# Políticas Institucionales

UNIMINUTO
Corporación Universitaria Minuto de Dios
Educación de Calidad al alcance de todos
Vigilada MinEducación

Consejo de Fundadores.

Acuerdo No. 345 del 21 de septiembre de 2021.

# POLÍTICA DE INFRAESTRUCTURA TECNOLÓGICA

## PRESENTACIÓN DE LA POLÍTICA

Para la Corporación Universitaria Minuto de Dios – UNIMINUTO es importante asegurar la disponibilidad, la calidad, la oportunidad, el análisis y la protección de la información, garantizando una adecuada gestión y administración integral de su Ecosistema Digital, y reconociendo que la articulación de la tecnología, los procesos, así como de las personas son fundamentales para la operación de la Institución.

En virtud de ello, establece la Política de Infraestructura Tecnológica en búsqueda de la aplicación de buenas prácticas y estándares internacionales que le permitan la operatividad de sus plataformas tecnológicas, garantizando así su disponibilidad, integridad y confidencialidad.

## REFERENTES

Normatividad Externa

a) Ley 30 de diciembre 28 de 1992, por el cual se organiza el servicio público de la Educación Superior.
b) Ley 1341 de julio 30 de 2009 Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las Comunicaciones -TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
c) Decreto 1330 de julio 25 de 2019 Ministerio de Educación Nacional. Artículo. 2.5.3.2.3.1.3, numeral c.
d) Resolución 15224 de agosto 24 de 2020 Ministerio de Educación Nacional. Artículo 27.

Referentes Institucionales

a) Proyecto Educativo Institucional – PEI de UNIMINUTO.
b) Política de la Infraestructura Tecnológica.
c) Lineamiento de respaldo de copias de seguridad.

Marco de Referencia

a) **ITIL V4:2019**: Este marco de referencia establece buenas prácticas de tecnología, el cual recomienda desarrollar procedimientos efectivos para controlar y definir la disponibilidad, la calidad y la oportunidad de los datos e información.
b) **NTC-ISO-IEC 27001:2013**: Esta norma internacional permite el aseguramiento y requisitos con un programa de sensibilización, cultura, adopción y comunicación en gestión de seguridad de los datos e información, según la política de seguridad de la información.
c) **ISO 20000-1**: La Organización Internacional de Estandarización (ISO), a través de las normas recogidas en ISO / IEC 20000, establece una implementación efectiva y un planteamiento estructurado para desarrollar servicios de tecnología de la información fiables en lo referente a la gestión de servicios de TI.
d) **ISO 20000-9**: GUÍA PARA LA APLICACIÓN DE ISO / IEC 20000-1 A SERVICIOS EN LA NUBE Se trata de una guía para implementar ISO / IEC 20000-1: 2011 en proveedores de servicios que ofrecen servicios en la nube (Cloud Services). Es aplicable a diferentes categorías de servicios en la nube, como las definidas en ISO / IEC 17788 / ITU-T Y.3500 e ISO / IEC 17789 / ITU-T Y.3502. Cubre todo tipo de servicios en la nube tales como:
    - Servicio (IaaS) – Infraestructura
    - Servicios (PaaS) – Plataformas
    - Servicio (SaaS) – Software

    Todos los requisitos en ISO / IEC 20000-1 pueden ser aplicables a los proveedores de servicios en la nube. La guía se presenta como un conjunto de escenarios que pueden abordar muchas de las actividades típicas

de un proveedor de servicios en la nube.

e) **ISO/IEC 27017**: Esta norma perteneciente a la familia ISO/IEC 27000:2015. Incluye pautas y directrices sobre los controles de seguridad de la información relacionadas con servicios en la nube.
f) **ISO / IEC 27018-2014**: Es la norma que establece criterios sobre controles y directrices con relación a medidas de protección de información de identificación personal (PII), de conformidad con los principios de privacidad en la norma ISO / IEC 29100 para entornos que de trabajo con sistemas de almacenamiento público en la nube.
g) **Normas IEEE 802.3**: Esta norma define un modelo de red de área local utilizando el protocolo de acceso al medio CSMA/CD con persistencia de 1, es decir, las estaciones están permanentemente a la escucha del canal y cuando lo encuentran libre de señal efectúan sus transmisiones inmediatamente. Esto puede llevar a una colisión que hará que las estaciones suspendan sus transmisiones, esperen un tiempo aleatorio y vuelvan a intentarlo.
h) **ANSI/TIA-942**: Es un estándar de calidad que especifica los requisitos para centros de datos. La topología presentada en la norma es aplicable a cualquier centro de datos de cualquier tamaño y cubre toda la infraestructura física, incluidos, entre otros requisitos: ubicación del sitio, sistema eléctrico, mecánico, seguridad contra incendios, telecomunicaciones, seguridad y entre otros. La última versión es la: ANSI/TIA 942 revisión B (12 julio de 2017).

**FORMULACIÓN DE LA POLÍTICA**

En aras de garantizar la operatividad de las plataformas tecnológicas, así como su disponibilidad, integridad y confidencialidad, la Institución adopta los siguientes presupuestos y estrategias:

- Disposición de un sistema de red LAN / WAN que interconecta la comunidad académica a través de los equipos de cómputo y los dispositivos móviles, lo que permite acceder a la red de internet y otros servicios, para desempeñar las funciones sustantivas y administrativas de UNIMINUTO. Así mismo, se asegura que el sistema de control de acceso permite o deniegue el acceso a la Institución o a las áreas restringidas y controladas (edificio, parqueadero, sala de reuniones, data center, etc).

- Aplicación de las mejores prácticas y estándares internacionales respecto al uso e implementación de los sistemas eléctricos. Adicionalmente, la utilización de mecanismos de control, seguridad y protección, garantizan el servicio continuo y constante de los data center y centros de cableado.

- La Infraestructura donde se alojan y funcionan los sistemas de información y plataformas tecnológicas de la Institución está protegida con un sistema de aire acondicionado que mantiene la temperatura de los data center, garantizando el funcionamiento óptimo de los componentes. A su vez, la Institución protege la infraestructura de los data center a través de un sistema de control y extinción de incendios que ayuda a minimizar los riesgos que puedan por conatos de incendios.

- Aseguramiento de un sistema de control de acceso a los data center para resguardar y proteger los sistemas de información, con lo que se garantiza la seguridad, disponibilidad y gestión.

- Proporcionar a la comunidad educativa la conectividad y la infraestructura adecuada para desarrollar la operación.

- Disposición de un modelo de servicios confiable y configurable, con el que se garantice una disponibilidad, integridad y confiabilidad, basados en la experiencia ofrecida por los aliados de servicio líderes del mercado mundial.

- Empleo de plataformas de software y hardware para asegurar la red corporativa y la protección contra ataques informáticos internos y externos.

- Garantizar un monitoreo permanente de la infraestructura física y lógica de los sistemas de información y plataformas tecnológicas, con el fin de asegurar la disponibilidad y continuidad.

- Monitoreo proactivo del estado y accesos a los recursos tecnológicos, con el fin de garantizar su uso eficiente, gestionar la capacidad, asegurar el cumplimiento de los niveles de servicio y su manejo adecuado.

- Uso de herramientas tecnológicas y procedimientos que permiten el monitoreo, la detección y respuesta extendida, el control del acceso físico y la correlación y análisis de la red, donde se almacenan los dispositivos para el procesamiento, almacenamiento y conectividad a las plataformas corporativas y educativas, tanto para infraestructura en nube y onpremise.

- Mantenimiento de la infraestructura tecnológica, de acuerdo con los lineamientos de infraestructura vigentes.

- Aseguramiento de la recuperación de datos a través de los lineamientos para la gestión de copias de seguridad y aplicaciones.

- Disposición de recursos físicos, económicos y el talento humano necesarios para ejecutar las tareas de mantenimiento, renovación y actualización de la infraestructura tecnológica.

- Aseguramiento de la renovación y actualización de la infraestructura tecnológica para ejercer labores administrativas, formativas, académicas, científicas, culturales, bienestar universitario, de extensión y proyección social.

- Gestión de controles adecuados que permitan garantizar la actualización y renovación de la infraestructura tecnológica.

- Garantizar que se cuenta un protocolo definido para la recuperación de los datos, la infraestructura tecnológica y las funcionalidades ante la interrupción de un sistema provocada por un desastre, bien sea natural o provocados (disaster recovery).

- Garantizar de la infraestructura tecnológica adecuada y conforme a la realidad de las sedes de acuerdo con las condiciones de la oferta, las modalidades, las áreas de conocimiento, el número de estudiantes y otras variables, que permitan el desarrollo gradual en la adopción y apropiación de las tecnologías.

- Disponer de los mecanismos y procedimientos necesarias, que permitan el uso adecuado de los recursos tecnológicos que brinda la Institución a la comunidad educativa, velando además por el debido cuidado en el acceso a redes externas.