Políticas Institucionales

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

Consejo de Fundadores
18 de marzo de 2022

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PRESENTACIÓN DE LA POLÍTICA

Para la Corporación Universitaria Minuto de Dios – UNIMINUTO, es fundamental la protección de la información buscando la disminución del impacto generado por los riesgos identificados de manera sistemática, con el objeto de mantener un nivel mínimo de exposición que permita responder por la integridad, confidencialidad y disponibilidad de la información.

Entendiendo el compromiso de preservar la **Seguridad de la Información, la Ciberseguridad y la Protección de los Datos Personales** en el desarrollo de las actividades que apoyan la gestión académica y administrativa de la Institución se considera pertinente actualizar y reglamentar las principales políticas y directrices en relación con aspectos generales de la gestión y administración de la seguridad de la información.

REFERENTES

1. 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 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 Se reglamenta parcialmente la Ley 1581 de 2012.
i. Decreto 1151 de 2008 Gobierno en línea.
j. Decreto Único Reglamentario 1074 de 2015 del Ministerio de Industria y Comercio
k. Resolución 15224 de 2020 Ministerio de Educación Nacional.
l. Acuerdo 02 de 2020 del Consejo Nacional de Educación Superior.

2. Referentes Institucionales

a. Acuerdo No. 345 del 21 de septiembre de 2021 - Política de Protección de Datos.
b. Acuerdo No.345 del 21 de septiembre de 2021- Política de gestión de la información.
c. Acuerdo 01 del 2018 del Consejo General de Tecnología – (Política de Seguridad de la Información).
d. Resolución Rectoral No. 1484 del 07 de septiembre de 2018 (Política de Tratamiento de la Información - Para la protección de los datos personales).
e. Resolución Rectoral No. 1542 de 19 de noviembre de 2020 – Programa Integral de Gestión de Datos Personales.

3. Marcos de Referencia

a. Norma ISO/IEC 27000 "Estándar de seguridad de la información; provee estándares y guías sobre buenas prácticas en sistemas de gestión de seguridad de la información".
b. Norma ISO/IEC 27002 "Guía de buenas prácticas en controles de seguridad de la información".
c. Norma ISO/IEC 27005 "Directrices para la gestión del riesgo en seguridad de la información"
d. Norma ISO/IEC 22301 "Fundamentos de un sistema de gestión de continuidad de negocio
e. Norma ISO/IEC 31000 que "Brinda principios y directrices para la gestión del riesgo".
f. Norma ISO/IEC 38501 "Marcos de trabajo para el gobierno y la gestión de tecnología de la información".

FORMULACIÓN DE LA POLÍTICA

La presente Política de Seguridad de la Información está orientada por los principios y la misión de UNIMINUTO, y tiene como objetivo definir los lineamientos y controles que deben ser adoptados e implementados para garantizar que los riesgos de la Seguridad de la Información, la Ciberseguridad y la Protección de Datos Personales sean conocidos, tratados, gestionados y asumidos de una forma documentada, sistemática, estructurada, eficiente y adaptada a los cambios que se produzcan en las personas, los procesos, el entorno y las tecnologías de información de UNIMINUTO.

Se trata de una política preventiva y estratégica que permita adelantarse a cualquier situación, evento o incidente que atente contra la integridad, confidencialidad y disponibilidad de la información, así como la protección de los datos personales, en sus diferentes sedes y unidades de servicios integrados y en general, en el Sistema UNIMINUTO. Para ello, la Institución ha adoptado los siguientes compromisos que le permiten dar cumplimiento a las obligaciones legales, estatutarias, contractuales y la normatividad institucional:

1. **Organización de la seguridad de la Información**

   a. Asignar los roles, responsabilidades y funciones que permitan garantizar la gestión de la seguridad de la información y la protección de los datos personales.

   b. Garantizar un proceso de formación especializada en seguridad de la información, ciberseguridad, ciber riesgos y protección de datos personales acorde a los roles, responsabilidades y funciones que permita una eficaz implementación y desarrollo del Sistema de Gestión de la Seguridad de la Información -SGSI y el Programa Integral de Gestión de Datos Personales - PIGDP.

   c. Planificar, desarrollar y gestionar la Seguridad de la Información y la Protección de Datos Personales en la Institución.

   d. Monitorear y controlar el desempeño del Sistema de Gestión de la Seguridad de la Información alineados a las buenas prácticas, los marcos de referencia y la norma ISO 27000, de acuerdo con el "**Manual de Seguridad Digital y Protección de Datos Personales**".

   e. Liderar las decisiones estratégicas en cuanto a los objetivos relacionados con la seguridad de la información y efectuar seguimiento a la efectividad de los controles y mecanismos que aseguren el cumplimiento de la gestión de seguridad de la información.

   f. Fomentar la participación y adopción de la Seguridad Digital y Protección de Datos Personales en la comunidad educativa, así como las partes interesadas que tengan un vínculo con la Institución.

   g. Establece mecanismos y protocolos de relacionamiento con autoridades de seguridad del Estado, entidades u organismos nacionales e internacionales que coordinen aspectos de ciberseguridad, ciberdefensa, ciber riesgos con el fin asegurar que la Institución se mantenga actualizada en aspectos relacionados con la Seguridad Digital.

2. **Seguridad digital para la gestión del talento humano**

   a. Establecer los mecanismos necesarios para que los colaboradores y contratistas comprendan y cumplan sus responsabilidades de acuerdo con los roles y accesos asignados a los sistemas de información y plataformas tecnológicas.

b. Asegurar que en los contratos de los colaboradores se incluya la inclusión de las cláusulas de confidencialidad, no divulgación de la información y tratamiento de datos personales, así como la obligatoriedad del cumplimiento de los controles de seguridad, las políticas y procedimientos aún después de finalizada la relación contractual.

c. Garantizar que los colaboradores desarrollen una ruta de aprendizaje y competencias que permitan comprender la importancia de proteger la información y Datos Personales de posibles riesgos en los entornos físicos y digitales.

d. Generar modelos basados en datos que permitan medir el grado de respuesta en la Comunidad Educativa para detectar eventos o incidentes de ciberseguridad.

3. Gestión de los activos de información

a) Aplicar los mecanismos, los procedimientos y los controles que permitan la gestión del inventario, la clasificación, la responsabilidad, la propiedad y la custodia de los activos de información de la Institución.

b) Gestionar el inventario de los activos de información desde las sedes y las Unidades de Servicios Integrados del Sistema UNIMINUTO.

c) Clasificar y etiquetar los activos de información en términos de la valoración, el nivel de criticidad, la confidencialidad y los requisitos legales.

4. Control de Accesos Digital

a. Asegurar los mecanismos y los controles para la gestión de acceso adecuado a las plataformas tecnológicas mediante la implementación de procesos que incluyan el ciclo de vida del control de acceso para los usuarios, desde la vinculación, hasta el retiro de la Institución de acuerdo con el "**Manual de Control de Acceso Digital**".

b. Definir y actualizar las matrices de roles y perfiles para el acceso a la plataforma tecnológica de acuerdo con las necesidades de UNIMINUTO.

c. Las credenciales (claves de acceso), códigos de acceso, tarjetas inteligentes, dispositivos de autenticación, llaves para protección de software, combinaciones de cajas fuertes o cualquier otro activo de información, son personales e intransferibles; su uso, administración y reserva es responsabilidad de cada usuario.

5. Gestión de la seguridad física y del entorno

a. Aplicar los controles y las restricciones de acceso físico pertinentes, con el fin de evitar los accesos no autorizados y mantener la seguridad sobre las instalaciones, los activos de información y las personas.

b. Aplicar los mecanismos y controles de acceso físico para evitar el daño, la pérdida o el robo de los activos de información y tecnológicos de la Institución.

c. Implementar las medidas para el control del ingreso y el retiro los activos de información de las instalaciones de la Institución.

d. Implementar mecanismos de control de acceso para las áreas seguras; tales como cámaras, puertas de seguridad, sistemas de control con lectores biométricos, sistema de alarmas, llaves, entre otras, de acuerdo con los procedimientos establecidos por UNIMINUTO.

6. **Gestión de la seguridad de las operaciones**

   a. Garantizar el aseguramiento en la plataforma tecnológica con mecanismos de ciberseguridad para evitar la materialización en riesgos de fraude y actividad ilícita.

   b. el uso exclusivo de las herramientas de colaboración y productividad para la ejecución del rol y funciones.

   c. Planificar, implementar y controlar de manera eficiente los cambios de tecnología, asegurando la continuidad y minimizando el impacto por la interrupción de los servicios soportados por la infraestructura tecnológica en la Institución.

   d. Garantizar que la información Institucional esté protegida contra la pérdida o destrucción de los datos, asegurando que periódicamente se realicen copias de seguridad.

   e. Hacer uso de la plataforma de colaboración y productividad como medio principal de almacenamiento de la información para el cumplimiento de sus funciones.

   f. Garantizar mecanismos y protocolos que permitan establecer un plan de seguimiento y control en el uso de los recursos, almacenamiento, procesamiento y proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido en la plataforma tecnológica de la Institución.

   g. Implementar herramientas emergentes que permitan proteger los sistemas de información, aplicaciones e infraestructura tecnológicas de ataques de ciberseguridad y códigos maliciosos.

   h. Definir los protocolos, los lineamientos, las herramientas emergentes o servicios necesarios para identificar las vulnerabilidades técnicas de los sistemas de información, aplicaciones e infraestructura tecnológicas.

   i. Ejecutar pruebas de Ethical hacking, ejercicios de intrusión y análisis de vulnerabilidades para identificar las brechas de ciberseguridad y generar plan de acción para fortalecer la seguridad digital en las plataformas tecnológicas.

   j. Monitorear la plataforma tecnológica con el fin de correlacionar los eventos, detectar vulnerabilidades y análisis de la ciberseguridad, que permita evaluar el estado de los ciber riesgos y generar estrategias para minimizar el impacto en la operación.

7. **Seguridad de las Comunicaciones**

   a. Establecer los estándares, las herramientas y los procedimientos para la administración, control y optimización de los servicios de conectividad.

   b. Proteger mediante mecanismos de cifrado la información sensible o confidencial que se transfiera a nivel interno y externo con la Institución.

8. **Adquisición, desarrollo, mantenimiento y retiro de sistemas de información, aplicaciones e Infraestructura tecnológica**

   a. Definir los procedimientos y los mecanismos que permitan asegurar la inclusión de requisitos y controles de seguridad digital, durante el ciclo de vida (adquisición, desarrollo, mantenimiento y retiro) de los sistemas de información, aplicaciones e infraestructura tecnológicas.

9. Relaciones con los proveedores y contratistas

a. Establecer y acordar cláusulas contractuales en seguridad de la información, confidencialidad y protección de datos personales con los proveedores y contratistas que acceden a las plataformas tecnológicas de la Institución.

b. Evaluar el cumplimiento de la seguridad de la información de los servicios de tecnología contratados con los proveedores.

10. Gestión de Incidentes de la Seguridad de la Información

a. Definir y establecer el procedimiento para el análisis, evaluación, relación de evidencias, tratamiento y reporte de los incidentes relacionados con la seguridad y privacidad de la información, datos personales y ciberseguridad con el fin de mitigar el riesgo asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información de UNIMINUTO.

b. Reportar los eventos e incidentes de seguridad de la información, protección de datos y ciberseguridad que comprometan la continuidad de la operación por amenazas, como: uso, divulgación, modificación o destrucción no autorizada de información y datos personales; un impedimento en la operación normal de las redes, sistemas de información o recursos informáticos; o una violación a la presente Política de Seguridad de la Información, la Política de Tratamiento de la Información y las disposiciones del Manual de Seguridad Digital.

11. Gestión de continuidad y disponibilidad tecnológica

a. Garantizar la gestión de la continuidad de los servicios tecnológicos a través de un plan de recuperación ante desastres, que permita asegurar que las plataformas tecnológicas críticas estén disponibles para el Sistema UNIMINUTO en caso de presentarse una interrupción en la operación.

b. Implementar controles y herramientas necesarias para asegurar que los recursos que componen las plataformas tecnológicas sean periódicamente respaldados, monitoreados y proyectados para futuros requerimientos de capacidad en procesamiento, almacenamiento y concurrencia.

12. Privacidad y Protección de Datos Personales

a. UNIMINUTO está comprometida con el respeto del derecho de Habeas data en cabeza de sus estudiantes, colaboradores y cualquier persona en general. En virtud de lo anterior, adoptó la Política de Tratamiento de Información, la cual es de obligatoria aplicación en todas las actividades y procedimientos que involucre el tratamiento de datos personales. Esta política es de estricto cumplimiento por parte de todos los colaboradores, contratistas y terceros que tengan vínculo con UNIMINUTO.

b. El incumplimiento de la Política de Tratamiento de Información acarreará las investigaciones disciplinarias correspondientes de conformidad con lo establecido en la normativa interna y el ordenamiento jurídico aplicable.

13. Cumplimiento de requisitos legales y contractuales

a. Gestionar los procesos y controles para dar cumplimiento a normatividad tanto externa como interna de la Institución, así como también lo establecido en acuerdos contractuales, en lo relacionado con aspectos de seguridad de la información, ciberseguridad y protección de datos personales.

14. Revisiones de Seguridad de la Información y Protección Datos Personales

a. Auditar a intervalos planificados o cuando ocurran cambios significativos tanto de regulación normativa de ley, procedimientos o procesos referentes en seguridad de la información y el cumplimiento a la protección de datos personales.

b. Realizar periódicamente auditoría de seguimiento a la plataforma tecnológicas para determinar el cumplimiento de las políticas y normatividad en seguridad de la información y protección de datos personales.

15. Divulgación, cultura y adopción de Seguridad Digital y Protección de Datos Personales

a. Definir los procedimientos, los controles y los mecanismos necesarios, para garantizar que la comunidad educativa y las partes interesadas conozcan y den cumplimiento a la presente política, así como de los documentos que la integran.

b. Articular las estrategias encaminadas a desarrollar competencias digitales en aspectos de seguridad mediante un ***Programa Integral de Adopción y Apropiación de Tecnología*** que integre las Rectorías, las Sedes, las Unidades Académicas, las Unidades Administrativas y en general a la Comunidad Educativa de UNIMINUTO y sus grupos de interés.

c. Implementar y mantener, como parte del desarrollo del modelo de gestión de seguridad de la información y protección de datos personales, el programa, los planes de cultura y adopción y socialización en la Institución, de manera que se minimice la probabilidad y el impacto de incidentes de seguridad de la información y protección de datos personales.

16. Deberes y sanciones

a. Cualquier persona que tenga vínculo con la Institución, estará obligado a conocer y cumplir la presente política y demás disposiciones institucionales que la desarrollen y que se encuentren publicados en la página web Institucional.

b. Cuando se identifique el incumplimiento de la presente política por parte de un colaborador, se pondrá en conocimiento a la Dirección de Talento Humano para los efectos de su competencia y atribuciones.