Políticas para el uso y desarrollo de tecnologías de información y comunicación de la UNED

1. Universalización de los servicios tecnológicos del campus digital institucional

Universalizar los servicios tecnológicos del campus digital institucional, para optimizar el desempeño de las actividades sustantivas de la universidad (docencia, investigación, extensión, producción de materiales y vida estudiantil) y la gestión administrativa, basado en los principios de equidad, usabilidad, accesibilidad, seguridad, transparencia, confidencialidad e inclusión.

2. Fortalecimiento de los procesos institucionales por medio de las TIC

Fortalecer los procesos institucionales estratégicos (académicos, estudiantiles, gestión administrativa, gestión política, entre otros), por medio del uso de las herramientas de Tecnologías de Información y Comunicación (TIC) que permitan organizarlos, ampliarlos, articularlos, actualizarlos, simplificarlos y estandarizarlos, con la finalidad de mejorar la gestión institucional.

3. Dotación de recursos para el uso y desarrollo de TIC

Incorporar en los planes estratégicos de tecnología de la información y comunicación institucional y en los correspondientes planes operativos anuales, los recursos financieros, humanos y técnicos necesarios para el uso y desarrollo de las TIC, con fundamento en las posibilidades institucionales.

4. Investigación en TIC

Realizar investigación en TIC, para el mejoramiento e integración de los sistemas de información y comunicación institucionales existentes, así como para el desarrollo, implementación y la valoración de la efectividad de nuevas herramientas TIC, que apoyen el fortalecimiento de la modalidad de educación a distancia, en concordancia con la misión social de la UNED.

5. Plataformas e infraestructura tecnológica

Utilizar prioritariamente criterios de neutralidad tecnológica al adquirir, instalar y actualizar la plataforma tecnológica, para: el soporte de los sistemas de información institucionales, brindar interoperabilidad con otras plataformas dentro y fuera de la

Institución, mantener escalabilidad y continuidad de los servicios académicos y administrativos institucionales.[1]

6. Seguridad de la información TIC

Implementar un marco de seguridad TIC que garantice de manera razonable, la protección, acceso, confidencialidad, discrecionalidad, integridad, disponibilidad y divulgación de la información.[2]

7. Diseño y gestión del modelo de arquitectura de información

a) Establecer una estrategia de documentación y organización de información integrada, estandarizada, relacionada y georeferenciada, que permita una actualización periódica, y apoye la toma de decisiones estratégicas y operativas.
b) Gestionar y validar la calidad de datos, por medio de los responsables o administradores de los procesos, con usuarios y perfiles claramente definidos y autorizados; con mecanismos de seguimiento y evaluación.
c) Optimizar las capacidades de la plataforma tecnológica institucional para realizar la captura, almacenamiento, transferencia, búsqueda, análisis y visualización de grandes volúmenes de información (big data).

8. Servicios estudiantiles, académicos y administrativos inclusivos centrados en el usuario

Establecer que la plataforma tecnológica que utilice la Universidad para brindar apoyo a la gestión académica, administrativa y de vida estudiantil a los diversos usuarios, sea accesible, ubicuo, segura y de calidad.

9. Alfabetización para el uso de TIC

Definir e implementar estrategias metodológicas innovadoras que permitan a los diversos actores universitarios, la generación de conocimientos, y el desarrollo de competencias, habilidades, destrezas y actitudes en el uso de TIC.

Acuerdo tomado por el Consejo Universitario, en sesión 2401-2015, Art. III, inciso 1-a) celebrada el 05 de febrero del 2015

[1] Se entiende por plataforma tecnológica, la infraestructura (servidores, equipos de comunicaciones y otros dispositivos), sus sistemas operativos y aplicaciones específicas.
[2] El marco de seguridad debe incluir:
a. Portafolio de recursos de TI.
b. Evaluación del riesgo de los recursos de TI.
c. Establecimiento de medidas de seguridad asociados a los riesgos en TI.
d. Evaluación del impacto de las medidas de seguridad.
e. Capacitación y concientización.