UNIMINUTO
Corporación Universitaria Minuto de Dios

CONSEJO GENERAL DE TECNOLOGÍA
ACUERDO No. 001
06 de abril de 2018

POR EL CUAL SE SEÑALA LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA CORPORACIÓN UNIVERSITARIA MINUTO DE DIOS - UNIMINUTO

El Consejo General de Tecnología de la Corporación Universitaria Minuto de Dios - UNIMINUTO, en uso de sus atribuciones estatutarias y reglamentarias, en especial las consagradas en el numeral primero del artículo 44 del Reglamento Orgánico y,

CONSIDERANDO

Que en virtud de lo dispuesto en el numeral primero del artículo 44 del Reglamento Orgánico es función del Consejo General de Tecnología el *"Apoyo en definición y actualización de las políticas generales del área"*.

Que para la Corporación Universitaria Minuto de Dios – UNIMINUTO es importante garantizar el uso eficaz, seguro y racional de la información, por lo que se hace necesario regular su empleo atendiendo las disposiciones legales y reglamentarias previstas para el efecto, en especial las contenidas en la 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"*, y la Norma ISO/IEC 31000 que *"Brinda principios y directrices para la gestión del riesgo"*.

Que para la Corporación Universitaria Minutos de Dios – UNIMINUTO, es fundamental la protección de la información buscando la disminución del impacto generado por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y disponibilidad de la información, acorde con las necesidades del sistema.

Que UNIMINUTO dispone de tecnologías para el procesamiento, transferencia y almacenamiento de la información, de recursos humanos que hacen uso de la misma, de sitios físicos donde se aloja información, de transferencia de información entre colaboradores y entidades externas.

Que el uso adecuado y seguro de la información y de los datos con que cuenta UNIMINUTO, demuestra la integridad, confidencialidad y disponibilidad de la información, generando un impacto positivo en el cumplimiento normativo, así como en la operación normal de la Institución.

Que la estrategia de la Seguridad de la Información es definida por el Consejo General de Tecnología, asimismo, la metodología y los criterios de evaluación de riesgos de la seguridad de la información, para garantizar el correcto tratamiento de los mismos.

Calle 81B No. 72B - 70 Línea de Atención al Cliente: 593 3004 Línea Nacional: 01 8000 936670 Fax: 430 8140
Bogotá D.C. • Colombia www.uniminuto.edu

Que la Corporación Universitaria Minuto de Dios - UNIMINUTO, entendiendo el compromiso de preservar la seguridad de la información en el desarrollo de las actividades que apoyan la gestión académico - administrativa de la Institución, considera la importancia de reglamentar las principales políticas y directrices en relación con aspectos generales de la gestión y administración de la seguridad de la información mediante la implementación de un Sistema de Gestión de Seguridad de la Información, buscando establecer su apropiación, cumplimiento y concienciación en concordancia con la misión y visión de UNIMINUTO.

Que para la Corporación Universitaria Minutos de Dios - UNIMINUTO, la información y los datos son un activo esencial, el cual permite apoyar el desarrollo de las funciones sustantivas de la Institución.

Que, en virtud de lo anterior, el Consejo General de Tecnología de la Corporación Universitaria Minuto de Dios - UNIMINUTO,

ACUERDA

ARTÍCULO PRIMERO: Señalar la Política de Seguridad de la Información de la Corporación Universitaria Minuto de Dios – UNIMINUTO, la cual consta del siguiente contenido:

1. **Términos y definiciones**

   Para efectos de dar cumplimiento al presente acuerdo, se tomarán las definiciones estipuladas en los glosarios de las normas ISO 27001 – 22301 – 31000 – 20000, así como también los siguientes términos:

   a) **Activo de Información**: Es todo aquello que UNIMINUTO considera importante o de alta validez en cuanto a la información o elemento relacionado con el tratamiento de la misma, infraestructura, sistemas de información, herramientas informáticas, bases de datos, archivos, entre otros.
   b) **Análisis de Riesgo:** Uso sistemático de la información para identificar fuentes y tratamiento del riesgo.
   c) **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
   d) **Dato sensible**: Información que afecta la intimidad de la persona o cuyo uso indebido puede generar su discriminación; tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos (huellas dactilares, entre otros).
   e) **Disponibilidad**: Característica, cualidad o condición de la información que permite encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos

Calle 81B No. 72B - 70 Línea de Atención al Cliente: 593 3004 Línea Nacional: 01 8000 936670 Fax: 430 8140
Bogotá D.C. • Colombia www.uniminuto.edu

o aplicaciones, garantizando el acceso a la misma y a los sistemas por personas autorizadas en el momento que se defina o así lo requieran.

f) **Evento de Seguridad de la Información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
g) **Integridad:** Propiedad que busca mantener los datos libres de modificaciones no autorizadas para mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
h) **Manual de Seguridad de la Información**: Es el documento rector que materializa las políticas de seguridad de la información, estas se encuentran enfocadas al cumplimiento de la normatividad legal vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001.
i) **Plataforma Tecnológica:** Sistema base de integración de infraestructura de tecnología de la información, sistemas de información, sistemas de comunicaciones unificadas, sistemas de telecomunicaciones, redes de datos y herramientas informáticas definidas por UNIMINUTO para la prestación de servicios tecnológicos.
j) **Riesgo**: Un posible evento que podría causar daño o pérdidas, o afectar la habilidad de alcanzar objetivos, asociado al impacto y probabilidad de ocurrencia.
k) **Servicio Tecnológico**: Es un medio para entregar valor a los usuarios, basándose en el uso de las tecnologías de la información para soportar los procesos de la Institución.
l) **Sistema de Información**: Conjunto de componentes de hardware y software interrelacionados que permiten registrar, procesar, almacenar, distribuir y consultar información, para apoyar al ambiente productivo y la toma de decisiones estratégicas de UNIMINUTO.
m) **Tratamiento del Riesgo:** Proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.
n) **Usuario**: Persona vinculada a la Corporación Universitaria Minuto de Dios - UNIMINUTO a la cual se le concede el acceso para el uso de la plataforma tecnológica de UNIMINUTO.

2. Introducción.

La presente Política de Seguridad de la Información está orientada por los principios y la misión de UNIMINUTO. 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 sean conocidos, tratados, gestionados y asumidos de una forma documentada, sistemática, estructurada, eficiente y adaptada a los cambios que se produzcan en 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, en sus diferentes sedes y unidades de servicios integrados y en general, en el Sistema UNIMINUTO.

Para UNIMINUTO la promulgación de la presente política de seguridad de la información, se define como un proceso que le permite a la comunidad educativa percibir un estado de confianza para el desarrollo de las actividades dentro de las áreas y su entorno, mediante la materialización de las estrategias definidas en planes de acción y la adopción de una serie de controles y disposiciones para reconocer la existencia de riesgos, identificarlos, establecer el plan de tratamiento y determinar el nivel de aceptación que está dispuesto asumir UNIMINUTO.

3. Acerca de la Gestión de Riesgos

La Gerencia de Servicios Tecnológicos en coordinación con la Gerencia de Tendencias y Riesgos de UNIMINUTO definirá e implementará la adopción de una metodología para el control y gestión de los riesgos tecnológicos que permita:

- Centrarse en los aspectos operacionales.
- Valorar desde el primer momento el nivel de aceptación del riesgo.
- Llevar a cabo el seguimiento de los aspectos críticos de la Institución y medir los riesgos.
- Desarrollar acciones preventivas para responder y recuperarse ante cualquier circunstancia de materialización del riesgo.

4. Alcance de la Política de Seguridad de la Información.

El alcance de la presente política se aplica a nivel Sistema UNIMINUTO, abarcando la comunidad educativa que participa en el desarrollo de las diferentes funciones sustantivas de la Institución, tales como estudiantes, profesores, colaboradores, egresados, terceros, y en general a toda persona, cualquiera que sea su vínculo con la Institución.

Estas disposiciones también involucran a contratistas, consultores y demás colaboradores, que laboran en las instalaciones de UNIMINUTO y que utilicen tecnologías de información y de comunicaciones propiedad de la Institución. Asimismo, estas disposiciones aplican a todos los equipos tecnológicos propios o arrendados que tiene UNIMINUTO.

5. Objetivos de la Política de Seguridad de la Información

Se establecen los siguientes objetivos rectores que permiten contribuir a cumplir y desarrollar los objetivos de la Política de Seguridad de la Información de UNIMINUTO:

a) Fomentar una cultura de seguridad de la información en el Sistema UNIMINUTO para asegurar su apropiación y cumplimiento.

Calle 81B No. 72B - 70 Línea de Atención al Cliente: 593 3004 Línea Nacional: 01 8000 936670 Fax: 430 8140
Bogotá D.C. • Colombia www.uniminuto.edu

b) Adoptar y gestionar un Manual de Seguridad de la Información que incorpore buenas prácticas y normas al cumplimiento de lineamientos y controles definidos para la seguridad de la información en UNIMINUTO.
c) Gestionar los riesgos de la seguridad de la información que permita identificarlos, evaluarlos, valorarlos y tratarlos de manera que se minimice su impacto en la operación de los procesos de la institución.
d) Asegurar que la estrategia de recuperación y restauración de los servicios tecnológicos y sistemas de información críticos esté alineada a la estrategia de continuidad de la operación de UNIMINUTO.
e) Controlar y supervisar los procesos de tecnología para identificar brechas de seguridad, optimizar los servicios tecnológicos y apoyar el cumplimiento de la normatividad.

6. Roles y responsabilidades para la Seguridad de la Información

Con el fin de monitorear y controlar el desempeño del Sistema de Gestión de la Seguridad de la Información y de acuerdo con lo establecido en la norma ISO 27001, se asignan los siguientes roles, responsabilidades y autoridades para garantizar la seguridad de la información y datos personales:

6.1. Comité de Seguridad de la Información

El Comité de Seguridad de la Información velará por la implementación y desarrollo de las políticas de gestión y directrices de seguridad de la información y protección de datos personales, con las siguientes funciones:

a) Coordinar la implementación del plan maestro y modelo de la seguridad de la información y datos personales.
b) Definir, aprobar y promoverla implementación, desarrollo y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información y el Programa Integral de Gestión de Datos Personales.
c) Definir y promover la cultura de la seguridad de la información y datos personales a todas las partes interesadas en el Sistema UNIMINUTO.
d) Evaluar y analizar los informes periódicos sobre el estado de la seguridad de la información y datos personales, asimismo definir los planes de acción para mitigar y/o eliminar los riesgos asociados a la información y datos personales.
e) Evaluar, definir y promover propuestas de implementación de seguridad de la información y datos personales.
f) Gestionar y tratar los incidentes críticos de seguridad de la información y datos personales.
g) Aprobar el Manual de Seguridad de la Información, la Política de Tratamiento de Información y Programa Integral de Gestión de Datos Personales. Asimismo, las actualizaciones que surjan como mejoramiento a la seguridad de la información y datos personales.

6.2. Director de Seguridad de la Información

Es el rol responsable de planificar, desarrollar y gestionar la seguridad de la información y datos personales con las siguientes funciones:

a) Cumplir la función de ***Oficial de Cumplimiento de Seguridad de la Información y Protección de Datos Personales***,
b) Dar trámite a las solicitudes de los titulares de los datos personales, para el ejercicio de los derechos de protección de datos personales y la normatividad que la regula.
c) Gestionar el Programa Integral de Gestión de datos personales.
d) Coordinar la implementación de los controles del Programa Integral de Gestión de Datos personales.
e) Gestionar la implementación efectiva de las políticas y procedimientos adoptados para cumplir las normas, así como la implementación de buenas prácticas y controles para la gestión de la información y datos personales definidos en la Institución.
f) Gestionar los incidentes de seguridad y/o el monitoreo continuo de las acciones correctivas.
g) Revisar, evaluar y mantener actualizado periódicamente el Manual de Seguridad de la Información y sugerir al Comité de Seguridad de la Información los cambios necesarios para mejoramiento del mismo.
h) Gestionar la implementación del programa de concientización en seguridad de la información y datos personales para el Sistema UNIMINUTO.
i) Gestionar las pruebas de seguridad para evaluar la arquitectura de seguridad y detectar posibles debilidades y amenazas. Asimismo, generar los planes de acción para mitigar los riesgos asociados a la seguridad de la información y datos personales.
j) Trabajar en coordinación con la Gerencia de Tendencias y Riesgos el tratamiento de los riesgos de la seguridad de la información y datos personales.
k) Realizar el monitoreo y control al Sistema de Gestión de Seguridad de la Información y Programa Integral de Gestión de Datos Personales.
l) Mantener actualizados los lineamientos, estándares, procedimientos y toda la documentación necesaria para el cumplimiento de la política de seguridad de la información y la Política de tratamiento de la Información.
m) Registrar las bases de datos personales de la Institución en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la Superintendencia de Industria y Comercio - SIC.
n) Acompañar y asistir a la Institución en la atención de visitas y los requerimientos que realice la SIC y obtener las declaraciones de conformidad de la SIC cuando sea requerido.
o) Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de las políticas de seguridad de la información y tratamiento de la información personal.

p) Definir e implementar un Plan de Recuperación de Desastres que permita responder a la continuidad y disponibilidad de los datos personales y servicios tecnológicos.
q) Dar a conocer las políticas de Seguridad de la Información y el Manual de Seguridad de la Información a los diferentes usuarios de la Institución.

6.3. Administrador de los Sistemas de Seguridad Informática

Es el rol encargado de la gestión y administración de las herramientas informáticas relacionadas con la seguridad de la información. Cumplirá las siguientes funciones principales:

a) Coordinar el tratamiento de los incidentes de seguridad de la información y datos personales en los niveles que corresponda.
b) Gestionar las solicitudes relacionadas con los incidentes de seguridad; y escalara los niveles de soporte y resolución correspondientes.
c) Generar el informe de historial de registro de eventos de seguridad con las recomendaciones necesarias.
d) Aplicar los controles y lineamientos definidos en el Manual de Seguridad de la Información.
e) Presentar informes y recomendaciones de seguridad de la información y datos personales.

6.4. Administrador del Sistema de Gestión de Seguridad de la Información

Es el rol encargado de la administración y el mantenimiento del Sistema de Gestión de Seguridad de la Información, con las siguientes funciones principales:

a) Mantener actualizadas la documentación y Manual de Seguridad de la Información para el cumplimiento del Sistema de Gestión de Seguridad de la Información.
b) Validar y proponer al Comité de Seguridad de la Información una metodología para la identificación, valoración, clasificación y tratamiento de los riesgos a los activos de información.
c) Validar la implementación y operación del Sistema de Gestión de Seguridad de la Información.
d) Validar el diseño y definición de los procedimientos y controles para detectar y dar respuesta oportuna a los incidentes de seguridad.
e) Definir y aplicar los procedimientos de seguimiento y revisión del Sistema de Gestión de Seguridad de la Información.
f) Coordinar la realización de análisis e investigaciones sobre los incidentes de seguridad de la información.
g) Realizar el monitoreo y control de la aplicación de los lineamientos definidos en el Manual de Seguridad de la Información.

6.5. Administrador del Programa Integral de Protección de Datos Personales

Es el rol encargado de la administración y el mantenimiento del Programa Integral de Protección de Datos Personales en coordinación con el Oficial de cumplimiento de Seguridad y Protección de Datos Personales, con las siguientes funciones principales:

a) Apoyar al Oficial de cumplimiento de Seguridad y Protección de Datos Personales, en la definición y desarrollo del Programa Integral de Gestión de datos personales.
b) Coordinar la implementación de los controles del Programa Integral de Gestión de Datos personales.
c) Apoyar al Oficial de Cumplimiento de Seguridad y Protección de Datos Personales en la coordinación con las demás áreas de la Institución para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.
d) Participar en el desarrollo de la apropiación y cultura de la protección de datos personales.
e) Medir la participación, y calificar el desempeño, en las capacitaciones de protección de datos personales.
f) Apoyar con la actualización del inventario de las bases de datos personales.
g) Apoyar en el análisis de las responsabilidades de cada cargo de la organización y proponer un diseño de programa de capacitación en protección de datos personales específico para cada uno de ellos.
h) Gestionar, realizar análisis e investigaciones de los incidentes de seguridad de datos personales con los responsables encargados del tratamiento de las bases de datos personalesy presentar al Oficial de Cumplimiento de Seguridad y Protección de Datos, las recomendaciones y acciones que surjan de este proceso.

6.6. Usuarios

Sus responsabilidades con respecto a la seguridad de la información son las siguientes:

a) Conocer y cumplir las políticas de Seguridad de la Información y el Manual de Seguridad de la Información.
b) Informar los incidentes de seguridad que atenten con la confidencialidad, integridad o disponibilidad de la información y datos personales o incumplimiento a la política de seguridad.
c) Participar y apropiar los programas de sensibilización y cultura de seguridad de la información y datos personales.

7. Gestión de Incidentes de la Seguridad de la Información.

Para la Corporación Universitaria Minuto de Dios - UNIMINUTO un incidente de seguridad de la información se define como un único o una serie de eventos de seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa

Calle 81B No. 72B - 70 Línea de Atención al Cliente: 593 3004 Línea Nacional: 01 8000 936670 Fax: 430 8140
Bogotá D.C. • Colombia www.uniminuto.edu

de comprometer la operación y de amenazar la seguridad de la información de UNIMINUTO. Asimismo, aquellos eventos que puede involucrar un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; 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. En razón a lo anterior, la Gerencia de Servicios Tecnológicos de UNIMINUTO garantizará que se defina y se establezca el procedimiento para el reporte, evaluación y tratamiento adecuado de los incidentes de seguridad.

8. Gestión de Activos de Información

Todas las sedes y las Unidades de Servicios Integrados del Sistema UNIMINUTO deben elaborar y mantener actualizado un inventario donde se identifiquen los activos de información y el responsable de los mismos.

9. Gestión de Accesos

Para UNIMINUTO es importante mantener controlado el acceso de los usuarios a la información alojada en los sistemas de información, medios físicos, digitales, aplicaciones y áreas críticas de información. Debido a que la información puede ser sensible o tener un carácter confidencial, se deben establecer los controles generales para garantizar el acceso adecuado a los activos de tecnología y de la información. Asimismo, contar con controles y restricción de acceso a las instalaciones donde dicha información se encuentra almacenada. Se establecen los siguientes lineamientos de control de acceso:

a) El responsable y/o líder funcional asignado a cada sistema de información, definirá y actualizará la matriz de clasificación de roles y perfiles para el acceso a los mismos de acuerdo con las necesidades de UNIMINUTO.

b) Las contraseñas (claves), 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 será responsabilidad de cada usuario.

10. Gestión de Cambios

Para UNIMINUTO es fundamental contar con servicios tecnológicos seguros, estables, fiables y disponibles, por lo que es importante gestionar y minimizar los riesgos cuando se requiera realizar cambios a la plataforma tecnológica de la Institución.

La Gerencia de Servicios Tecnológicos definirá un procedimiento para la gestión de cambios a la plataforma y los servicios tecnológicos, que incorpore al menos los siguientes lineamientos:

a) Todos los cambios propuestos serán evaluados por sus beneficios, riesgos e impacto sobre la plataforma y los servicios tecnológicos.

Calle 81B No. 72B - 70 Línea de Atención al Cliente: 593 3004 Línea Nacional: 01 8000 936670 Fax: 430 8140
Bogotá D.C. • Colombia www.uniminuto.edu

b) Dar prioridad a los cambios de manera que los recursos que se asignan para el cambio produzcan el mayor beneficio en función de las necesidades de la Institución.
c) Asegurar que todos los cambios propuestos tengan planes de pruebas y rollback, asimismo que cada despliegue incluya un plan de respaldo para restaurar al estado anterior en el caso de que la implementación falle.
d) Asegurar que el sistema de gestión de la configuración se actualiza para reflejar el efecto de cualquier cambio.

11. Gestión de Continuidad y Disponibilidad

Con el fin de garantizar la continuidad de los servicios tecnológicos se debe contar con un Plan de Continuidad y Disponibilidad, que permita asegurar que los servicios tecnológicos críticos estén disponibles para el Sistema UNIMINUTO, en caso de presentarse una interrupción. Para ello se deben contemplar los siguientes aspectos:

a) 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.
b) Definir e implementar el plan de recuperación de desastres.
c) Minimizar el tiempo de interrupción tras cualquier incidencia, mejorando el tiempo de recuperación.

12. Seguridad de la Información en el Recurso Humano

El recurso humano es el activo más importante para UNIMINUTO, por lo que se hace necesario que los estudiantes, profesores, colaboradores, y demás miembros de la comunidad educativa, comprendan sus derechos y responsabilidades frente al cumplimiento de la Política de Seguridad de la Información. La Gerencia de Servicios Tecnológicos en articulación con la Gerencia de Gestión Humana, definirán un Plan de Socialización de la Seguridad de la Información con los siguientes lineamientos:

a) Acuerdos contractuales con empleados y contratistas sus responsabilidades y las de UNIMINUTO, en cuanto a la seguridad de la información.
b) Contratos con cláusulas de confidencialidad y no divulgación de la información, así como la obligatoriedad del cumplimiento de las políticas, procedimientos, restricciones y controles de seguridad de la información, aún después de terminada la relación contractual.
c) Comunicaciones a los líderes de los sistemas de información, la desvinculación del colaborador o contratista y/o el cambio de rol dentro de UNIMINUTO, con el fin que realicen los ajustes de acceso a los servicios tecnológicos.

Calle 81B No. 72B - 70 Línea de Atención al Cliente: 593 3004 Línea Nacional: 01 8000 936670 Fax: 430 8140
Bogotá D.C. • Colombia www.uniminuto.edu

13. Respaldo de la Información

Para UNIMINUTO es importante garantizar que la información institucional esté protegida contra la pérdida o destrucción de los datos, asegurando que periódicamente se realicen copias de respaldo, se almacenen y se custodien en ambientes seguros. Asimismo, se realicen pruebas de restauración, con el fin de minimizar el impacto en el restablecimiento de los servicios tecnológicos, en caso de ocurrencia de un desastre o degradación de los servicios tecnológicos y sistemas de información. La Gerencia de Servicios Tecnológicos definirá e implementará el procedimiento para asegurar las copias de respaldo de los sistemas de información y aplicativos, considerando los siguientes lineamientos:

a) Los medios de las copias de seguridad se almacenarán localmente y en un sitio de custodia externa, garantizando en ambos casos la presencia de mecanismos de protección ambiental y mecanismos de control de acceso físico.
b) Definición e implementación los lineamientos de responsabilidad, almacenamiento y respaldo de la información institucional de los colaboradores.

14. Privacidad y Protección de Datos Personales

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 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 obren en nombre de UNIMINUTO.

El incumplimiento de la misma acarreará las sanciones correspondientes de conformidad con lo establecido en el ordenamiento jurídico vigente.

15. Cumplimiento de Requisitos Legales y Contractuales

Todas las áreas de UNIMINUTO acorde a sus responsabilidades, deben 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 tecnología y seguridad de la información, considerando como mínimo los siguientes controles:

a) Identificación de la legislación aplicable y de los requisitos contractuales.
b) Cumplimiento al Reglamento de Propiedad Intelectual de UNIMINUTO.
c) Cumplimiento Política de Tratamiento de Seguridad de la información de UNIMINUTO, en especial lo relacionado con el uso de software instalado en la Institución.
d) Cumplimiento de la Política de Tratamiento de Información de UNIMINUTO.

Calle 81B No. 72B - 70 Línea de Atención al Cliente: 593 3004 Línea Nacional: 01 8000 936670 Fax: 430 8140
Bogotá D.C. • Colombia www.uniminuto.edu

e) Reglamentación de controles criptográficos.

16. Divulgación, Socialización y Capacitación

UNIMINUTO a través de la Gerencia de Gestión Humana, en coordinación con la Dirección de Mercadeo y Comunicaciones y la Gerencia de Servicios Tecnológicos, definirá los procesos, procedimientos, controles y demás mecanismos necesarios, para la divulgación, socialización y capacitación del presente documento, considerando como mínimo las siguientes directrices:

a) Velar para que en el proceso de inducción de un nuevo colaborador se dé a conocer la presente política, así como de los documentos que la integran
b) Realizar todos los ajustes de tipo contractual y reglamentario para que, en los documentos jurídicos se incorpore el cumplimiento de la presente política.
c) UNIMINUTO debe implementar y mantener, como parte del desarrollo de su modelo de gestión de seguridad de la información, programas, planes de capacitación, entrenamiento y socialización en toda la institución, de manera que se minimice la ocurrencia y el impacto de incidentes de seguridad de la información.

17. Deberes y Sanciones

El personal vinculado a la Corporación Universitaria Minuto de Dios - UNIMINUTO mediante contrato laboral, de prestación de servicios o actividad docente en cualquiera de sus modalidades, estará obligado a conocer las siguientes disposiciones y el desarrollo de la normatividad publicada en los medios oficialmente establecidos por la Institución.

El no cumplimiento de las disposiciones o deberes establecidos en el presente documento o el incurrir en alguna de las prohibiciones que estipulan las leyes y el Reglamento Interno de Trabajo de UNIMINUTO.

Cuando se identifique el incumplimiento de las políticas contenidas en este documento por parte de un colaborador, se remitirá el reporte pertinente a la Gerencia de Gestión Humana para los efectos de su competencia y atribuciones.

ARTÍCULO SEGUNDO. Recomendar al Gerente de Servicios Tecnológicos que en virtud de lo dispuesto en el literal i) del artículo 36 del Reglamento Orgánico, proponga ante la Rectoría General para que mediante resolución rectoral se realice la constitución del Comité de Seguridad de la Información, así como también los roles y responsabilidades que permitan dar cumplimiento a lo dispuesto en el presente acuerdo, y las adicionales que considere pertinentes.

Calle 81B No. 72B - 70 Línea de Atención al Cliente: 593 3004 Línea Nacional: 01 8000 936670 Fax: 430 8140
Bogotá D.C. • Colombia www.uniminuto.edu

ARTÍCULO TERCERO. El presente Acuerdo rige a partir de la fecha de su expedición.

Comuníquese y Cúmplase, dado en Bogotá D.C, el día 06 de abril de 2018.

DR. HUGO VALDERRAMA
Presidente Consejo General de Tecnología

PADRE HAROLD CASTILLA DEVOZ
Rector General

ING. SAUL ANTONIO REYES ARIAS
Secretario

Proyectó: Ing. Ricardo Ramírez - Director de Seguridad de la Información

Revisó: Dirección Jurídica.

Calle 81B No. 72B - 70 Línea de Atención al Cliente: 593 3004 Línea Nacional: 01 8000 936670 Fax: 430 8140
Bogotá D.C. • Colombia www.uniminuto.edu