

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 PROTECCIÓN DE DATOS

PRESENTACIÓN DE LA POLÍTICA

Para la Corporación Universitaria Minuto de Dios – UNIMINUTO es importante garantizar el aseguramiento integral de las plataformas y la protección de los datos. Por ello, adopta la presente política de tratamiento de datos, con el fin de evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, demostrando así su compromiso y respeto por la propiedad intelectual, la responsabilidad social y ambiental, así como los derechos de la comunidad académica y de cualquier persona en general.

REFERENTES

Normatividad Externa

- a. Ley 527 de 1999 sobre la firma electrónica.
- b. Ley 1273 de 2008 Delitos informáticos y protección el bien jurídico o tutelado que es la información.
- c. Ley 1266 de 2008 Habeas data financiera y seguridad en datos personales.
- d. Ley 1341 de 2009 Tecnologías de la Información y aplicación de seguridad.
- e. Ley 1581 de 2012 para la protección de datos personales.
- f. Decreto 1330 de 2019 del Ministerio de Educación Nacional.
- g. Decreto 2364 de 2012 Firma electrónica.
- h. Decreto 1377 de 2013 protección de datos personales.
- i. Decreto 1151 de 2008 Gobierno en línea.
- j. Resolución 15224 de 2020 Ministerio de Educación Nacional.
- k. Acuerdo 02 de 2020 del Consejo Nacional de Educación Superior.

Referentes Institucionales

- a. Proyecto Educativo Institucional – PEI de UNIMINUTO
- b. Política de seguridad de la Información (Acuerdo Consejo de Servicios Tecnológicos No. 001 del 6 de abril de 2018)
- c. Política de Tratamiento de la Información (Para la protección de los datos personales, Resolución Rectoral No. 1484 del 07 de septiembre de 2018).
- d. Política de Gestión de la Información.
- e. Manual Interno de protección de datos personales, programa de gestión de datos y responsabilidad demostrada.
- f. Manual de control de accesos.
- g. Lineamiento de copias de seguridad.

FORMULACIÓN DE LA POLÍTICA

Para garantizar la debida protección y gestión de los datos en la Institución, UNIMINUTO está comprometida con el tratamiento adecuado y seguro de estos, durante su recolección y almacenamiento. Para ello, la Institución ha adoptado los siguientes presupuestos que le permiten dar cumplimiento al ordenamiento jurídico como a la normatividad institucional:

- Aplicación de controles adecuados de seguridad de la información, garantizando la privacidad de la

información desde la recolección, almacenamiento, uso, tratamiento, transferencia o eliminación, con el fin de evitar la pérdida de la integridad, la confidencialidad y la disponibilidad.

- Promoción de implementación de mecanismos para prevenir accesos no autorizados o fraudulentos que permita generar un impacto positivo en el cumplimiento del mandato legal y normatividad vigente aplicable.
- Incentivar el uso adecuado y seguro de los sistemas de información, el respeto al cumplimiento de Habeas Data velando por el derecho de todos los miembros de su comunidad educativa, así como de las personas en general.
- Adopción de la política para la seguridad de la información y la política de tratamiento de la información para la protección de los datos personales.
- Propender por el uso de buenas prácticas, medidas y controles de seguridad de los datos, estableciendo su apropiación y obligatorio cumplimiento, en concordancia con la misión y visión de UNIMINUTO.
- Implementación de controles y medidas de seguridad de forma preventiva y estratégica, que permita aplicarlos de una forma sistemática, estructurada y adaptada a los cambios que se produzcan en los procesos, el entorno y las tecnologías emergentes.
- Asignación de responsabilidades y autorizaciones a los roles indicados para garantizar el cumplimiento de las directrices establecidas, con el fin de monitorear y controlar el desempeño de la presente política.
- Determinación de estrategias para orientar la definición y actualización de lineamientos para la seguridad digital y la protección de datos.
- Garantía de la supervisión y auditoría a la gestión de la seguridad de la información y protección de datos, con el propósito de asegurar el cumplimiento de los requisitos normativos, legales y de regulación nacional e internacional.
- Compromiso en la protección de los datos frente a eventuales amenazas a los que pueden estar expuestos, mediante mecanismos y controles que permitan evitar la adulteración, la pérdida, la consulta, el uso o el acceso no autorizado.
- Disposición de mecanismos humanos, técnicos y logísticos para que se realicen y ejecuten los backups, así como las pruebas de restauración de los sistemas de información, de acuerdo con los lineamientos de copias de seguridad.
- Monitoreo constantemente a los cambios significativos de los riesgos que afecten la seguridad de los datos frente a posibles amenazas.
- Gestión de la protección de los datos con tecnologías emergentes, apoyada en los procesos, con el propósito de facilitar la mitigación y el control de los riesgos, generando un grado de confianza en las partes interesadas.
- Aplicación de mecanismos de encriptación para la transmisión de los datos y en sistemas de información que lo requieran en el almacenamiento, con el fin de garantizar la confidencialidad e integridad de los datos y minimizar los riesgos por robo, fraude o uso fraudulento.
- Desarrollo de programas enfocados a fortalecer la cultura de seguridad digital, así como incentivar la adopción y concienciación de la protección de los datos.

- Ejecución de programas para mantener actualizados al personal técnico en aspectos de ciberseguridad.
- Implementación de estrategias y procedimientos para la gestión del riesgo de amenazas. Asimismo, incorporación de planes de recuperación de desastres ante eventos o incidentes que puedan afectar la continuidad de la operación de UNIMINUTO.
- Disposición de la infraestructura tecnológica adecuada para protección y seguridad de los datos. Asimismo, adopción de medidas de monitoreo y control permanente, con el fin de identificar, detectar y priorizar incidentes o eventos que puedan afectar la seguridad de los datos.
- Garantía del ejercicio libre del derecho fundamental de habeas data en cabeza de toda su comunidad académica y cualquier persona que tenga algún vínculo con la Institución, disponiendo los medios que le permitan acceder, consultar, rectificar, modificar, actualizar, eliminar y demás derechos contenidos en la normativa aplicable a sus datos personales.
- Disponer de procedimientos y protocolos de seguridad que permitan blindar la información para el acceso a proveedores y entidades externas que tenga acceso a los datos.

Así las cosas, UNIMINUTO desarrolla estrategias y procedimientos para la gestión del riesgo de amenazas, mediante la incorporación de planes de recuperación de desastres ante eventos o incidentes que puedan afectar la continuidad de la operación de UNIMINUTO, disponiendo de la infraestructura tecnológica adecuada para protección y seguridad de los datos, y la adopción de medidas de monitoreo y control, con el fin de identificar, detectar y priorizar incidentes o eventos que puedan afectar la seguridad de los datos.