
Política de Alto Nivel de Seguridad de la Información y Ciberseguridad

1. Justificación:

La Política de Alto Nivel de Seguridad de la Información y Ciberseguridad de la UNED es el marco rector institucional que define la visión, los principios, las directrices estratégicas y las responsabilidades generales para la protección de la información y los activos tecnológicos de la universidad. Reconoce la información como un activo estratégico esencial para el cumplimiento de los objetivos académicos, administrativos y misionales de la UNED, y establece las bases para preservar su confidencialidad, integridad, disponibilidad y trazabilidad. Esta política orienta la toma de decisiones en materia de seguridad de la información, ciberseguridad y tecnologías emergentes, promoviendo una gestión alineada con estándares internacionales, la normativa nacional y el modelo de gobierno institucional.

La existencia de esta política es necesaria ante un entorno digital cada vez más complejo y expuesto a amenazas cibernéticas, incidentes de seguridad y riesgos tecnológicos que pueden afectar la continuidad operativa, la credibilidad institucional y el cumplimiento legal de la UNED. El uso intensivo de tecnologías de información, servicios en la nube, teletrabajo y soluciones basadas en Tecnologías Emergentes exige contar con directrices claras y homogéneas que permitan identificar, evaluar y tratar los riesgos de manera sistemática. La política responde a esta necesidad proporcionando un marco preventivo y correctivo que fortalece la resiliencia institucional, reduce la probabilidad de incidentes y orienta la adopción segura y ética de nuevas tecnologías.

Asimismo, la adopción de esta política y la Guía de Seguridad de la Información y Ciberseguridad representa un paso fundamental en el proceso de madurez institucional de la UNED en materia de gestión de la seguridad de la información y la ciberseguridad. Este proceso implica avanzar hacia un modelo de gobernanza más sólido, donde las

Consejo Universitario

directrices estratégicas se articulan con estructuras organizacionales claras, necesarios para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) de la UNED. Del mismo modo, la política promueve una participación corresponsable de las autoridades universitarias, las personas funcionarias, la comunidad estudiantil y diversos actores relacionados, quienes desempeñan un papel esencial en la protección de la integridad, disponibilidad y confidencialidad de la información institucional. Este involucramiento colectivo fortalece la cultura organizacional de seguridad, consolidando prácticas sostenibles que permiten a la universidad anticipar, gestionar y mitigar riesgos de forma progresiva, sistemática y alineada con estándares internacionales.

Para la implementación efectiva de la política, la UNED cuenta con la Guía de Seguridad de la Información y Ciberseguridad, la cual constituye su documento operativo. Esta guía traduce las directrices de alto nivel en controles, procedimientos, guías, responsabilidades y prácticas concretas de obligatorio cumplimiento para personas funcionarias, comunidad estudiantil, proveedores y terceros. De esta manera, la política establece el qué y el por qué, mientras que la guía define el cómo, permitiendo la implementación, supervisión y mejora continua del Sistema de Gestión de Seguridad de la Información. En conjunto, ambos instrumentos consolidan una cultura institucional de seguridad, responsabilidad compartida y cumplimiento normativo, fortaleciendo la capacidad de la UNED para proteger sus activos de información y sostener sus operaciones de forma segura y confiable.

2. Propósito:

Establecer el marco rector de gobierno, gestión y mejora continua de la seguridad de la información y la ciberseguridad en la UNED, mediante la definición de principios, directrices estratégicas y responsabilidades generales que orienten la protección de la información, los activos tecnológicos y los servicios institucionales.

Consejo Universitario

3. Alcance:

Las directrices establecidas en la presente política deben ser observados para promover la protección y la seguridad de toda la información y de la infraestructura tecnológica de la Universidad Estatal a Distancia (UNED). Asimismo, dichas directrices deben ser conocidos, acatados y aplicados por la totalidad de las personas funcionarias de la UNED, la población estudiantil, así como por terceros que cuenten con acceso a los sistemas de información y a la red institucional.

4. Responsabilidades:

- **Comisión Estratégica de Tecnología de Información y Comunicaciones (CETIC):** Debe conocer y dar visto bueno al documento de Política de Alto Nivel de Seguridad de la Información y Ciberseguridad de la UNED, aprobar los niveles de seguridad y transmitir las directrices de aplicación de ésta.
- **Consejo Universitario (CU):** Debe aprobar el documento de Política de Alto Nivel de Seguridad de la Información y Ciberseguridad de la UNED.
- **Unidad de Seguridad Digital (USD):** Debe velar por el cumplimiento de la presente política, implementando los niveles de seguridad adecuados aprobados por la CETIC y el CU, como también concientizar a todos los funcionarios de la UNED, población estudiantil, en Gestión de Seguridad de la Información.
- **Responsable de la Seguridad de la Información (CISO):** Debe velar por la actualización de la presente política y las próximas versiones de esta.
- **Dirección de Tecnología Información y Comunicaciones (DTIC):** Debe designar el personal idóneo para que establezca y configure los controles de seguridad de la información y ciberseguridad, acogiendo las directrices de seguridad definidos en la presente política. A su vez, apoyar activamente en la implementación de controles de seguridad de la información y ciberseguridad dentro de la universidad.

Consejo Universitario

Nota: Hasta que no exista la figura de CISO a nivel institucional, la USD será la responsable de esta labor.

5. Definiciones:

- **Activos de información:** un activo se define como cualquier ítem de valor para la organización donde se almacena y procesa información. (ISO, s.f.)
- **Ciberseguridad:** Prevención de daños, protección y restauración de ordenadores, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicaciones por cable y comunicaciones electrónicas, incluida la información contenida en ellos, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio. (NIST)
- **CSIRT-UNED:** (Computer Security Incident Response Team, por sus siglas en inglés) es el equipo institucional responsable de coordinar la prevención, detección, análisis, respuesta y recuperación ante incidentes de seguridad de la información y ciberseguridad que afecten a los sistemas, los servicios tecnológicos y los activos de información de la UNED.
- **Confidencialidad:** Preservar las restricciones autorizadas sobre el acceso y la divulgación de la información, incluidos los medios para proteger la privacidad personal y la información patentada (NIST)
- **Disponibilidad:** Garantizar el acceso oportuno y confiable a la información y su uso (NIST)
- **Dueño del activo de información:** funcionario con autoridad estatutaria u operativa sobre determinada información y responsable de establecer los controles para su generación, clasificación, recolección, procesamiento, difusión y disposición. (ISO:27001).
- **Integridad:** característica de la información por la cual solo que es modificada por personas o sistemas autorizados y de una forma permitida. (ISO:27001).
- **Seguridad de la información:** Es la preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO:27001)

Consejo Universitario

- **Sistema de Gestión de Seguridad de la Información:** parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información. (ISO:27001)
- **Tecnologías Emergentes:** son aquellas innovaciones científicas y tecnológicas que están en una fase temprana de desarrollo, pero que tienen el potencial de transformar profundamente la sociedad, la economía, las industrias y la forma en que vivimos o trabajamos.

6. Marcos de Referencia Aplicables

- Norma ISO/IEC 27001:2022
- Norma ISO/IEC 22989:2022
- NIST SP 800-53

7. Legislación y normativa interna relacionada:

- Código de buenas prácticas para la ciberseguridad de la IA.
- Estrategia Nacional de Ciberseguridad.
- Estrategia Nacional de Inteligencia Artificial.
- Guía de Clasificación, Etiquetado y Manejo de Activos de Información.
- Guía de Seguridad de la Información y Ciberseguridad
- Ley N.º 8968: Ley de protección de la persona frente al tratamiento de sus datos personales.
- Manual de seguridad de la información y ciberseguridad de la UNED.
- Marco de gobierno y gestión de TI de la UNED, objetivo de gobierno y objetivo de gestión: seguridad de la información.
- Normas sobre el uso del correo electrónico en la UNED.
- Normas técnicas para el gobierno y gestión de las tecnologías de la información del MICITT, proceso XI seguridad y ciberseguridad.
- Plan Táctico de Tecnologías de Información

- Reglamento de Uso de Recursos Informáticos de la UNED.

8. Directrices generales de la política de alto nivel de seguridad de la información y ciberseguridad.

La Universidad Estatal a Distancia (UNED) reconoce la información como un activo esencial para el logro de sus objetivos institucionales; por ello, establece la necesidad de identificar, proteger y gestionar de manera adecuada sus activos de información frente a los riesgos que puedan afectarlos.

Los objetivos que se presentan a continuación se sustentan en las directrices definidas en la Guía de Seguridad de la Información y Ciberseguridad, así como en el Marco de Gobierno de Tecnologías de Información de la UNED:

Esta política contempla los siguientes objetivos:

- a. Establecer la gobernanza en seguridad de la información, ciberseguridad y tecnologías emergentes, velando por la protección de la información y de los activos tecnológicos institucionales sea dirigida, gestionada y supervisada de manera integral, basada en la gestión de riesgos y en alineación con los objetivos estratégicos de la institución.
- b. Establecer los controles en materia de seguridad de la información, ciberseguridad y tecnologías emergentes, basados en los riesgos identificados y alineados con buenas prácticas internacionales, que salvaguarden la protección adecuada de los activos de información institucionales.
- c. Proteger la disponibilidad, integridad y confidencialidad de la información y de los servicios tecnológicos que respaldan los procesos administrativos y académicos, con el fin de preservar la operación continua ante eventos adversos o incidentes de seguridad.
- d. Promover una cultura institucional sólida de seguridad de la información y ciberseguridad, orientada a fortalecer la sostenibilidad y la efectividad de las

Consejo Universitario

medidas implementadas para la protección de la información y de los activos tecnológicos institucionales.

- e. Gestionar de forma efectiva los incidentes de seguridad de la información y ciberseguridad, en coordinación con el CSIRT-UNED y los entes nacionales, con el fin de mejorar la respuesta institucional y minimizar el impacto de los eventos de seguridad.
- f. Velar por el cumplimiento efectivo de los requisitos legales, regulatorios, normativos e institucionales aplicables a la seguridad de la información, ciberseguridad y tecnologías emergentes, fomentando el monitoreo, la evaluación y la mejora continua de los controles, procesos y prácticas de seguridad, con el fin de fortalecer la gestión de riesgos y la protección de los activos de información de la institución.

Para el efecto de nuestro compromiso se lista las siguientes directrices generales:

- Se debe aplicar la metodología del sistema específico de valoración del riesgo institucional (SEVRI) para la identificación y evaluación de los riesgos de TI, seguridad de la información y ciberseguridad, a partir de la cual se definan las acciones, controles y criterios necesarios para el tratamiento de los riesgos.
- Se deben establecer directrices para la evaluación, adopción, uso seguro y supervisión de las tecnologías emergentes o habilitadoras (tales como inteligencia artificial, internet de las cosas, blockchain, realidad aumentada y virtual, automatización avanzada, entre otras), tomando en consideración los siguientes aspectos:
 - Impacto en la seguridad de la información, privacidad de datos personales y derechos de las personas estudiantes y colaboradores.
 - Riesgos de integridad, disponibilidad y confidencialidad asociados a nuevas plataformas o herramientas.
 - Cumplimiento de la legislación costarricense vigente.

Consejo Universitario

- Toda persona funcionaria que labore directamente con la UNED debe conocer y comprender los riesgos asociados a la información, así como adoptar y aplicar las políticas establecidas, con el fin de promover el adecuado desarrollo, desempeño y la mejora continua de la seguridad de la información, la ciberseguridad y el uso de tecnologías emergentes.
- Se debe de identificar y documentar los riesgos para la seguridad de la información, el entorno de amenazas de seguridad de la información, ciberseguridad y tecnologías emergentes actual o previsto, lecciones aprendidas de eventos o incidentes, resultado de revisiones, evaluaciones o auditorías.
- La UNED debe implementar mecanismos de respuesta inmediatos, de intervención y adaptación ante cualquier evento que pueda comprometer la seguridad de la información, la infraestructura tecnológica, los servicios institucionales o el funcionamiento operativo. Esto incluye incidentes de ciberseguridad, fallas críticas, vulnerabilidades emergentes, cambios tecnológicos disruptivos o variaciones sustanciales en el entorno digital o de amenazas.
- La UNED deberá realizar auditorías de seguridad de la información, ciberseguridad y tecnologías emergentes conforme a un enfoque basado en riesgos, considerando la criticidad de los activos de información y servicios tecnológicos, los resultados de evaluaciones previas, la disponibilidad de recursos y las necesidades institucionales, con el fin de verificar el cumplimiento de las políticas, normas y procedimientos de seguridad de la información y ciberseguridad.
- La UNED debe mantener un inventario actualizado de todos los activos de información y que estos sean clasificados, etiquetados, utilizados, protegidos, retenidos y eliminados conforme a su nivel de sensibilidad, los requisitos legales y las necesidades académicas y operativas de acuerdo con la Guía de Clasificación, Etiquetado y Manejo de Activos de Información. Toda información deberá contar con controles adecuados para prevenir acceso no autorizado, pérdida, alteración, destrucción o divulgación indebida.

Consejo Universitario

- El acceso, manejo y tratamiento de la información deberán basarse en el principio de mínimo privilegio, estableciendo que los usuarios solo accedan a lo estrictamente necesario. La institución implementará medidas técnicas, organizativas y de concientización para prevenir la fuga de información, mantener la trazabilidad de cambios o solicitudes formales, velar por la destrucción de datos una vez cumplida su finalidad o periodo de retención.
- Todo acceso a los sistemas, servicios tecnológicos, infraestructura tecnológica y activos de información institucionales deberá ser previamente autorizado conforme a procedimientos formalmente establecidos, aplicando los principios de necesidad de conocer y mínimo privilegio. Los accesos otorgados a terceros deberán contar con una justificación, responsable institucional, alcance definido, vigencia determinada y mecanismos de trazabilidad y supervisión. Ninguna autoridad, jefatura o persona funcionaria podrá autorizar excepciones a los controles de acceso establecidos fuera de los procedimientos institucionales aprobados.
- La planificación táctica de las Tecnologías de Información y Comunicación deberá desarrollarse conforme a lo establecido en la presente política y en el Marco de Gobierno de TI, integrando los principios y disposiciones de seguridad de la información, ciberseguridad y tecnologías emergentes, así como criterios de gestión de riesgos, protección de los activos de información, continuidad de los servicios y cumplimiento normativo como parte integral de la planificación tecnológica.
- La Unidad de Seguridad Digital debe procurar que todas las personas funcionarios de la UNED como también la población estudiantil, estén familiarizados con esta política.

9. Vigencia y actualización

Esta política debe ser revisada anualmente o cuando se produzcan cambios relevantes en la estrategia institucional, por la Dirección de Tecnologías de Información y Comunicaciones (DTIC), en coordinación con la Unidad de Seguridad Digital (USD) en

Consejo Universitario

cumplimiento con los nuevos requerimientos en materia de seguridad de información, ciberseguridad y tecnologías emergentes.

Los resultados de esta revisión serán enviados al CONRE para su análisis y comunicados al Consejo Universitario para lo que corresponda.

--

Acuerdo tomado por el Consejo Universitario de la Universidad Estatal a Distancia, en sesión ordinaria 3152-2026, Artículo IV-A, inciso 2) celebrada el 17 de setiembre del 2026