VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1	feb-2022	Versión inicial del documento

En cumplimiento a lo dispuesto en la Ley estatutaria 1341 de 2009 y a su Decreto Reglamentario 1078 de 2015, El COLEGIO MONTESSORI SAS, informa la política aplicable a la entidad para la seguridad y privacidad de la información.

I.IDENTIFICACION

NOMBRE DE LA INSTITUCIÓN: COLEGIO MONTESSORI SAS

DIRECCION: Manga, avenida Jiménez Calle 26 18-86

CORREO ELECTRÓNICO: protecciondedatos@montessoricartagena.edu.co

TELEFÓNO DEL RESPONSABLE: 3106203025

LEGISLACIÓN APLICABLE Y ÁMBITO DE APLICACIÓN

La presente se aplica a la política general de seguridad y privacidad de la información recolectados por El COLEGIO MONTESSORI SAS y se ha redactado teniendo en cuenta:

- Constitución Política, articulo 15
- Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- La Ley 1341 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
- NTC 27001:2006. Sistema de Gestión de Seguridad de la Información.

II.INSTITUCION

Somos una Institución educativa que ofrece servicios a los niveles de educación preescolar, básica y media académica, cuyo objetivo es el desarrollo y la formación en valores de seres humanos íntegros, gestores de su perfectibilidad y trascendencia, bilingües, competentes y comprometidos con la transformación de Colombia

La dirección del COLEGIO MONTESSORI SAS, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para COLEGIO MONTESSORI SAS, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de COLEGIO MONTESSORI SAS
- Garantizar la continuidad del negocio frente a incidentes.
- COLEGIO MONTESSORI SAS ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

III. POLITICA DE SEGURIDAD DE LA INFORMACION

I. Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para la institución y por consiguiente debe ser debidamente protegida. El establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad de la Información garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones sustantivas de la entidad apoyadas en un correcto sistema de información. La institución establecerá los mecanismos para respaldar la difusión, estudio, actualización y consolidación tanto de la presente política como de los demás componentes del Sistema de Gestión de la Seguridad de la Información y alinearlos de forma efectiva con los demás sistemas de gestión.

II. Alcance

Esta Política se establece en cumplimiento de la legislación vigente (ley 1437 de 2011- Ley 1581 de 2012 – Decreto 4886 de 2011 y la resolución 55845 de 2021) con el objetivo de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del Colegio Montessori SAS de Cartagena de Indias. Es de aplicación para toda la comunidad educativa: Docentes, personal administrativo, personal de servicios generales, proveedores, estudiantes, padres de familia, ex alumnos, ex empleados, egresados, visitantes.

III. Responsabilidades

Directora General

Directora Financiera y administrativa: Responsable de garantizar los recursos económicos necesarios para la implementación, sostenimiento y mejora de esta política.
Jefe de gestión Habeas Data: Responsable de garantizar que lo establecido en esta politica se cumpla.
Responsable de gestionar los indicadores de gestión.
Responsable de gestionar la administración de los riesgos de esta política.
Comité de seguridad de la información: Es la máxima autoridad institucional en materia de seguridad de la información.
Director de Gestión Integral: Responsable de garantizar que esta política y todas las actividades que de ella se deriven, cumplan con requisitos legales, de norma ISO, del cliente y de la organización.
Jefe de gestión Humana: Responsable de garantizar la seguridad de la información de empleados, ex empleados, aspirantes y registrar la base de datos.

Jefe de Gestión de sistemas y comunicaciones: Responsable de garantizar que todos los equipos tienen licencia.
Secretaria Académica: Responsable de garantizar la seguridad de la información de las familias, los estudiantes, ex-alumnos y egresados y registrar la base de datos.

IV. Glosario

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.
Seguridad de la Información: La seguridad de la información se entiende como la preservación de las siguientes características:
Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta el Colegio Montessori SAS de Cartagena de Indias
Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
Tecnología de la Información: Se refiere al hardware y software operados por el Colegio Montessori SAS de Cartagena de Indias o por un tercero que procese información en su nombre, para llevar a cabo una función propia del colegio, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Evaluación de Riesgos. Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en el servicio educativo que presta el colegio Montessori SAS de Cartagena de Indias.
Administración de Riesgos: Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.
Comité de Seguridad de la Información: Es un órgano del gobierno escolar encargado de impulsar, velar y responder por la seguridad de la información del Colegio Montessori SAS de Cartagena de Indias
Incidente de Seguridad: Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.
Propietarios de la Información: Son los funcionarios, unidades académicas o dependencias responsables de la generación o recopilación de la información, con competencia jurídica para administrar y disponer de su contenido.
Activos de Información: Son los bienes relacionados a un sistema de información en cualquiera de sus etapas. Ejemplos de activos son:
Información: Bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, resultados de proyectos de investigación, etc.
Software: Software de aplicaciones, software de sistemas, herramientas de desarrollo, etc.
Activos físicos: Computadoras, equipamiento de redes y comunicaciones, medios de almacenamiento, mobiliario, lugares de emplazamiento.
Servicios: Servicios informáticos y de comunicaciones.
Aplicación: Se refiere a un sistema informático, tanto desarrollado por la UNC como por terceros, o al sistema operativo o software de base, que integren los sistemas de información o donde estos estén alojados.

V. Procedimientos internos relacionados con esta política.

I. El uso aceptable de los activos de la información
II. Escritorio limpio y claro de la pantalla, de los computadores institucionales
III. La transferencia de información.
IV. Los dispositivos móviles y el teletrabajo.
V. Las restricciones a la instalación de software y el uso.5.
VI. Copia de seguridad.

VII. La protección contra el malware.
VIII. La gestión de vulnerabilidades técnicas.
IX. Controles criptográficos.
X. Las comunicaciones de seguridad.
XI. La intimidad y la protección de la información personal identificable

VI. Comité de seguridad de la información

La seguridad y privacidad de la información de nuestra Comunidad Educativa, estará monitoreada, controlada por el Comité de seguridad de la Información.
Este comité estará conformado por:
1. Jefe de Gestión de la Información y Habeas Data (GIHD)
2. Jefe de Gestión del Conocimiento (GCTO)
3. Jefe de Gestión Sistemas y Comunicaciones (GSC)
4. Director de Sistema Integrado de Calidad (GI)
5. Directora Financiera Administrativa (GFA)

FUNCIONES DEL CSI

a- Revisar y aprobar, la Política y las responsabilidades generales en materia de seguridad de la información.
b- Monitorear cambios significativos en la exposición de activos de información frente a las amenazas más importantes.
c- Revisar y monitorear de los incidentes relativos a la seguridad.
d- Aprobar las principales iniciativas para incrementar la seguridad de la información.
e- Acordar funciones y responsabilidades específicas relativas a seguridad de la información Para toda la UNC.
f- Acordar metodologías y procesos específicos relativos a la seguridad de la información.
g- Acordar y brindar apoyo y difusión a las iniciativas de seguridad de la información.
h- Velar por que la seguridad sea parte del proceso de planificación de la información.
i- Garantizar que la seguridad sea parte del proceso de planificación de la información.
j- Evaluar y coordinar la pertinencia y la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
k- Promover la difusión y apoyo a la seguridad de la información dentro de la Comunidad Educativa Montessori
l- Desarrollar toda actividad relacionada con la seguridad de la información que le encomiende Dirección general

FUNCIONAMIENTO DEL CSI

1- Este Comité hace parte del gobierno escolar
2- Sesionará cada dos meses de manera ordinaria y pueden convocarse sesiones extraordinarias si la situación lo amerita.

3. La Coordinadora del CSI, será la jefe de Gestión de Habeas Data

VII. Objetivos

a) Proteger, preservar y administrar objetivamente la información del COLEGIO MONTESSORI SAS junto con las tecnologías utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

b) Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos del COLEGIO MONTESSORI SAS para asegurar su permanencia y nivel de eficacia.

c) Definir las directrices del COLEGIO MONTESSORI SAS para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

VII. Responsabilidad La Política de Seguridad de la Información

Es de aplicación obligatoria para todo el personal del COLEGIO MONTESSORI SAS, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe. Las directivas institucionales aprueban esta Política y son responsables de la autorización de sus modificaciones. El Comité de seguridad de la información será responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la entidad, lo cual incluye la operación del SGSI y supervisión del cumplimiento, dentro de la dependencia, de aspectos inherentes a los temas tratados en la presente Política. Los propietarios de activos de información (ver su definición en el glosario) son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado. Gestión Humana en conjunto con la gestión de Información y Habeas Data cumplirá la función de notificar a todo el personal que se vincula contractualmente con el COLEGIO MONTESSORI SAS, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de

los Compromisos de Confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos.

VIII. Seguridad de la información en el Recurso Humano.

Todo el personal del COLEGIO MONTESSORI SAS, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. El jefe de sistemas y comunicaciones deben mantener un directorio completo y actualizado de tales perfiles, determina cuales son los atributos que deben definirse para los diferentes perfiles y debe elaborar, mantener, actualizar, mejorar y difundir el manual de "Responsabilidades Personales para la Seguridad de la Información

. La responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el jefe de departamento o supervisor del contrato; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

IX. Responsabilidades del personal del COLEGIO MONTESSORI SAS

Cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y las tareas que desempeñe debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información institucional. Los procedimientos para obtener tales perfiles y las características de cada uno de ellos deben ser mantenidos y actualizados por cada dependencia. El Estatuto General y el Estatuto Docente deben contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones. Gestión Humana en conjunto con la gestión de información y habeas Data y la gestión de sistemas y comunicaciones se encargarán de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que propenda por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.

X. Responsabilidades de los estudiantes.

Para poder usar los recursos del COLEGIO MONTESSORI SAS, los acudientes deben leer y aceptar en cada matrícula un acuerdo con los términos y condiciones. La gestión de sistemas y comunicaciones debe asegurar los mecanismos para la difusión y aceptación de dichas condiciones por medio de registros y manuales en línea.

XI. Responsabilidades de Usuarios Externos

Todos los usuarios externos y personal de empresas externas deben estar autorizados por la gestión de sistemas y comunicaciones en conjunto con el comité de seguridad de la información quienes serán responsables del control y vigilancia del uso adecuado de la información y los recursos de TI institucionales.

Los procedimientos para el registro de tales usuarios deben ser creado y mantenido por el jefe de sistemas y comunicaciones. Los usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de TI institucionales. Las cuentas de usuarios externos deben ser de perfiles específicos y tener caducidad no superior a tres (3) meses, renovables de acuerdo a la naturaleza del usuario.

XII. Usuarios invitados y servicios de acceso público

El acceso de usuarios no registrados solo debe ser permitido al sitio web de información institucional. El acceso y uso a cualquier otro tipo de recurso de información y TI no es permitido a usuarios invitados o no registrados.

XII. Seguridad Física y del entorno

I. Acceso: Se debe tener acceso controlado y restringido a los cuartos de servidores principales, subsidiarios y a los cuartos de comunicaciones. El jefe de sistemas y comunicaciones elaborará y mantendrá las normas, controles y registros de acceso a dichas áreas.

II. Seguridad en los equipos: Los servidores que contengan información y servicios institucional deben ser mantenidos en un ambiente seguro y protegido por los menos con:

• Controles de acceso y seguridad física.

• Detección de incendio y sistemas de extinción de conflagraciones.

• Controles de humedad y temperatura.

• Bajo riesgo de inundación.

• Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS). Toda información institucional en formato digital debe ser mantenida en servidores aprobados por el jefe de sistemas y comunicaciones.

. El jefe de sistemas y comunicaciones debe asegurar que la infraestructura de servicios de TI este cubierta por mantenimiento y soporte adecuados de hardware y software.

Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de la institución el cual debe estar capacitado acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional. Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo a las políticas y estándares que para tal efecto elabore y mantenga El jefe de sistemas y comunicaciones Las dependencias tienen la responsabilidad de adoptar y cumplir las normas definidas para la creación y el manejo de copias de seguridad.

III. Copias de Seguridad: Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el jefe de sistemas y comunicaciones. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

El jefe de sistemas y comunicaciones debe realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas. Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin. El jefe de sistemas y comunicaciones debe proveer las herramientas para que las dependencias puedan administrar la información y registros de copias de seguridad.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.

Los usuarios deben entregar al respectivo jefe de dependencia las copias de seguridad para su registro y custodia.

IV. Administración de Configuraciones de Red

La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad.

V. Internet y Correo Electrónico

Las normas de uso de Internet y de los servicios de correo electrónico serán elaboradas, mantenidas y actualizadas por el Jefe de sistemas y comunicaciones, debe velar por el cumplimiento del código de ética institucional y el manejo responsable de los recursos de tecnologías de la información.

VI. Instalación de Software

Todas las instalaciones de software que se realicen sobre sistemas del COLEGIO MONTESSORI SAS deben ser aprobadas por el Jefe de sistemas y comunicaciones, de acuerdo a los procedimientos elaborados para tal fin por dichas dependencias.

No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas.

El jefe de sistemas y comunicaciones deben desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad que debe ser investigado. Corresponde al jefe de sistemas y comunicaciones mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos institucionales.

VII. Control de Acceso

I. Categorías de Acceso

El acceso a los recursos de tecnologías de información institucionales debe estar restringidos según los perfiles de usuario definidos por el jefe de sistemas y comunicaciones.

II. Control de Claves y Nombres de Usuario

El acceso a información restringida debe estar controlado. Se recomienda el uso de sistemas automatizados de autenticación que manejen credenciales o firmas digitales. Corresponde al jefe de sistemas y comunicaciones, mantener y publicar los documentos de servicios de red que ofrece la institución a su personal, estudiantes, docentes y terceros.

El jefe de sistemas y comunicaciones deben elaborar, mantener y publicar procedimientos de administración de cuentas de usuario para el uso de servicios de red. El acceso a sistemas de cómputo y los datos que contienen es responsabilidad exclusiva del personal encargado de tales sistemas.

EL COLEGIO MONTESSORI SAS debe propender por mantener al mínimo la cantidad de cuentas de usuario que el personal, los estudiantes, docentes y terceros deben poseer para acceder a los servicios de red. El control de las contraseñas de red y uso de equipos es responsabilidad del jefe de sistemas y comunicaciones.

Dichas contraseñas deben ser codificadas y almacenadas de forma segura. Las claves de administrador de los sistemas deben ser conservadas por el jefe de sistemas y comunicaciones y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.

VIII. Computación Móvil

EL COLEGIO MONTESSORI S.A.S reconoce el alto grado de exposición que presenta la información y los datos almacenados en dispositivos portátiles (computadores portátiles, notebooks, PDA, celulares, etc.). Corresponde a Gestión Humana en conjunto con la gestión de Habeas Data y la gestión de sistemas y comunicaciones elaborar, mantener e implementar planes de capacitación que propendan por la formación y mantenimiento de la conciencia en cuestión de seguridad de la información. Las redes inalámbricas potencialmente introducen nuevos riesgos de seguridad que deben ser identificados, valorados y tratados de acuerdo a los lineamientos de la Política de Seguridad en redes inalámbricas que debe elaborar la Gestión de sistemas y comunicaciones.

IX. Acceso Remoto

El acceso remoto a servicios de red ofrecidos por el COLEGIO MONTESSORI SAS debe estar sujeto a medidas de control definidas por la Gestión de sistemas y comunicaciones, las cuales deben incluir acuerdos escritos de seguridad de la información.