A implementação da POSIN observará o princípio da gradualidade, devendo ser realizada de forma progressiva, respeitando a realidade institucional e os processos vigentes, sob coordenação das instâncias de gestão competentes.

Art. 4º. Ficam revogadas as disposições em contrário, em especial a Resolução nº 3/2022/CGIRC.

Art. 5º. Esta Resolução entra em vigor na data de sua publicação.

DIANA ARAUJO PEREIRA

Resolução nº 3/2026/CGirc, com publicação no Boletim de Serviço nº 114, de 03 de Julho de 2026.

Política de Segurança da Informação

UNILA

Versão 2.0
Foz do Iguaçu, novembro de 2025

Comitê Permanente de Governança, Integridade, Riscos e Controle (CGIRC)

REITORA
Diana Araujo Pereira

PRÓ-REITOR DE ADMINISTRAÇÃO, GESTÃO E INFRAESTRUTURA
Diogo Andre Bastian

PRÓ-REITORA DE ASSUNTOS ESTUDANTIS
Maria Geusina da Silva

PRÓ-REITORA DE EXTENSÃO
Andreia da Silva Moassab

PRÓ-REITOR DE GESTÃO DE PESSOAS
Felipe Cordeiro

PRÓ-REITORA DE GRADUAÇÃO
Antonio Machado Felisberto Junior

PRÓ-REITORA DE PESQUISA E PÓS-GRADUAÇÃO
Laura Fortes

PRÓ-REITOR DE PLANEJAMENTO, ORÇAMENTO E FINANÇAS
Giuliano Silveira Derrosso

PRÓ-REITOR DE RELAÇÕES INSTITUCIONAIS E INTERNACIONAIS
Suellen Mayara Peres de Oliveira

SECRETÁRIA DE APOIO CIENTÍFICO E TECNOLÓGICO
Ricardo Morel Hartmann

SECRETÁRIA DE COMUNICAÇÃO SOCIAL
Michele Dacas

PREFEITO UNIVERSITÁRIO
Iván Dario Gómes Araújo

DIRETOR DO INSTITUTO LATINO-AMERICANO DE CIÊNCIAS, ARTE, CULTURA E HISTÓRIA
Márcia Cossetin

DIRETOR DO INSTITUTO LATINO-AMERICANO DE CIÊNCIAS DA VIDA E DA NATUREZA
Márcio de Sousa Góes

DIRETOR DO INSTITUTO LATINO-AMERICANO DE ECONOMIA, SOCIEDADE E POLÍTICA
Fábio Borges

DIRETOR DO INSTITUTO LATINO-AMERICANO DE TECNOLOGIA, INFRAESTRUTURA E TERRITÓRIO
Juliana Ramme

Equipe Técnica de Elaboração

Wilson Varaschin
Ruminiki Pavei Schmoeller
Carlos Alberto Meier Basso
Márcio Fernandes da Costa

Equipe Técnica de Revisão

Wilson Varaschin
Márcio Fernandes da Costa

Colaboração

Diego Soares Alves
Geraldino Alves Bartozek

Controle de versões			
Versão	**Data**	**Autor(es)**	**Descrição**
1.0	25/07/2022	Equipe Técnica de Elaboração	Elaboração da política
2.0		Equipe Técnica de Revisão	As principais alterações incluem: • Estruturação conforme modelo recomendado pela ISO/IEC 27003:2020; • Expansão do escopo para ambientes físicos, digitais, remotos e em nuvem; • Definição clara de ativos de informação e critérios de classificação; • Inclusão de princípios como rastreabilidade, defesa em profundidade e responsabilização individual; • Criação de fluxos operacionais para tratamento de incidentes (Anexo III); • Reforço na integração com a governança de TIC e gestão de riscos; • Atualização dos termos de responsabilidade (Anexos I e II); • Estabelecimento de indicadores de desempenho e conformidade (ISO/IEC 27004); • Reestruturação da governança de segurança da informação, com atribuições detalhadas para CGD, CGIRC, DPO, ETIR e demais agentes.

Sumário

Aviso Preliminar

Esta versão da Política de Segurança da Informação e Comunicação (POSIN) substitui integralmente a Resolução CGIRC nº 3/2022, publicada em 25 de julho de 2022. A revisão foi conduzida pelo Comitê de Governança Digital (CGD) e aprovada pelo Comitê Permanente de Governança, Integridade, Riscos e Controle (CGIRC), incorporando avanços técnicos, normativos e organizacionais necessários à maturidade da gestão da segurança da informação na UNILA.

A nova versão foi estruturada conforme os princípios da norma ISO/IEC 27003:2020, com foco na clareza, rastreabilidade e alinhamento estratégico. Foram incorporadas referências às normas ISO/IEC 27001:2024, 27002:2022, 27701:2019, 27014:2021, 31000:2018 e 22301:2024, bem como às legislações vigentes, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD), a Lei de Acesso à Informação (LAI) e o Marco Civil da Internet.

Entre as principais melhorias estão:

- Expansão do escopo para ambientes físicos, digitais, remotos e em nuvem;
- Definição clara de ativos de informação e critérios de classificação;
- Inclusão de princípios como rastreabilidade, defesa em profundidade e responsabilização individual;
- Criação de fluxos operacionais para tratamento de incidentes (Anexo III);
- Reforço na integração com a governança de TIC e gestão de riscos;
- Atualização dos termos de responsabilidade (Anexos I e II);
- Estabelecimento de indicadores de desempenho e conformidade (ISO/IEC 27004);
- Reestruturação da governança de segurança da informação, com atribuições detalhadas para CGD, CGIRC, DPO, ETIR e demais agentes.

Introdução

A crescente digitalização dos processos acadêmicos, administrativos e científicos da Universidade Federal da Integração Latino-Americana (UNILA) impõe desafios cada vez mais complexos à proteção dos ativos de informação institucionais. Em um cenário marcado por riscos cibernéticos, exigências legais rigorosas e dependência tecnológica crescente, torna-se essencial estabelecer uma política clara, robusta e alinhada às melhores práticas internacionais de segurança da informação.

A Política de Segurança da Informação e Comunicação (POSIN) foi elaborada com base nas diretrizes da ISO/IEC 27001, ISO/IEC 27701, ISO 31000 e demais normas correlatas, bem como nas legislações brasileiras aplicáveis, como a Lei Geral de Proteção de Dados Pessoais (LGPD) e a Lei de Acesso à Informação (LAI). Seu propósito é garantir a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações sob responsabilidade da UNILA, promovendo uma cultura organizacional de segurança, responsabilidade e conformidade.

Propósito

Esta política tem como propósito estabelecer os princípios, diretrizes, responsabilidades e controles necessários para assegurar a proteção dos ativos de informação da UNILA, em todas as suas formas e suportes, contra ameaças internas e externas, acidentais ou deliberadas. A POSIN visa garantir que os dados institucionais sejam tratados com segurança, ética e em conformidade com os requisitos legais, contratuais e normativos aplicáveis, contribuindo para a continuidade dos serviços, a confiança da comunidade acadêmica e a integridade da missão institucional.

Escopo

A POSIN aplica-se a todas as unidades organizacionais, ambientes físicos e digitais, sistemas, redes, serviços em nuvem, processos e pessoas que, sob qualquer vínculo, utilizem ou acessem ativos de informação da UNILA. Isso inclui servidores públicos, empregados, estudantes, pesquisadores, colaboradores, parceiros, prestadores de serviço e visitantes.

Além disso, esta política se integra e complementa outros instrumentos institucionais, como o Plano de Desenvolvimento Institucional (PDI), o Plano Diretor de TIC (PDTIC), o Plano Estratégico de TIC (PETIC), a Política de Gestão de Riscos e o Programa de Integridade da UNILA.

Declarações da política

Capítulo I – Disposições Gerais

Art. 1º Fica instituída a Política de Segurança da Informação da Universidade Federal da Integração Latino-Americana - UNILA, com a finalidade de estabelecer princípios, diretrizes, responsabilidades e competências para a gestão da segurança da informação.

Art. 2º Esta Política aplica-se a todas as unidades organizacionais, instalações físicas e ambientes virtuais sob gestão da UNILA, incluindo infraestruturas de nuvem, redes privadas e sistemas remotos, abrangendo os ativos de informação definidos no Art. 6º.

Art. 3º Estão sujeitos a esta Política todos os agentes que, sob qualquer vínculo, utilizem ou acessem ativos de informação da UNILA, incluindo:

I - estudantes, pesquisadores e bolsistas;
II - colaboradores, parceiros e prestadores de serviços;
III - servidores públicos, empregados públicos e pessoal equiparado;
IV - visitantes e demais pessoas em dependências da UNILA.

Art. 4º O acesso a ativos de informação institucionais está condicionado à assinatura prévia de Termo de Responsabilidade, conforme modelo constante no Anexo I ou Anexo II, conforme o perfil de acesso e vínculo do usuário desta Política, que formaliza o compromisso com a proteção de dados pessoais, nos termos do art. 46 da Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Parágrafo único. Os contratos firmados com terceiros deverão conter cláusulas específicas de conformidade com esta Política, conforme regulamentação complementar.

Art. 5º São objetivos da Política de Segurança da Informação:

I - adotar decisões baseadas em riscos, alinhadas ao apetite institucional e à Política de Gestão de Riscos da UNILA;
II - assegurar conformidade com requisitos legais, normativos, contratuais e internos;
III - estimular a cultura organizacional de segurança por meio de ações de capacitação e conscientização;
IV - integrar requisitos de segurança aos processos de aquisição, contratação, desenvolvimento de sistemas, parcerias e projetos;
V - monitorar e aprimorar continuamente os controles de segurança, com base em indicadores, auditorias e revisões periódicas; e
VI - promover uma abordagem integrada e abrangente de segurança da informação, considerando aspectos físicos, digitais e organizacionais.

Art. 6º Constituem Ativos de Informação da UNILA os recursos essenciais ao cumprimento de suas finalidades institucionais, classificados como:

I - **informações:** dados em qualquer meio físico ou digital, incluindo:
II - **categorias**: pessoais, sensíveis, acadêmicos, científicos, administrativos, estratégicos e de propriedade intelectual;
III - **digitais:** bancos de dados, arquivos eletrônicos, e-mails, mídias digitais;

IV - **físicos:** documentos em papel, fichários, microfilmes, plantas, registros manuscritos, mídias magnéticas ou ópticas;
V - infraestrutura:
VI - **física:** salas de arquivo, cofres, sistemas de arquivamento, salas de servidores e data centers;
VII - **lógica:** sistemas, redes, dispositivos de armazenamento;
VIII - **pessoas:** indivíduos com acesso autorizado às informações;
IX - **processos institucionais:** atividades e fluxos que geram, modificam ou utilizam informações; e
X - serviços externos:
XI - digital: serviços em nuvem.
XII - físico: empresas de gestão documental, digitalização, descarte seguro.

Art. 7º Todos os ativos de informação definidos no art. 6º, independentemente de suporte, formato ou localização, estão sob responsabilidade da UNILA e sujeitos às normas desta Política e às regulamentações complementares.

Art. 8º A classificação de valor dos ativos de informação definidos no Art. 4º considerará os seguintes critérios:

I - impacto à missão institucional, avaliando consequências operacionais, financeiras, legais e reputacionais em caso de comprometimento;
II - criticidade do ativo para processos essenciais da Universidade, com base em:

a) custo de reposição ou reconstituição;
b) sensibilidade frente a acesso não autorizado; e
c) tempo máximo tolerável de indisponibilidade (RTO - *Recovery Time Objective*);

III - requisitos de confidencialidade, integridade e disponibilidade derivados de:

a) contratos com partes interessadas;
b) obrigações legais e regulatórias; e
c) políticas internas da UNILA.

Art. 9º A gestão de acessos e responsabilidades observará regras de segregação funcional, especialmente em:

I - designação de responsabilidades que assegurem independência nas atividades de controle, com:

a) atribuições claras na estrutura organizacional; e
b) mecanismos de prestação de contas à alta administração.

II - funções críticas de segurança da informação, vedando a acumulação de atividades incompatíveis, tais como:

a) concepção, operação e auditoria de sistemas;
b) concessão, utilização e fiscalização de acessos; e
c) contratação, supervisão e auditoria de serviços externos.

Art. 10. Para os efeitos desta Política e de suas regulamentações, aplicam-se os termos:

I - **Apetite ao risco:** nível de risco que uma organização está disposta a aceitar;

II - **Autenticidade:** propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

III - **Avaliação de riscos:** processo global de identificação de riscos, análise de riscos e avaliação de riscos;

IV - **Critérios de risco:** termos de referência diante dos quais a significância de um risco é avaliada;

V - **Confidencialidade:** propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

VI - **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;

VII - **Governança de Segurança da Informação**: conjunto de mecanismos adotados pela Alta Administração, CGIRC e CGD para orientar, supervisionar e garantir a efetividade das ações de segurança da informação, por meio de:

a) direcionamento estratégico alinhado aos objetivos institucionais;
b) implementação de controles técnicos e processuais;
c) monitoramento contínuo, prestação de contas e auditorias independentes; e
d) vinculação legal dos agentes por meio do Termo de Responsabilidade

VIII - **Incidente de Segurança da Informação: e**vento confirmado ou suspeito que compromete a confidencialidade, integridade ou disponibilidade de ativos de informação;

IX - **Indicador de Conformidade:** métrica que avalia o grau de aderência a normas, políticas e requisitos legais;

X - **Indicadores de desempenho:** métricas utilizadas para avaliar a eficácia dos controles de segurança, conforme ISO/IEC 27004.

XI - **Integridade:** propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XII - **Menor Privilégio:** princípio que determina que cada usuário deve ter apenas os acessos estritamente necessários para desempenhar suas funções;

XIII - **Não-repúdio:** garantia de que a informação é genuína e que sua origem pode ser verificada;

XIV - **Plano de Continuidade de Negócios:** informação documentada que orienta a organização a responder a uma disrupção e retomar, recuperar e restaurar a entrega de produtos e serviços de acordo com os objetivos de continuidade de negócios;

XV - **Risco:** Efeito da incerteza (estado, mesmo parcial, de deficiência de informação relacionada à compreensão ou conhecimento) nos objetivos (resultado a ser alcançado);

XVI - **Segregação de Funções:** princípio que determina a distribuição das responsabilidades entre diferentes pessoas ou áreas para evitar conflitos de interesse e reduzir riscos operacionais;

XVII - **SGSI (Sistema de Gestão de Segurança da Informação)** - Estrutura para gerenciar políticas, processos e controles de segurança, alinhada à ISO/IEC 27001;

XVIII - **SLAs/OLAs:** Acordos de Nível de Serviço (SLA) e Acordos Operacionais Internos (OLA) que definem prazos, responsabilidades e padrões de desempenho;

XIX - **Termo de Responsabilidade -** Documento obrigatório para acesso a ativos institucionais, formalizando deveres de proteção e conformidade com a LGPD, conforme modelo constante no Anexo I desta Política;

XX - **Usuário de Informação -** Pessoa física habilitada pela administração para acessar ativos de informação da UNILA, incluindo servidores, empregados, prestadores de serviços, discentes e pesquisadores vinculados a projetos institucionais; e

XXI - **Vulnerabilidade:** condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha.

Parágrafo único. Os termos definidos nesta Política complementam o Glossário de Segurança da Informação aprovado pela Portaria GSI/PR nº 93/2021, devendo ser utilizados para interpretação e aplicação da POSIN.

Capítulo II – Princípios e Diretrizes

Seção I – Dos Princípios

Art. 11. As ações de segurança da informação da UNILA seguem os seguintes princípios:

I - **alinhamento estratégico** da segurança da informação aos objetivos institucionais;

II - **aplicação do princípio do menor privilégio** e segregação de funções para evitar conflitos de interesse;

III - capacidade de resposta rápida a incidentes, com foco na resiliência organizacional;

IV - conformidade com normas legais, regulatórias e contratuais aplicáveis;

V - continuidade dos serviços essenciais, com planos testados regularmente;

VI - **defesa em profundidade**, com múltiplas camadas de proteção;

VII - **equilíbrio entre transparência e privacidade**, conforme a Lei nº 12.527/2011 (Lei de Acesso à Informação) e a Lei nº 13.709/2018 (LGPD);

VIII - **melhoria contínua dos controles**, com base em métricas, lições aprendidas e evolução das ameaças;

IX - **promoção da cultura de segurança**. por meio de capacitação contínua e comunicação clara;

X - **proteção da informação** quanto à disponibilidade, integridade, confidencialidade, autenticidade, não-repúdio e confiabilidade;

XI - proteção reforçada de dados pessoais e sensíveis, conforme LGPD e ISO/IEC 27701;

XII - **rastreabilidade de acessos e ações** por meio de registros auditáveis;

XIII - **responsabilização individual** por condutas que comprometam a segurança da informação; e

XIV - uso proporcional de recursos de segurança, conforme a criticidade dos ativos.

Seção II – Dos Referenciais Técnicos e Diretrizes

Art. 12. As normas, procedimentos e metodologias de segurança da informação da UNILA deverão observar os princípios e diretrizes estabelecidos nesta Política, bem como os seguintes referenciais técnicos:

I - adotar como referência obrigatória os seguintes padrões:

a) ISO/IEC 27001 e ISO/IEC 27002, que tratam do Sistema de Gestão da Segurança da Informação (SGSI);
b) ISO/IEC 27701, sobre Gestão da privacidade e proteção de dados pessoais;
c) ISO/IEC 27005, ISO 31000 e ISO 31010, referentes à Gestão e avaliação de riscos;
d) ISO 22301, relativa à Continuidade de negócios;
e) ISO/IEC 27014, ISO/IEC 38500, sobre Governança de segurança da informação e de TIC;
f) ISO/IEC 27004, que estabelece Indicadores e métricas de desempenho;
g) CIS Critical Security Controls, para Defesa cibernética; e
h) as Diretrizes do GSI/PR e da ANPD.

II - diretrizes operacionais específicas estão detalhadas nos artigos seguintes desta Política, incluindo:

a) gestão de riscos e ativos: arts. 13 a 15;
b) controle de acesso e responsabilização: arts. 16 a 20;
c) monitoramento e auditoria: arts. 22 a 28;
d) capacitação e comunicação: arts. 31 e 32;
e) contratos com terceiros: art. 35; e
f) art. 51 e Anexo III: tratamento de incidentes (Fluxo de Gestão de Incidentes de Segurança da Informação).

Capítulo III – Gestão de Riscos e Ativos

Art. 13. Toda alteração em ativos de informação deverá ser precedida de processo formal de avaliação de riscos e impactos, com aprovação do Gestor de Segurança da Informação, observando:

I - a criticidade do ativo para os serviços institucionais;
II - os controles de segurança existentes e os ajustes necessários; e
III - os requisitos legais e contratuais aplicáveis.

Art. 14. O investimento em medidas de segurança da informação será dimensionado com base nos seguintes critérios:

I - avaliação de custo-benefício dos controles propostos, priorizando soluções eficazes e alinhadas às diretrizes desta Política;
II - criticidade operacional dos serviços impactados, considerando os planos de continuidade e recuperação de desastres;
III - exigências legais, regulatórias e contratuais;
IV - indicadores de desempenho e conformidade definidos no Sistema de Gestão de Segurança da Informação – SGSI; e
V - resultados da análise de riscos e da classificação dos ativos, conforme os arts. 6º a 8º.

Art. 15. A Gestão da Segurança da Informação da UNILA é composta, no mínimo, pelos seguintes processos institucionais:

I - auditoria e conformidade;
II - controles de acesso;
III - gestão da continuidade de serviços e recuperação de desastres;
IV - gestão de ativos de informação;
V - gestão de incidentes de segurança da informação;
VI - gestão do uso dos recursos operacionais e de comunicações;

VII - gestão de riscos;
VIII - segurança física e do ambiente; e
IX - tratamento da informação: classificação, rotulagem, armazenamento, descarte e compartilhamento, conforme diretrizes da POSIN e da Lei Geral de Proteção de Dados – LGPD.

§ 1º O CGD poderá definir outros processos complementares, desde que alinhados aos princípios e diretrizes desta Política e destinados à implementação de ações de segurança da informação.
§ 2º Para cada processo, deverá ser avaliada a pertinência de elaboração de políticas, normas, procedimentos, orientações ou manuais específicos, em conformidade com a legislação vigente e com as boas práticas de segurança da informação

Capítulo IV – Controle de Acesso e Responsabilização

Art. 16. O acesso a ativos de informação será limitado ao mínimo necessário para o desempenho das funções específicas, aplicando-se os princípios do menor privilégio e da necessidade de conhecer.

Parágrafo único. O acesso estará condicionado à assinatura de Termo de Responsabilidade, preferencialmente eletrônico, conforme modelo constante no Anexo I ou Anexo II, conforme o perfil de acesso e vínculo do usuário que formalize:

I - a ciência desta Política e dos regulamentos complementares;
II - as consequências administrativas em caso de descumprimento; e
III - o compromisso com a proteção de dados pessoais.

Art. 17. Os Usuários de Informação são responsáveis por:

I - comunicar imediatamente ao Gestor de Segurança da Informação ou à Equipe de Tratamento de Incidentes Cibernéticos (ETIR) qualquer incidente, violação ou suspeita de comprometimento de ativos;
II - cumprir integralmente as diretrizes, normas e procedimentos definidos na POSIN e em seus regulamentos complementares;
III - participar dos programas de capacitação e conscientização em segurança da informação promovidos pela UNILA; e
IV - proteger os ativos de informação sob sua guarda ou acesso, observando os princípios da confidencialidade, integridade, disponibilidade e legalidade.

Art. 18. O acesso a ativos de informação institucionais está condicionado à assinatura de Termo de Responsabilidade, conforme modelo constante no Anexo I ou Anexo II, conforme o perfil de acesso e vínculo do usuário, que formaliza:

I - a ciência da POSIN e das normas complementares;
II - as consequências administrativas em caso de descumprimento; e
III - o compromisso com a proteção de dados pessoais;

Art. 19. Os Usuários de Informação serão responsabilizados por ações que comprometam a segurança dos ativos institucionais, conforme previsto nesta Política e na legislação vigente.

§ 1º A responsabilização será proporcional à gravidade da infração e ao impacto causado.
§ 2º Casos de violação serão tratados conforme os procedimentos definidos pelo Gestor de Segurança da Informação e pelas instâncias disciplinares competentes.

Art. 20. É vedada a utilização dos recursos de tecnologia da informação disponibilizados pela UNILA para:

I - acesso, guarda ou divulgação de material incompatível com o ambiente do serviço;
II - práticas que infrinjam a legislação vigente.
III - violação de direitos autorais;

Art. 21. São vedadas as seguintes condutas:

I - compartilhamento com terceiros de credenciais de acesso (usuário, senha, certificado digital), de uso pessoal e intransferível, mesmo que temporariamente;
II - exploração de vulnerabilidades nos sistemas institucionais, as quais devem ser comunicadas imediatamente ao Gestor de Segurança da Informação ou à ETIR;
III - modificar configurações de segurança sem autorização expressa do Gestor de Segurança da Informação; e
IV - utilização ou instalação de recursos de TIC não homologados ou adquiridos pela UNILA.

Capítulo V –Monitoramento, Auditoria e Conformidade

Art. 22. Os ativos digitais estarão sujeitos a monitoramento contínuo e auditorias regulares, com registro de logs que permitam:

I - identificação de acessos não autorizados;
II - investigação de incidentes; e
III - reconstituição de eventos.

Art. 23. Os ativos físicos estarão sujeitos a controles de custódia, rastreamento de movimentação e auditorias periódicas.

Art. 24. As atividades de monitoramento e auditoria deverão respeitar:

I - as regras de sigilo aplicáveis às informações classificadas.
II - os limites legais;
III - o princípio da proporcionalidade;

Art. 25. O CGD receberá, em periodicidade definida, relatórios técnicos e estratégicos sobre a implementação da POSIN, o desempenho da segurança da informação e a conformidade institucional, conforme segue:

I - Relatórios do Gestor de Segurança da Informação (trimestral):

a) ações corretivas e preventivas implementadas;
b) avanços, dificuldades e propostas de melhoria;
c) controles aplicados em ambientes físicos e digitais;
d) indicadores de desempenho definidos na POSIN (conforme ISO/IEC 27004);
e) incidentes registrados e tratados;
f) situação dos planos de gestão de riscos e conformidade; e
g) resultados dos testes e atualizações dos planos de continuidade e recuperação de desastres.

II - Relatórios dos agentes operacionais:

a) Gestor de TIC (semestral): disponibilidade de serviços críticos, status de continuidade e análise de incidentes técnicos;

b) Encarregado de Dados (anual): conformidade com a LGPD, mapa de riscos de privacidade e demandas de titulares;
c) Assessor de Controle Interno (anual): aderência a controles internos, divergências frente a recomendações de órgãos de controle e lacunas críticas; e
d) ETIR (trimestral e imediato): incidentes cibernéticos tratados, eventos críticos e inventário de vulnerabilidades.

Art. 26. O CGD poderá solicitar relatórios extraordinários sempre que houver:

I - alterações normativas ou regulatórias que impactem a segurança da informação;
II - necessidade de deliberação urgente sobre temas relacionados à POSIN; e
III - ocorrência de eventos relevantes ou incidentes críticos.

Art. 27. Caso os relatórios mencionados no art. 24 identifiquem situações de risco grave, o CGD emitirá alerta estratégico imediato ao CGIRC, com recomendações de ação.

Art. 28. Os planos, indicadores e relatórios da POSIN deverão estar alinhados aos instrumentos de planejamento e prestação de contas da governança de TIC e da gestão de riscos da UNILA, incluindo:

I - Plano de Desenvolvimento Institucional (PDI);
II - Plano Estratégico de TIC (PETIC);
III - Plano Diretor de TIC (PDTIC);
IV - Plano de Gestão de Riscos Institucional;
V - Relatórios de conformidade e auditoria interna; e
VI - Painéis de indicadores estratégicos e operacionais.

Capítulo VI – Integração com a Governança de TIC e Gestão de Riscos

Art. 29. Compete ao CGD consolidar os relatórios previstos no art. 25 e elaborar análise estratégica anual a ser submetida ao CGIRC, contendo:

I - avaliação de riscos emergentes:

a) cenários de ameaças cibernéticas relevantes; e
b) tendências tecnológicas com impacto em segurança;

II - panorama da implementação da POSIN:

a) grau de cumprimento por unidade administrativa; e
b) progresso em planos de ação prioritários.

III - propostas de melhoria institucional:

a) ajustes normativos necessários;
b) investimentos críticos para o próximo ciclo; e
c) recomendações para atualização da matriz de riscos.

Parágrafo único. O relatório consolidado deverá ser submetido ao CGIRC até 31 de março do ano subsequente.

Art. 30. O cumprimento desta Política e dos normativos complementares será avaliado periodicamente pela UNILA, por meio de:

I - auditorias internas e externas;
II - certificações de requisitos de segurança da informação;

III - garantia de cláusulas de responsabilidade e sigilo em contratos, convênios e instrumentos congêneres; e
IV - verificações de conformidade.

Capítulo VII –Capacitação e Cultura de Segurança

Art. 31. Esta Política, suas atualizações e normas complementares serão formalmente comunicadas a todos os usuários de informação, com divulgação obrigatória:

I - anualmente, como parte do ciclo de conscientização institucional;
II - após atualizações relevantes; ou
III - no momento da admissão ou contratação.

Art. 32. A UNILA implementará programa contínuo de capacitação em segurança da informação, obrigatório para todos os usuários, contendo:

I - conteúdo sobre ameaças contemporâneas (ex.: *phishing*, *ransomware*);
II - instruções específicas sobre tratamento de dados pessoais conforme a LGPD;
III - simulações de incidentes para funções críticas; e
IV - treinamentos iniciais e periódicos, adaptados aos perfis de risco;

§ 1º Os materiais educacionais serão disponibilizados em ambiente virtual institucional, em formatos acessíveis, com versões atualizadas semestralmente.
§ 2º Terceiros e parceiros com acesso a ativos institucionais receberão capacitação equivalente às suas responsabilidades.

Capítulo VIII – Usuários de Informação e Responsabilidades Individuais

Art. 33. Todos os Usuários de Informação deverão participar de programas de capacitação em segurança da informação, privacidade e conformidade, conforme previsto no Art. 16 da POSIN.

Parágrafo único. A participação será registrada e considerada obrigatória para manutenção de acesso a ativos críticos.

Art. 34. As unidades organizacionais da UNILA devem promover ações de treinamento e conscientização para que seus colaboradores compreendam:

a) suas responsabilidades quanto à segurança da informação; e
b) os procedimentos voltados à proteção de dados pessoais e institucionais.

Parágrafo único. A capacitação deverá ser adequada aos papéis e responsabilidades dos colaboradores, conforme perfil de risco e acesso aos ativos.

Capítulo IX –Contratos Com Terceiros

Art. 35. Os contratos firmados com terceiros que tenham acesso a ativos de informação da UNILA deverão conter cláusulas que:

I - definam responsabilidades específicas em caso de violação ou incidente de segurança;
II - exijam conformidade com esta Política e com os regulamentos complementares; e
III - estabeleçam a realização de auditorias de segurança periódicas.

Capítulo X - Governança e Gestão da Segurança da Informação

Seção I – Da Estrutura e Competências de Governança de Segurança da Informação

Art. 36. A estrutura de governança da segurança da informação observará os princípios definidos na Política de Integridade da UNILA e nas normas ISO/IEC 27014 e ISO/IEC 38500, especialmente quanto a:

I - comportamento ético e supervisão efetiva;
II - desempenho e conformidade;
III - direcionamento estratégico; e
IV - responsabilidade institucional.

Art. 37. A governança da segurança da informação será composta pelas seguintes instâncias:

I - Alta Administração;
II - Comitê Permanente de Governança, Integridade, Riscos e Controle (CGRIC); e
III - Comitê de Governança Digital (CGD).

Art. 38. Compete à Alta Administração (Reitor(a), Vice-Reitor(a), Pró-Reitores, Diretores de Institutos e equivalentes):

I - avaliar riscos institucionais relacionados à segurança da informação;
II - garantir recursos humanos, financeiros e tecnológicos para implementação da POSIN;
III - integrar a segurança ao planejamento estratégico e à gestão de riscos;
IV - promover a cultura de segurança da informação;
V - supervisionar o desempenho da segurança com base em indicadores e relatórios técnicos; e
VI - tratar a segurança da informação como prioridade institucional.

Art. 39. Compete ao CGIRC:

I - aprovar a POSIN e suas alterações;
II - deliberar sobre diretrizes estratégicas e normas institucionais;
III - designar o Gestor de Segurança da Informação, garantindo-lhe autonomia técnica;
IV - emitir recomendações para aprimoramento dos controles e da cultura organizacional;
V - estabelecer limites de exposição a riscos;
VI - homologar planos de gestão de riscos e continuidade;
VII - promover integração entre governança, riscos, segurança da informação e proteção de dados;
VIII - supervisionar a implementação da POSIN e seu desempenho; e
IX - supervisionar diretrizes de continuidade e recuperação de desastres.

Art. 40. Compete ao CGD:

I - acompanhar planos de continuidade e recuperação de desastres;
II - acompanhar a segregação funcional nos processos de TIC e segurança;
III - aprovar normas complementares de segurança da informação;
IV - constituir grupos de trabalho técnicos;
V - monitorar a implementação da POSIN e reportar ao CGIRC;
VI - participar da elaboração da POSIN com as áreas técnicas;
VII - propor a POSIN e suas alterações ao CGIRC;

VIII - propor investimentos e assessorar ações de segurança;
IX - propor planos de gestão de riscos, continuidade e tratamento de incidentes; e
X - revisar anualmente os riscos e propor ajustes nos controles.

Parágrafo único. A composição, estrutura e funcionamento do CGD serão definidos em ato administrativo próprio.

Seção II – Da Estrutura e Competências da Gestão de Segurança da Informação

Art. 41. A gestão da segurança da informação será composta por:

I - Gestor de Segurança da Informação;
II - Gestor de Tecnologia da Informação e Comunicação;
III - Encarregado pelo Tratamento de Dados Pessoais (DPO);
IV - Assessor Especial de Controle Interno;
V - Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos (ETIR); e
VI - Agente Responsável pela ETIR.

Art. 42. Compete ao Gestor de Segurança da Informação:

I - acompanhar a atuação da ETIR e a integração com o SGSI;
II - acompanhar medidas corretivas em casos de violação;
III - acompanhar planos de continuidade e recuperação de desastres;
IV - assessorar o CGD e a Alta Administração na implementação da Política;
V - avaliar riscos e vulnerabilidades em processos e sistemas;
VI - coordenar a elaboração, revisão e atualização da POSIN;
VII - coordenar o Plano de Gestão de Riscos de Segurança da Informação e Cibernética;
VIII - definir e revisar indicadores de desempenho e métricas;
IX - elaborar relatórios periódicos sobre o desempenho da segurança da informação;
X - manter interlocução com órgãos externos, quando necessário;
XI - promover capacitação e divulgação da POSIN;
XII - propor recursos necessários à implementação da Política;
XIII - reportar-se diretamente ao CGD e à Alta Administração;
XIV - supervisionar controles em ambientes físicos e digitais; e
XV - verificar resultados de auditorias e propor melhorias.

Art. 43. Compete ao Gestor de TIC:

I - apoiar a identificação e tratamento de riscos tecnológicos;
II - atuar em conformidade com o Programa de Integridade da UNILA;
III - garantir conformidade com requisitos legais e regulatórios;
IV - implementar e manter sistemas e serviços conforme a POSIN;
V - integrar requisitos de segurança aos processos de desenvolvimento e operação de soluções tecnológicas;
VI - participar dos planos de continuidade e recuperação de TIC;
VII - promover capacitação da equipe de TIC;
VIII - reportar-se ao CGD e ao Gestor de Segurança da Informação; e
IX - supervisionar controles técnicos nos ambientes digitais.

Art. 44. Compete ao Encarregado de Dados Pessoais (DPO):

I - atuar como canal de comunicação com os titulares de dados;
II - coordenar o Plano de Gestão de Riscos de Privacidade;

III - estabelecer comunicação com CGD, Gestor de Segurança da Informação e áreas envolvidas;
IV - garantir conformidade com os princípios da LGPD;
V - integrar a gestão de riscos de privacidade ao SGSI;
VI - integrar os princípios do Programa de Integridade às ações de proteção de dados;
VII - participar da definição e revisão da POSIN e dos planos de riscos; e
VIII - supervisionar riscos relacionados à privacidade e proteção de dados.

Art. 45. Compete ao Assessor Especial de Controle Interno:

I - acompanhar a conformidade com normas e recomendações dos órgãos de controle;
II - acompanhar tecnicamente a implementação da POSIN;
III - apoiar a Auditoria Interna, quando solicitado, sem interferir na autonomia dos trabalhos;
IV - apoiar a institucionalização do SGSI;
V - apoiar ações de capacitação e promoção da cultura de segurança; e
VI - orientar gestores sobre controles internos e mitigação de riscos.

Art. 46. Compete à ETIR:

I - apoiar investigações e recuperação de sistemas;
II - atuar na detecção, registro, análise e resposta a incidentes;
III - manter registros rastreáveis de incidentes e ações;
IV - observar os princípios da proporcionalidade, legalidade e ética institucional;
V - participar dos planos de continuidade e recuperação;
VI - propor medidas de prevenção e correção de vulnerabilidades; e
VII - reportar periodicamente ao CGD e ao Gestor de Segurança da Informação.

Parágrafo único. A ETIR será composta por servidores da área de TIC, designados por portaria da Reitoria, com atribuições específicas e coordenação técnica definida.

Capítulo XI – Avaliação e da Prestação de Contas

Art. 47. A implementação da POSIN será integrada à Governança de Tecnologia da Informação e Comunicação (TIC) da UNILA, observando os princípios de:

I - comportamento ético;
II - desempenho e conformidade;
III - direcionamento estratégico; e
IV - responsabilidade institucional.

Art. 48. As ações de segurança da informação serão articuladas com os processos de gestão de riscos institucionais, em conformidade com a Política de Gestão de Riscos da UNILA e os princípios da ISO 31000, incluindo:

I - definição de apetite ao risco e critérios de impacto, conforme diretrizes do CGIRC;
II - identificação, avaliação, tratamento e monitoramento de riscos relacionados à segurança da informação e privacidade;
III - integração dos riscos de segurança aos planos de continuidade de negócios e recuperação de desastres; e
IV - registro e acompanhamento dos riscos em sistema institucional, com atualização periódica e validação pelo CGD.

Art. 49. A avaliação de riscos deverá utilizar metodologias compatíveis com a norma ISO 31010, conforme a natureza, complexidade e criticidade dos ativos envolvidos, podendo incluir:

I - análise de cenários;
II - análise de causa raiz;
III - avaliação baseada em indicadores;
IV - avaliação qualitativa e quantitativa; ou
V - matriz de probabilidade e impacto.

Art. 50. O Sistema de Gestão de Segurança da Informação (SGSI) deverá manter alinhamento com os processos de governança de TIC, incluindo:

I - planejamento estratégico de serviços e infraestrutura tecnológica;
II - gestão de mudanças e controle de ativos de informação;
III - monitoramento de desempenho e conformidade com SLAs e OLAs;
IV - avaliação contínua da eficácia dos controles técnicos e administrativos, conforme ISO/IEC 27004.

Capítulo XII –Tratamento de Incidentes

Art. 51. É dever do Usuário de Informação comunicar imediatamente qualquer suspeita ou ocorrência de incidente de segurança da informação ao Gestor de Segurança da Informação ou à ETIR.

§ 1º a omissão na comunicação poderá ser considerada infração à Política de Segurança da Informação.
§ 2º a comunicação deverá ser realizada por meio dos seguintes canais:

I - Central de Serviços – Formulário "***Segurança da Informação – Denúncias***"; ou
II - E-mail institucional: **gsi@unila.edu.br**;

Capítulo XIII – Disposições Finais

Art. 52. A não observância do disposto nesta Política sujeita o infrator às sanções administrativas previstas na legislação vigente, sem prejuízo das responsabilidades penal e civil.

Parágrafo único. É assegurado aos envolvidos o contraditório e a ampla defesa.

Art. 53. Esta Política será revisada:

I - periodicamente, a cada quatro anos;
II - ou com maior frequência, sempre que houver mudanças relevantes no ambiente institucional, nos riscos à segurança da informação ou nas melhores práticas aplicáveis.

Art. 54. Os casos omissos e dúvidas sobre a POSIN e seus documentos complementares devem ser submetidos ao Comitê de Governança Digital.

Art. 55. Esta Política substitui e absorve as disposições da Portaria nº 261/2021-GR, incorporando sua estrutura e competências à governança institucional da segurança da informação da UNILA.

Art. 56. Revoga-se a Resolução nº 3/2022/CGIRC, que instituiu a Política de Segurança da Informação (POSIN) da Universidade Federal da Integração Latino-Americana – UNILA, publicada no Boletim de Serviço nº 133, de 25 de julho de 2022.

Art. 57. O modelo do Termo de Responsabilidade será disponibilizado como Anexo I (usuários institucionais) e Anexo II (estudantes e pesquisadores), podendo ser atualizado por ato do CGD.

Art. 58. As unidades administrativas da UNILA deverão revisar, no prazo máximo de 180 (cento e oitenta) dias a contar da publicação desta Política, todos os normativos internos que tratem de:

I - matrícula, inscrição, registro acadêmico e demais procedimentos que envolvam o tratamento de dados pessoais;

II - processos administrativos, acadêmicos ou operacionais que utilizem ou compartilhem informações de titulares de dados;

III - sistemas, formulários, contratos ou instrumentos que envolvam coleta, armazenamento ou transmissão de dados pessoais ou sensíveis.

§ 1º A revisão deverá observar os princípios da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente os artigos 6º e 45.

§ 2º A revisão deverá considerar, quando aplicável, os princípios da Lei nº 13.726/2018, que trata da racionalização de atos e procedimentos administrativos e da proteção de dados no setor público.

§ 3º O Comitê de Governança Digital poderá emitir orientações complementares para apoiar as unidades na adequação dos normativos.

Art. 59. Esta Política entra em vigor na data de sua publicação.

Anexo I – TERMO DE RESPONSABILIDADE PARA USUÁRIOS DE INFORMAÇÃO

1. OBJETIVO

Formalizar o compromisso do(a) usuário(a) de informação com a Política de Segurança da Informação e Comunicação – POSIN da Universidade Federal da Integração Latino-Americana – UNILA, conforme disposto nos artigos 3º incisos II a IV, 10, 16 a 19 e 57 da POSIN e no artigo 46 da Lei nº 13.709/2018 – LGPD.

2. IDENTIFICAÇÃO DO USUÁRIO

Nome completo: _____ Matrícula/SIAPE: _____
Cargo/Função: _____ E-mail institucional: _____
Unidade/Departamento: _____

3. DECLARAÇÃO DE CIÊNCIA E COMPROMISSO

Declaro, para os devidos fins, que:

- Tomei conhecimento da Política de Segurança da Informação e Comunicação – POSIN, aprovada pela Resolução nº [XX/2025]/2025 do Comitê de Permanente de Governança, Integridade, Riscos e Controle - CGIRC;
- Estou ciente das minhas responsabilidades quanto à proteção dos ativos de informação sob minha guarda ou acesso;
- Comprometo-me a cumprir integralmente as diretrizes, normas e procedimentos definidos na POSIN e em seus regulamentos complementares;
- Reconheço que o descumprimento das obrigações previstas poderá acarretar sanções administrativas, civis e penais, conforme legislação vigente.

4. PROTEÇÃO DE DADOS PESSOAIS

Nos termos do artigo 46 da Lei nº 13.709/2018 – LGPD, comprometo-me a:

- Tratar dados pessoais com responsabilidade, segurança e respeito à privacidade;
- Adotar medidas para prevenir acessos não autorizados, vazamentos ou qualquer forma de uso indevido;
- Comunicar imediatamente à autoridade competente qualquer incidente de segurança envolvendo dados pessoais.

5. VEDAÇÕES

Estou ciente de que é vedado:

- Compartilhar credenciais de acesso com terceiros;
- Utilizar sistemas institucionais para fins pessoais que comprometam a segurança ou a integridade dos ativos de informação;
- Modificar configurações de segurança sem autorização expressa;
- Utilizar recursos de TIC não homologados pela UNILA.

6. VIGÊNCIA E ATUALIZAÇÃO

Este termo permanecerá vigente enquanto perdurar o vínculo funcional, acadêmico ou contratual com a UNILA, podendo ser atualizado conforme alterações na POSIN ou na legislação aplicável.

7. ASSINATURA

Local e data: _____ Assinatura do(a) usuário(a): _____

Este termo poderá ser formalizado por meio eletrônico, conforme previsto no parágrafo único do Art. 16 da POSIN.

Anexo II – TERMO DE RESPONSABILIDADE PARA USUÁRIOS DE INFORMAÇÃO – SIMPLIFICADO

UNIVERSIDADE FEDERAL DA INTEGRAÇÃO LATINO-AMERICANA – UNILA
TERMO DE RESPONSABILIDADE – ESTUDANTES E PESQUISADORES

Eu, **[NOME COMPLETO]**, matrícula **[NÚMERO]**, vinculado(a) ao curso/projeto **[NOME]**, declaro que:

1. Estou ciente de que o acesso a sistemas, redes, documentos e dados da UNILA está sujeito às regras da Política de Segurança da Informação e Comunicação – POSIN.
2. Comprometo-me a:
   a. Utilizar os recursos institucionais exclusivamente para fins acadêmicos e autorizados;
   b. Proteger as informações acessadas, especialmente dados pessoais e acadêmicos;
   c. Não compartilhar minhas credenciais de acesso com terceiros;
   d. Comunicar imediatamente qualquer incidente ou suspeita de violação à equipe responsável.
3. Reconheço que o descumprimento das regras poderá resultar em sanções administrativas e acadêmicas, conforme regulamentos internos da UNILA.

Local e data: _____

Assinatura: _____

Este termo poderá ser formalizado por meio eletrônico, conforme previsto no parágrafo único do Art. 16 da POSIN.

Anexo III - Fluxo de Gestão de Incidentes de Segurança da Informação

Instrumento complementar à POSIN – conforme Art. 15, inciso V

1. PROPÓSITO

Estabelecer o fluxo institucional para identificação, registro, análise, resposta e encerramento de incidentes de segurança da informação, visando minimizar impactos, restaurar serviços e prevenir recorrências, conforme diretrizes da POSIN - 2025 e padrões ISO/IEC 27035 e ITIL v4.

2. ÂMBITO

Aplica-se a todos os ativos de informação sob gestão da UNILA, incluindo sistemas, redes, documentos, dados pessoais e ambientes físicos ou digitais, bem como aos usuários de informação.

3. DEFINIÇÕES

- Incidente de Segurança da Informação: Evento confirmado ou suspeito que compromete a confidencialidade, integridade ou disponibilidade de ativos de informação.
- ETIR: Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, conforme Art. 44 da POSIN.
- Usuário de Informação: Pessoa física habilitada para acessar ativos institucionais (Art. 10, XIX).
- SGSI: Sistema de Gestão de Segurança da Informação (Art. 10, VII).

4. RESPONSABILIDADES

Papel	Responsabilidades
Usuário de Informação	Comunicar imediatamente qualquer suspeita ou ocorrência de incidente (Art. 51)
ETIR	Detectar, registrar, analisar e responder aos incidentes (Art. 46)
Gestor de Segurança da Informação	Coordenar o tratamento, propor ações corretivas e reportar ao CGD (Art. 42)
Gestor de TIC	Apoiar tecnicamente a contenção e recuperação (Art. 43)
CGD	Receber relatórios periódicos e emitir alertas estratégicos (Art. 40 e 26)

5. FLUXO OPERACIONAL

5.1. Detecção e Comunicação

- Incidente identificado por usuário, sistema ou auditoria.
- Comunicação imediata via:
    - E-mail: gsi@unila.edu.br
    - Formulário: “Segurança da Informação – Denúncias” (Central de Serviços)

5.2. Registro

- ETIR registra o incidente em sistema institucional, com:
    - Data/hora
    - Ativo afetado
    - Tipo de incidente
    - Impacto estimado
    - Origem da comunicação

5.3. Classificação

- Classificação por criticidade:
    - Baixa: sem impacto operacional
    - Média: impacto limitado e reversível
    - Alta: afeta serviços críticos ou dados sensíveis
    - Grave: risco legal, reputacional ou institucional

5.4. Análise Técnica

- ETIR realiza análise de causa raiz, coleta de evidências e avaliação de impacto.
- Apoio do Gestor de TIC e áreas envolvidas.

5.5. Resposta e Contenção

- Ações imediatas para mitigar o incidente:
    - Isolamento de sistemas
    - Revogação de acessos
    - Aplicação de correções

5.6. Recuperação

- Restauração dos serviços e ativos afetados.
- Verificação da integridade e funcionalidade.

5.7. Encerramento

- Registro das ações tomadas.
- Classificação final do incidente.
- Comunicação ao CGD e, se necessário, ao CGIRC (Art. 26).

5.8. Lições Aprendidas

- ETIR elabora relatório técnico com:
    - Causa raiz
    - Medidas corretivas
    - Propostas de melhoria
- Integração ao SGSI e ao plano de gestão de riscos.

6. MONITORAMENTO E CONFORMIDADE

- Indicadores definidos no SGSI (Art. 15º IV e Art. 42 VII)
- Auditorias periódicas (Art. 22 e Art. 24)
- Relatórios trimestrais e extraordinários ao CGD (Art. 40 e 26)

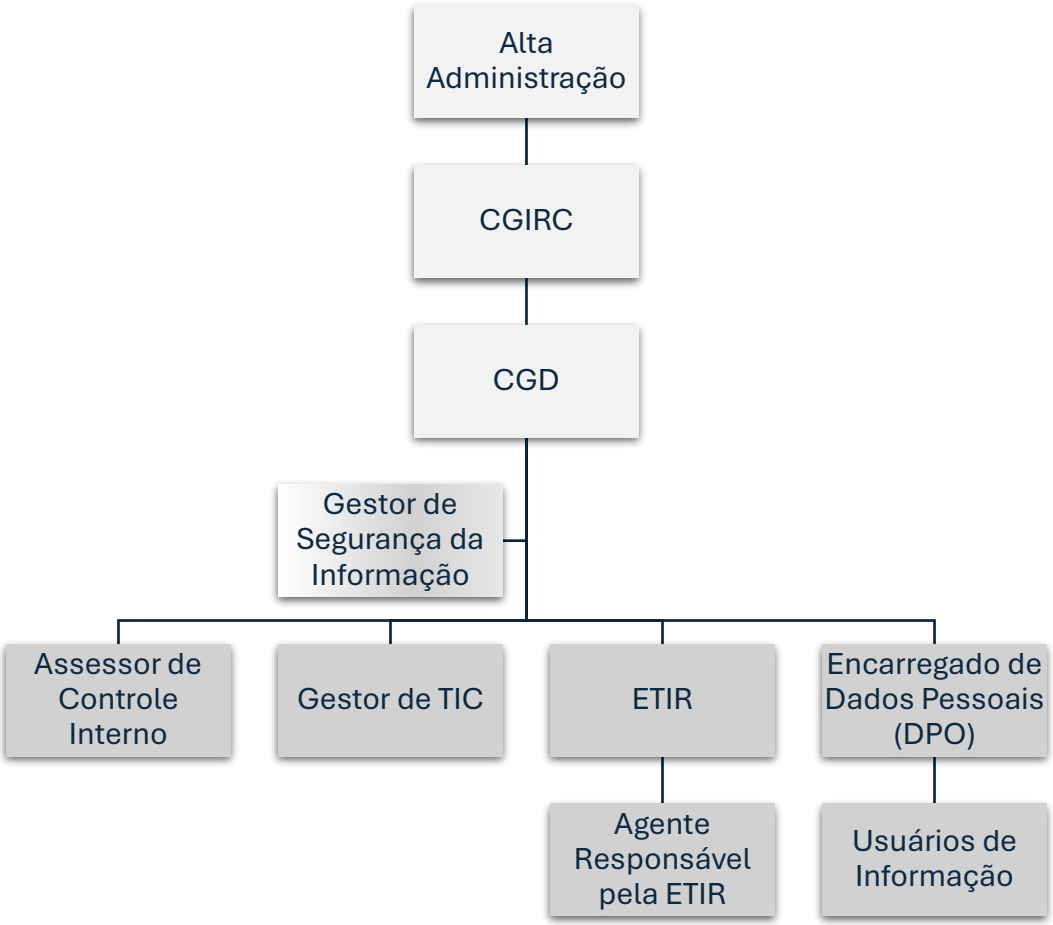
7. REVISÃO E ATUALIZAÇÃO

Este fluxo será revisado anualmente ou sempre que houver:

- Alterações na POSIN;
- Mudanças nos riscos institucionais;

Atualizações nas normas ISO/IEC 27035 ou ITIL v4.

Anexo IV - Estrutura de Governança e Segurança da Informação



Descrição das funções principais

- **Alta Administração** (Reitor(a), Vice, Pró-Reitores, Diretores)**:** Define prioridades, aloca recursos e supervisiona o desempenho da segurança da informação.
- **CGIRC:** Aprova a POSIN, define diretrizes estratégicas e supervisiona riscos institucionais.
- **CGD:** Coordena a implementação da POSIN, propõe normas e acompanha planos de continuidade.
- **Gestor de Segurança da Informação:** Coordena o SGSI, avalia riscos, propõe melhorias e reporta ao CGD.
- **Gestor de TIC:** Implementa soluções tecnológicas seguras e integra segurança aos processos de TIC.
- **DPO (Encarregado de Dados Pessoais):** Garante conformidade com a LGPD e atua como canal com titulares de dados.
- **Assessor de Controle Interno:** Acompanha conformidade com normas e apoia auditorias.
- **ETIR:** Detecta, analisa e responde a incidentes de segurança da informação.
- **Agente da ETIR:** Coordena tecnicamente a equipe de resposta a incidentes.
- **Usuários de Informação:** Devem cumprir a POSIN, proteger ativos e comunicar incidentes.

Referências Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2024 – Tecnologia da informação — Segurança da informação, cibersegurança e proteção da privacidade — Sistemas de gestão de segurança da informação — Requisitos**. Rio de Janeiro: ABNT, 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2022 – Tecnologia da informação — Segurança da informação, cibersegurança e proteção da privacidade — Controles de segurança da informação**. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27701:2019 – Técnicas de segurança — Extensão da ISO/IEC 27001 e ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes**. Rio de Janeiro: ABNT, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27014:2021 – Tecnologia da informação — Segurança da informação, cibersegurança e proteção da privacidade — Governança da segurança da informação**. Rio de Janeiro: ABNT, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000:2018 – Gestão de riscos — Diretrizes**. Rio de Janeiro: ABNT, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 22301:2024 – Segurança e resiliência — Sistemas de gestão da continuidade de negócios — Requisitos**. Rio de Janeiro: ABNT, 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados Pessoais – LGPD). *Diário Oficial da União: seção 1*, Brasília, DF, 15 ago. 2018.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal (Lei de Acesso à Informação – LAI). *Diário Oficial da União: seção 1*, Brasília, DF, 18 nov. 2011.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). *Diário Oficial da União: seção 1*, Brasília, DF, 24 abr. 2014.

CENTER FOR INTERNET SECURITY. **CIS Critical Security Controls v8 – Controles Essenciais para Defesa Cibernética Eficaz**. East Greenbush, NY: CIS, 2021. Tradução técnica não oficial.

PRESIDÊNCIA DA REPÚBLICA. GSI/PR. **Portaria nº 93, de 26 de fevereiro de 2021**. Aprova o Glossário de Segurança da Informação da Administração Pública Federal. *Diário Oficial da União: seção 1*, Brasília, DF, 1 mar. 2021.

MINUTA Nº 1/2026 - CGD (10.00.00.20)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 05/05/2026 09:06)
SALANIR FERNANDES DOS SANTOS JUNIOR
CHEFE DE COORDENADORIA - TITULAR
CTIC (10.01.05.20.03)
Matrícula: ###148#7

Visualize o documento original em https://sig.unila.edu.br/documentos/ informando seu número: ***1****, ano:* ***2026****, tipo:* ***MINUTA****, data de emissão:* ***05/05/2026*** *e o código de verificação:* ***03a2a908b5***