CONSEJO DIRECTIVO
RESOLUCIÓN No. 1799

Por la cual se aprueban los Lineamientos para la Seguridad de la Información de la Institución Universitaria Colegios de Colombia – UNICOC

El Consejo Directivo de la Institución Universitaria Colegios de Colombia – Unicoc, en uso de sus atribuciones estatutarias y en especial de las contenidas en el Artículo 14 de sus numerales 1 y 13 y

CONSIDERANDO

PRIMERO. Que es función del Consejo Directivo fijar la Política General, la Misión, el Proyecto Educativo Institucional y orientar los objetivos de la Institución Universitaria Colegios de Colombia Unicoc.

SEGUNDO. Que es función del Consejo Directivo velar porque la marcha de la Institución este acorde con las disposiciones legales y estatutarias.

TERCERO. Que los **Lineamientos para la Seguridad de la Información** de UNICOC, buscan garantizar la protección y privacidad de los datos, preservando la confidencialidad de la información personal, académica y administrativa. Asimismo, estos lineamientos aseguran que la Institución cumpla con las normativas de seguridad de la información, tanto nacionales como protocolos internacionales, estableciendo controles que se ajustan a los estándares de protección de datos y privacidad.

CUARTO. Que en la sesión del Consejo Directivo celebrada el día trece (13) de mayo del año 2025, una vez hecho el tránsito por las respectivas instancias, se presentó para aprobación del Consejo Directivo los **Lineamientos para la Seguridad de la Información,** según consta en el Acta No. 442 y en el orden del día correspondiente a la sesión mencionada.

Que, en mérito de lo expuesto, este Consejo Directivo

RESUELVE:

ARTÍCULO PRIMERO. Aprobar de forma unánime, según consta en el Acta 442, los **Lineamientos para la Seguridad de la Información** de la Institución Universitaria Colegios de Colombia- UNICOC.

ARTÍCULO SEGUNDO. Los **Lineamientos para la Seguridad de la Información** de UNICOC se aprueban de manera integral así:

LINEAMIENTOS PARA LA SEGURIDAD DE LA INFORMACIÓN

1. Introducción

1.1. Propósito de los lineamientos

El propósito de estos lineamientos de seguridad de la información es establecer una guía clara y estructurada para gestionar, proteger y salvaguardar la información dentro de la institución, tanto en los ámbitos académicos como administrativos y tecnológicos. Estos lineamientos tienen como objetivo propender por que la información esté protegida contra riesgos y amenazas cibernéticas, manteniendo su confidencialidad, integridad y disponibilidad.

En un contexto de constante evolución tecnológica, donde el uso de tecnologías avanzadas como las TIC y la Inteligencia Artificial (IA) se ha vuelto esencial para las operaciones educativas y administrativas, los lineamientos buscan crear un entorno seguro mediante la implementación de controles específicos y medidas de protección. Además, fomentan la adopción de una cultura de ciberseguridad entre todos los miembros de la comunidad colegial.

Estos lineamientos se alinean con el Plan Estratégico de Desarrollo Institucional (PEDI), especialmente en el Área Estratégica de Sistema Integrado de Información, promoviendo la sostenibilidad, trazabilidad y seguridad del patrimonio informático y documental institucional. Están diseñados no solo para proteger la información interna de la institución, sino también para garantizar el cumplimiento de las regulaciones locales e internacionales en materia de privacidad y seguridad de la información. Apuntan hacia normativas, como las ISO 27001, 27110 y 27400, y con las políticas internas de la institución, como la Política TIC y la Política de Inteligencia Artificial.

A través de estos lineamientos, la institución se compromete a garantizar la protección y privacidad de los datos, preservando la confidencialidad de la información personal, académica y administrativa. Asimismo, estos lineamientos aseguran que la institución cumpla con las normativas de seguridad de la información, tanto nacionales como protocolos internacionales, estableciendo controles que se ajustan a los estándares de protección de datos y privacidad.

Además, se busca fortalecer la ciberseguridad institucional mediante un enfoque preventivo, implementando medidas que mitiguen los riesgos y las amenazas cibernéticas. Esto incluye la identificación de riesgos potenciales, la implementación de controles adecuados y la creación de un plan de respuesta ante incidentes de seguridad. Los lineamientos también promueven la concienciación y formación continua en ciberseguridad, fomentando buenas prácticas en el manejo de datos y garantizando que toda la comunidad educativa esté preparada para proteger la información de manera efectiva.

Finalmente, estos lineamientos contribuyen a la sostenibilidad de las infraestructuras tecnológicas de la institución, asegurando un uso eficiente y seguro de los recursos tecnológicos, incluidos

1.2. Alcance y ámbito de aplicación

Los presentes lineamientos de seguridad de la información se aplican de manera integral a todos los sistemas, procesos y personas que interactúan con la información dentro de la institución. El alcance abarca todos los niveles de la organización, incluyendo el personal directivo, administrativo, académico, estudiantes, contratistas y cualquier otro actor que tenga acceso a los activos de información de la institución. Estos lineamientos establecen las responsabilidades y procedimientos que deben ser seguidos por todos los usuarios para garantizar la seguridad de la información, independientemente del tipo de datos que manejen o los medios a través de los cuales accedan a ellos.

El ámbito de aplicación de estos lineamientos cubre todos los activos de información, tales como documentos electrónicos, bases de datos, sistemas informáticos, redes, dispositivos móviles, aplicaciones y cualquier otra tecnología utilizada en la recolección, almacenamiento, procesamiento y transmisión de información. Asimismo, incluye los servicios externos contratados por la institución que tengan acceso o interactúen con la información de la misma.

Estos lineamientos se aplican a todos los procesos relacionados con el ciclo de vida de la información, desde su creación o recolección, hasta su archivo, eliminación o destrucción, con especial atención a la protección de datos personales, información confidencial y activos críticos. La implementación de estas medidas tiene como fin evitar pérdidas, filtraciones, accesos no autorizados, modificaciones indebidas, o cualquier otro tipo de incidente que pueda comprometer la confidencialidad, integridad o disponibilidad de la información.

Específicamente, los lineamientos son aplicables en los siguientes contextos:

- Infraestructura tecnológica:
  Toda la infraestructura que soporta los sistemas de información de la institución, incluyendo redes, servidores, bases de datos, dispositivos de almacenamiento, sistemas de seguridad y soluciones basadas en la nube.

- Usuarios de la información:
  Personal administrativo, académico, estudiantes, y cualquier usuario que acceda o maneje información institucional, independientemente de su rol o ubicación, ya sea dentro o fuera de las instalaciones de la institución.

- Sistemas y aplicaciones:
  Software y aplicaciones utilizadas para gestionar, procesar o almacenar información. Esto incluye sistemas de gestión académica, plataformas de aprendizaje, sistemas financieros, y cualquier otro software de uso institucional.

- Proveedores de servicios externos:
  Entidades externas que proporcionan servicios tecnológicos, de infraestructura o de información a la institución, como proveedores de plataformas de gestión de datos, almacenamiento en la nube, o aplicaciones de inteligencia artificial. Todos los proveedores deben cumplir con los estándares de seguridad definidos por la institución y ajustarse a las normativas de protección de datos vigentes.

- Tecnologías emergentes:
  Los lineamientos también se extienden al uso de nuevas tecnologías como la Inteligencia Artificial Generativa (IAG) y el Internet de las Cosas (IoT), asegurando que su implementación cumpla con los requisitos de seguridad y privacidad establecidos por la institución, minimizando riesgos y amenazas emergentes.

Estos lineamientos son obligatorios para todos los miembros de la comunidad colegial y cualquier persona o entidad que tenga acceso a la información institucional. El incumplimiento de estos puede derivar en sanciones disciplinarias y, en el caso de proveedores externos, en la terminación de contratos o acuerdos.

1.3. Relación con la política TIC y de Inteligencia Artificial

Los presentes lineamientos de seguridad de la información están estrechamente alineados con las directrices establecidas en la Política TIC Institucional y la Política de Inteligencia Artificial (IA) de la institución. Estas políticas establecen los tecnológicos que guían el desarrollo, la implementación y el uso responsable de las tecnologías de la información, en un marco que prioriza la protección de los datos y la seguridad en el entorno digital.

1.3.1. Protección de la Información y Privacidad de los Datos

Una de las principales prioridades tanto de la Política TIC como de los presentes lineamientos es garantizar la protección de la información y la privacidad de los datos de todos los miembros de la comunidad institucional. Esto incluye la implementación de medidas que aseguren que la información personal, académica, financiera y administrativa esté resguardada frente a accesos no autorizados, alteraciones indebidas o destrucción no intencional.

Los lineamientos establecen controles de acceso que aseguran que solo personal autorizado pueda acceder a la información sensible, conforme a su rol dentro de la institución. Además, se garantiza que los datos personales y académicos de los estudiantes, profesores, y personal administrativo se manejen bajo estrictos protocolos de seguridad y con total respeto a la normativa de protección de datos vigente, tanto a nivel nacional como internacional.

La Política TIC Institucional proporciona el marco normativo bajo el cual se implementan tecnologías de seguridad como el cifrado de datos, mecanismos de autenticación robustos, y políticas de gestión de contraseñas, todo con el fin de proteger la integridad y la confidencialidad de la información. Los presentes lineamientos complementan estas medidas asegurando su cumplimiento en todos los sistemas y procesos tecnológicos de la institución.

1.3.2. Fortalecimiento de la Ciberseguridad en Sistemas con IA

En un contexto donde el uso de la Inteligencia Artificial (IA) cobra cada vez mayor relevancia, los presentes lineamientos incorporan directrices específicas para asegurar que la implementación y uso de IA en la institución esté alineada con los principios de ciberseguridad establecidos en la Política TIC y la Política de IA.

La IA presenta nuevas oportunidades, pero también introduce riesgos adicionales para la seguridad de la información. Por lo tanto, se hace necesario un enfoque de seguridad adaptativa que permita monitorear y mitigar los riesgos específicos que puedan surgir del uso de tecnologías avanzadas. Los lineamientos aseguran que los sistemas de IA que procesan grandes volúmenes de datos sean configurados y utilizados de forma segura, evitando cualquier tipo de exposición no autorizada de datos sensibles o vulnerabilidades en la infraestructura tecnológica.

El fortalecimiento de la ciberseguridad incluye la implementación de mecanismos de detección de amenazas avanzadas, basados en IA, que permiten identificar patrones de comportamiento anómalos o potenciales ataques en tiempo real. De esta forma, la IA no solo se convierte en un recurso valioso para los procesos educativos y administrativos, sino también en una herramienta clave para prevenir incidentes de seguridad.

1.3.3. Cumpliendo de Normativas Nacionales e Internacionales en TIC e IA

Tanto la Política TIC como la Política de IA subrayan la importancia de cumplir con todas las normativas nacionales e internacionales relacionadas con la protección de datos, la privacidad y la ciberseguridad. Los presentes lineamientos reflejan este compromiso, alineándose con las regulaciones nacionales como la Ley 1581 de 2012 de Protección de Datos Personales y las normativas internacionales, tales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

Además, estos lineamientos cumplen con estándares internacionales de gestión de la seguridad de la información, incluyendo las normativas ISO 27001, que especifica los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI); la ISO 27110, que ofrece directrices para la estandarización de medidas de seguridad adaptables a diferentes contextos; y la ISO 27400, que proporciona un marco para la seguridad y privacidad en soluciones de Internet de las Cosas (IoT).

Al garantizar el cumplimiento de estas normativas, la institución se asegura de que todos los procesos tecnológicos, tanto en el ámbito de las TIC como de la IA, se lleven a cabo bajo los más altos estándares de seguridad y respeto a la privacidad. De esta manera, se promueve un entorno confiable y seguro para

el manejo de la información, reduciendo los riesgos de incumplimiento legal o vulnerabilidades que puedan afectar la integridad de los sistemas institucionales.

2. Principios de Seguridad de la Información

Los presentes lineamientos se fundamentan en los principios de confidencialidad, integridad, disponibilidad y responsabilidad en el uso de las TIC y la Inteligencia Artificial, y deben cumplirse en todas las operaciones de la institución para garantizar la seguridad de la información. A continuación, se describen los lineamientos que cada actor de la institución debe seguir para asegurar el cumplimiento de estos principios:

- Confidencialidad

  La información deberá ser protegida contra accesos no autorizados, garantizando que solo las personas o entidades debidamente autorizadas puedan acceder a ella. El acceso a los sistemas de información deberá gestionarse mediante mecanismos de autenticación robustos, como la autenticación multifactor, y deberán implementarse políticas claras de control de accesos basadas en roles y permisos.

  Toda la información deberá ser cifrada tanto en tránsito como en reposo para asegurar que no pueda ser interceptada o accedida de manera no autorizada. El alojamiento de la información deberá realizarse en datacenters Tier 3, que ofrezcan un nivel de seguridad física y lógica adecuado para proteger los datos de posibles amenazas.

- Integridad

  La integridad de la información deberá garantizarse a través de controles que aseguren que los datos no sean alterados sin autorización. Cualquier modificación a los datos deberá ser registrada y auditada, de modo que se mantenga una trazabilidad completa de las alteraciones realizadas.

  Los sistemas utilizados para el almacenamiento y procesamiento de la información deberán contar con mecanismos de validación de datos y recuperación ante errores, asegurando que cualquier fallo sea detectado y corregido a tiempo. El acceso a los registros y auditorías deberá estar restringido y protegido para evitar manipulaciones no autorizadas.

- Disponibilidad

La información y los sistemas deberán estar disponibles para los usuarios autorizados en el momento en que se requieran. Los servicios deberán alojarse en plataformas tecnológicas que ofrezcan alta disponibilidad y redundancia, con mecanismos de respaldo y recuperación ante desastres para minimizar el tiempo de inactividad.

El alojamiento de los datos deberá realizarse en datacenters Tier 3, que garanticen un entorno con redundancia en energía, enfriamiento y conectividad para asegurar la continuidad del servicio en caso de fallos. Además, deberá implementarse un plan de continuidad operativa que asegure la disponibilidad de la información en escenarios de emergencia.

- Responsabilidad en el Uso de las TIC e IA
  Todos los usuarios de la institución deberán hacer un uso responsable y ético de las TIC y los sistemas de IA. El acceso a la información y los recursos tecnológicos deberá gestionarse bajo estrictos principios de responsabilidad, asegurando que cada usuario cumpla con las políticas de seguridad de la institución y mantenga la confidencialidad y seguridad de los datos a los que acceda.

  La institución deberá proporcionar formación continua a todos los miembros de la comunidad educativa para garantizar que estén informados sobre las buenas prácticas de ciberseguridad y sobre cómo proteger la información a la que tienen acceso. Las tecnologías emergentes, como la IA, deberán ser utilizadas de manera ética, asegurando que su implementación no comprometa la seguridad ni la privacidad de los datos.

3. Clasificación de la información

Para garantizar una gestión segura y eficiente de la información, la institución establece un sistema de clasificación de la información basado en su nivel de sensibilidad, criticidad y necesidad de protección. Esta clasificación permitirá aplicar controles proporcionales a los riesgos asociados, garantizar el cumplimiento normativo y facilitar la toma de decisiones frente al acceso, conservación y disposición final de los datos. La información biométrica (huellas, rostros, datos de vigilancia) tendrá un tratamiento especial conforme al Reglamento General y la Ley 1581 de 2012, con medidas reforzadas de seguridad y trazabilidad

3.1. Escalas de clasificación

- Información Pública
  Información que puede ser divulgada sin restricciones. Su acceso está garantizado por normativas de transparencia (Ley 1712 de 2014) y no representa riesgos para la institución ni para los titulares de los datos.
  Ejemplos: reglamentos institucionales, resultados de convocatorias, horarios académicos.

- Información Interna
  Información de uso exclusivo dentro de la comunidad institucional. Su divulgación no está permitida sin autorización expresa y su uso está restringido al desarrollo de las funciones académicas o administrativas.
  Ejemplos: comunicaciones internas, reportes de gestión, planes de clase, actas de comités.

- Información Confidencial
  Información cuyo acceso está limitado solo a personal autorizado debido a su sensibilidad o implicaciones legales. Su divulgación, pérdida o alteración puede generar riesgos institucionales, legales o reputacionales.
  Ejemplos: datos personales, historias académicas y clínicas, nómina, contratos, evaluaciones.

- Información Sensible o de Alto Riesgo
  Datos que afectan directamente la privacidad o la integridad de personas o procesos estratégicos. Incluye datos biométricos, financieros o datos protegidos por reserva legal.
  Ejemplos: huellas digitales, reconocimiento facial, información médica, denuncias disciplinarias.

3.2. Aplicación de controles por niveles de clasificación

Clasificación	Acceso	Medidas de seguridad	Tiempo de retención
Pública	Abierto	Sin restricciones	Según TRD institucional
Interna	Comunidad institucional	Autenticación básica, cifrado de tránsito	Según TRD institucional
Confidencial	Personal autorizado	Cifrado en reposo y tránsito, MFA, auditoría	Según TRD o disposición legal

Sensible/Alto Riesgo	Solo roles específicos	Cifrado fuerte, trazabilidad, respaldo, custodia física reforzada	Según TRD o norma legal específica

3.3. Revisión y actualización de clasificación

Las categorías asignadas a los documentos o sistemas de información deberán revisarse anualmente o cuando se produzcan cambios significativos en su uso, formato, legislación aplicable o nivel de riesgo. La Dirección de Gestión Documental, en articulación con la Dirección TIC y el Comité Interno de Archivo, será responsable de actualizar las clasificaciones cuando sea necesario.

4. Objetivos de Seguridad de la Información

Los siguientes objetivos de seguridad de la información están diseñados para guiar las acciones y políticas de la institución en la protección de la información, el cumplimiento normativo y la promoción de un entorno seguro y responsable en el uso de las TIC e IA. Cada objetivo debe ser alcanzado mediante la implementación de los lineamientos descritos y el compromiso de todos los miembros de la comunidad institucional.

- Garantizar la Protección de los Datos de la Comunidad
  La institución deberá establecer mecanismos efectivos para asegurar la protección de todos los datos personales, académicos, administrativos y financieros de la comunidad. Esto incluirá la adopción de medidas de seguridad como el cifrado de datos en tránsito y en reposo, la gestión de accesos basada en permisos específicos, y la implementación de políticas de privacidad que limiten el acceso solo a personas autorizadas.

  Los datos deberán estar alojados en entornos que ofrezcan niveles de seguridad física y lógica adecuados, tales como datacenters Tier 3, y los sistemas deberán contar con redundancia para garantizar la protección y disponibilidad continua de la información. Cualquier incidente de seguridad relacionado con la exposición o alteración de datos deberá ser tratado de manera inmediata mediante procedimientos de respuesta a incidentes claramente establecidos.

- Promover el Uso Responsable y Ético de las TIC e IA
  La institución deberá fomentar un uso responsable y ético de las TIC y las IA, tanto en el ámbito académico como administrativo. Todos los usuarios que interactúen con los sistemas de información deberán ser formados

continuamente en prácticas de ciberseguridad y en la protección de la privacidad de los datos.

Se deberán implementar políticas claras que regulen el uso de las TIC e IA, asegurando que las tecnologías avanzadas se utilicen de manera que respeten los derechos y la privacidad de los individuos. Cualquier uso de IA deberá ser supervisado para evitar que comprometa la seguridad de la información, y deberá cumplir con los principios éticos de transparencia y rendición de cuentas.

- Fortalecer la Cultura de Ciberseguridad
  La creación y fortalecimiento de una cultura de ciberseguridad dentro de la institución será una prioridad. Esto implicará la sensibilización de todos los miembros de la comunidad educativa, desde estudiantes hasta el personal administrativo y académico, sobre la importancia de la seguridad de la información y los riesgos asociados a su mal manejo.

  La institución deberá implementar programas de capacitación continua en buenas prácticas de ciberseguridad, con especial énfasis en la protección de datos personales, la identificación de amenazas cibernéticas y la respuesta a incidentes de seguridad. Además, se fomentará la participación activa de la comunidad en la detección y reporte de vulnerabilidades, promoviendo un enfoque preventivo y colaborativo hacia la ciberseguridad.

5. Gestión de Riesgos

La gestión de riesgos en seguridad de la información tiene como objetivo identificar, evaluar y mitigar los riesgos asociados al manejo y protección de los datos dentro de la institución. Los siguientes lineamientos establecen los pasos y responsabilidades que deberán seguirse para asegurar una gestión proactiva y efectiva de los riesgos. La protección de la información también deberá estar articulada con los instrumentos archivísticos vigentes (TRD, TVD, Cuadro de Clasificación Documental), asegurando que la sensibilidad de la información se refleje en los tiempos de conservación, acceso y disposición final.

5.1. Identificación y Evaluación de Riesgos

La institución deberá implementar un proceso sistemático de identificación de riesgos en todas las áreas que involucren el uso, almacenamiento y transmisión de

información sensible. Este proceso incluirá la detección de vulnerabilidades en los sistemas tecnológicos, procesos operativos y en el acceso de los usuarios.

Cada riesgo identificado deberá ser evaluado en términos de su probabilidad de ocurrencia y su impacto potencial en la confidencialidad, integridad y disponibilidad de la información. La evaluación de riesgos deberá realizarse periódicamente y actualizarse ante cambios significativos en la infraestructura tecnológica o en la normativa de seguridad.

5.2. Mitigación de Riesgos

Una vez identificados y evaluados los riesgos, la institución deberá desarrollar e implementar estrategias de mitigación que minimicen el impacto de dichos riesgos en los sistemas de información. Estas estrategias pueden incluir medidas de control como el cifrado de datos, la limitación de accesos, la aplicación de parches y actualizaciones de seguridad, así como la implementación de políticas de acceso basadas en el rol.

Los planes de mitigación deberán ser revisados y ajustados regularmente para asegurar su efectividad frente a nuevos riesgos o amenazas emergentes. La institución también deberá contar con planes de contingencia para mantener la operatividad de sus servicios en caso de incidentes.

5.3. Plan de Respuesta ante Incidentes de Seguridad

La institución deberá contar con un plan de respuesta ante incidentes de seguridad que establezca los procedimientos a seguir en caso de detectar una brecha de seguridad o acceso no autorizado. Este plan deberá incluir un protocolo claro para la detección, análisis, contención, erradicación y recuperación de los incidentes de seguridad, garantizando una respuesta oportuna y efectiva.

Los equipos responsables deberán estar capacitados en la ejecución del plan de respuesta, y el plan deberá ser probado y revisado de manera regular para asegurar su vigencia y eficacia. Además, la institución deberá mantener registros detallados de los incidentes y generar informes que faciliten el análisis posterior y la mejora continua de las políticas de seguridad.

6. Controles y Medidas de Seguridad de la información

Los controles y medidas de seguridad de la información son mecanismos y prácticas establecidas para proteger los activos de información de la institución y asegurar que

los datos se manejen de acuerdo con los principios de confidencialidad, integridad y disponibilidad. A continuación, se describen los controles específicos que deben implementarse para mitigar riesgos y proteger la información de accesos no autorizados, alteraciones indebidas y posibles amenazas cibernéticas. Los documentos en soporte físico deben almacenarse en condiciones de seguridad equivalentes a los digitales, utilizando mobiliario cerrado, control de acceso físico, registro de préstamos y protocolos de eliminación segura conforme al Reglamento General para la Gestión Documental

6.1. Controles de Acceso y Autorización

La institución deberá implementar controles de acceso que aseguren que solo los usuarios autorizados puedan acceder a la información sensible. Estos controles deberán basarse en mecanismos de autenticación multifactor y permisos que limiten el acceso en función de los roles y responsabilidades de cada usuario. Las credenciales de acceso deberán gestionarse de manera segura, incluyendo el uso de contraseñas fuertes y el establecimiento de políticas de expiración y renovación de estas.

6.2. Protección de Datos Personales y Sensibles

Se deberá garantizar la protección de los datos personales y sensibles mediante el uso de medidas de encriptación que aseguren que la información esté protegida tanto en tránsito como en reposo. Los sistemas de almacenamiento de datos deberán cumplir con normativas de protección de datos y privacidad, limitando el acceso a datos personales únicamente a usuarios autorizados y conforme a sus funciones dentro de la institución.

6.3. Cifrado y Almacenamiento Seguro de Información

Toda información sensible o confidencial deberá ser cifrada para prevenir accesos no autorizados. El cifrado deberá aplicarse tanto a los datos almacenados como a los datos en tránsito. Los dispositivos y sistemas de almacenamiento utilizados por la institución deberán contar con configuraciones de seguridad robustas, y los medios de almacenamiento externo deberán ser gestionados de acuerdo con políticas de cifrado y control de acceso.

6.4. Monitoreo, Detección y Respuesta a Amenazas

La institución deberá establecer un sistema de monitoreo continuo que permita detectar posibles amenazas y actividades inusuales que puedan comprometer la seguridad de la información. Este monitoreo deberá incluir el análisis de registros

de acceso, patrones de tráfico en la red y cualquier actividad sospechosa en los sistemas críticos.
En caso de detectar una amenaza, el sistema de respuesta deberá activarse de manera inmediata, iniciando los procedimientos de contención, análisis y resolución de incidentes, conforme al plan de respuesta ante incidentes de seguridad.

6.5. Seguridad en Infraestructura Tecnológica

La infraestructura tecnológica de la institución deberá estar protegida mediante configuraciones de seguridad específicas para redes, servidores y dispositivos. Las redes deberán contar con segmentación, cortafuegos y sistemas de prevención de intrusiones para protegerse contra accesos no autorizados y ataques externos. Los servidores deberán mantenerse actualizados con los parches de seguridad necesarios, y los dispositivos de los usuarios deberán cumplir con políticas de seguridad, incluyendo el uso de antivirus, configuraciones de seguridad y restricciones de acceso.

7. Cultura de Ciberseguridad y Buenas Prácticas

Fomentar una sólida cultura de ciberseguridad y promover buenas prácticas en el uso de la información y las tecnologías son componentes esenciales para la protección de los activos de información de la institución. Estos lineamientos aseguran que todos los miembros de la comunidad educativa, desde el personal administrativo hasta los estudiantes, estén capacitados y comprometidos en la protección de la seguridad de la información y en la utilización ética de las TIC e IA.

7.1. Uso Responsable y Ético de la IA y las TIC

La institución promoverá el uso responsable y ético de las TIC y la Inteligencia Artificial (IA). Todos los usuarios deberán conocer sus responsabilidades al utilizar herramientas tecnológicas, especialmente en lo relacionado con el uso de IA. Esto incluye actuar con respeto a la privacidad, garantizar la transparencia en el manejo de datos y asumir la responsabilidad por sus acciones dentro del entorno digital.

El uso de IA deberá cumplir con principios de equidad y transparencia, y su implementación deberá ser monitoreada para evitar cualquier posible vulneración de los derechos de los individuos y proteger la integridad de los datos personales.

7.2. Formación Continua en Seguridad de la Información

La institución deberá implementar un programa de formación continua en seguridad de la información que esté disponible para todos los miembros de la comunidad

educativa. Este programa incluirá capacitación en identificación de amenazas, protección de datos personales, uso seguro de las TIC y ciberseguridad general.

La capacitación deberá actualizarse regularmente para incluir las últimas prácticas y medidas de protección, adaptándose a las nuevas amenazas y tecnologías emergentes. Además, se incentivará a todos los miembros a participar activamente en estas capacitaciones para asegurar un alto nivel de concienciación sobre ciberseguridad en toda la institución.

7.3. Buenas Prácticas en Protección de Datos Personales y Académicos

La institución deberá promover buenas prácticas en la protección de datos personales y académicos, asegurando que todos los usuarios comprendan la importancia de manejar la información de manera segura y responsable. Estas prácticas incluirán el manejo adecuado de contraseñas, la protección de dispositivos de acceso a la red institucional y la utilización de métodos seguros para compartir información.

Se deberá establecer un código de conducta en el manejo de la información, que estipule claramente las prácticas y responsabilidades de cada usuario en la protección de los datos y que promueva el reporte inmediato de incidentes de seguridad o vulnerabilidades identificadas.

8. Cumplimiento y Auditoria de Seguridad de la Información

Para asegurar la efectividad y el cumplimiento de los lineamientos de seguridad de la información, es fundamental llevar a cabo auditorías periódicas y verificar que las prácticas y políticas implementadas cumplan con las normativas y estándares de seguridad establecidos. Estos lineamientos aseguran una evaluación constante de los sistemas y procesos, así como la adopción de mejoras continuas para mantener la seguridad y protección de los datos.

8.1. Auditoria de los Sistemas de IA y Tecnologías de la Información

La institución realizará auditorías periódicas a sus sistemas de información y tecnologías, incluyendo aquellos que incorporan IA. Estas auditorías permitirán evaluar la eficacia de los controles de seguridad implementados, así como identificar vulnerabilidades o aspectos que requieran mejora en la infraestructura tecnológica y en el uso de IA.

Las auditorías deberán ser llevadas a cabo por personal capacitado o por terceros especializados, asegurando una evaluación imparcial y detallada. Los resultados deberán documentarse, y las recomendaciones para corregir o mejorar la seguridad de los sistemas deberán ser implementadas en un plazo razonable.

8.2. Cumplimiento de Regulaciones y Normativas

La institución deberá garantizar que todos los procesos y sistemas relacionados con la gestión de la información cumplan con las regulaciones y normativas nacionales e internacionales aplicables. Esto incluye el cumplimiento de la Ley de Protección de Datos Personales, así como de normativas internacionales como las ISO 27001, 27110 y 27400.

Los equipos responsables deberán mantenerse actualizados en cuanto a las regulaciones vigentes y realizar las adaptaciones necesarias para asegurar el cumplimiento continuo. Cualquier cambio en la normativa deberá ser evaluado y, en caso de ser necesario, deberán ajustarse los lineamientos y políticas de la institución para reflejar los nuevos requisitos.

8.3. Gestión de No Conformidades y Planes de mejora

En caso de detectar no conformidades o fallas en el cumplimiento de los lineamientos de seguridad, la institución deberá establecer un plan de acción para corregir dichas deficiencias. Esto incluye la identificación de la causa raíz de la no conformidad y la implementación de medidas correctivas para evitar que el problema vuelva a ocurrir.

Además, la institución deberá desarrollar planes de mejora continua en seguridad de la información, basados en las evaluaciones y auditorías realizadas. Estos planes deberán ser revisados y actualizados periódicamente para asegurar que reflejen las necesidades cambiantes y los desafíos de seguridad de la institución.

El cumplimiento de los planes de mejora y la resolución de no conformidades serán supervisados y evaluados para asegurar su efectividad, garantizando que la institución mantenga un alto nivel de seguridad en la protección de la información.

9. Responsabilidades en la Seguridad de la Información

Las responsabilidades en seguridad de la información son fundamentales para asegurar que todos los miembros de la institución comprendan y asuman su papel en la protección de los datos. Estos lineamientos asignan roles claros en la gestión, implementación y cumplimiento de las políticas de seguridad de la información para garantizar un entorno seguro y controlado. El Comité Interno de Archivo, en conjunto con la Dirección de TIC y la Dirección de Gestión Documental, deberá coordinar las acciones de seguridad de la información que afecten el ciclo de vida documental, asegurando la coherencia entre la infraestructura tecnológica y los instrumentos de gestión documental.

9.1. Roles y Responsabilidades de la Dirección Institucional

La dirección institucional es responsable de establecer y apoyar la estrategia de seguridad de la información. Deberá garantizar que los recursos necesarios, tanto humanos como financieros, estén disponibles para implementar las políticas de seguridad. La dirección también deberá promover una cultura de ciberseguridad y asegurar que la seguridad de la información sea una prioridad institucional.

La alta dirección es responsable de aprobar los lineamientos de seguridad, realizar revisiones periódicas para evaluar su efectividad y ajustar las políticas conforme a las necesidades y cambios en el entorno tecnológico y normativo. Además, deberá supervisar el cumplimiento de las normativas y liderar la respuesta ante incidentes de seguridad críticos.

9.2. Responsabilidades del Personal Administrativo, Académico y Técnico

Todo el personal administrativo, técnico y académico tiene la responsabilidad de cumplir con los lineamientos de seguridad de la información en sus respectivas funciones. Esto incluye proteger la información a la que tienen acceso, cumplir con los controles de seguridad establecidos y reportar cualquier actividad sospechosa o incidente de seguridad.

El personal técnico, en particular, es responsable de implementar los controles de acceso, monitoreo y protección en los sistemas y redes de la institución. Además, deberá mantener actualizadas las configuraciones de seguridad y responder rápidamente ante cualquier vulnerabilidad o falla detectada en los sistemas.

El personal académico y administrativo deberá garantizar la seguridad y privacidad de la información relacionada con los estudiantes y los contenidos académicos, y promover el uso responsable de las TIC e IA en el ámbito educativo.

9.3. Responsabilidades de los Usuarios generales y Miembros de la Comunidad Colegial

Todos los usuarios, incluyendo estudiantes y otros miembros de la comunidad colegial, son responsables de utilizar las TIC e IA de manera ética y segura. Deberán cumplir con las políticas de seguridad establecidas, proteger la confidencialidad de sus credenciales de acceso y seguir las buenas prácticas en el manejo de información personal y académica.

Los usuarios deberán reportar inmediatamente cualquier anomalía, intento de acceso no autorizado o incidente de seguridad a las áreas de soporte correspondientes. Asimismo, deberán participar en las capacitaciones y formaciones en ciberseguridad para estar al tanto de las mejores prácticas y ser conscientes de los riesgos que enfrentan en el entorno digital.

10. Revisión y Actuación de los Lineamientos

Para garantizar que los lineamientos de seguridad de la información se mantengan efectivos y alineados con los avances tecnológicos, cambios normativos y las necesidades de la institución, es fundamental establecer un proceso de revisión y actualización continua. Este proceso asegura que los lineamientos se adapten y respondan a los desafíos de seguridad en un entorno en constante evolución.

10.1. Procedimiento de Revisión periódica

La institución deberá establecer un calendario de revisión periódica de los lineamientos de seguridad de la información. Esta revisión se realizará al menos una vez al año, aunque podrán programarse revisiones adicionales en caso de cambios significativos en la infraestructura tecnológica, incidentes de seguridad importantes o modificaciones en las normativas legales.

Durante la revisión, se evaluará la efectividad de los lineamientos, identificando áreas de mejora y cualquier ajuste necesario para fortalecer la seguridad de la información. Los resultados de la revisión deberán ser documentados y aprobados por la dirección institucional.

10.2. Actualización según Cambios Normativos o Tecnológicos

La institución deberá actualizar los lineamientos cuando se produzcan cambios en las normativas legales, estándares internacionales o en la tecnología utilizada. Esta actualización garantizará el cumplimiento continuo con las leyes y regulaciones

aplicables, como la Ley de Protección de Datos y los estándares ISO 27001, 27110 y 27400, entre otros.

Cualquier actualización deberá incluir una evaluación de impacto para asegurar que los cambios propuestos no afecten la seguridad o privacidad de los datos. Una vez realizadas las actualizaciones, deberán comunicarse adecuadamente a todos los miembros de la institución, garantizando que estén al tanto de las nuevas directrices y requerimientos de seguridad.

10.3. Roles y Responsables en la Actualización

La dirección institucional será responsable de liderar y aprobar las actualizaciones de los lineamientos, asegurando que estos se adapten a los nuevos requisitos de seguridad y que cumplan con los estándares de la institución. Los equipos técnicos y de cumplimiento serán los encargados de evaluar y proponer cambios en los lineamientos, basándose en las mejores prácticas de la industria y en los resultados de las revisiones periódicas.

Asimismo, todos los miembros de la comunidad educativa deberán ser informados sobre los cambios en los lineamientos y recibir la capacitación necesaria para implementar las nuevas prácticas de seguridad. Este enfoque garantizará que los lineamientos se mantengan efectivos y que la comunidad esté preparada para afrontar los riesgos de seguridad emergentes.

Referencias

- Institución Universitaria Colegios de Colombia (Unicoc). (2017). *Plan Estratégico de Desarrollo Institucional (PEDI) 2017–2025*. Unicoc.
- Institución Universitaria Colegios de Colombia (Unicoc). (2024). *Política de Tecnologías de la Información y Comunicación (TIC)* (Versión 1.1). Unicoc.
- Institución Universitaria Colegios de Colombia (Unicoc). (2024). *Política de Inteligencia Artificial*. Unicoc.
- Institución Universitaria Colegios de Colombia (Unicoc). (2025). *Política de Gestión Documental*. Resolución 1762 del Consejo Directivo. Unicoc.
- Institución Universitaria Colegios de Colombia (Unicoc). (2024). *Reglamento General para la Gestión Documental y la Administración de Archivos*. Unicoc.
- International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. ISO.

- International Organization for Standardization. (2021). *ISO/IEC 27110:2021 Information technology — Cybersecurity framework development guidelines*. ISO.
- International Organization for Standardization. (2022). *ISO/IEC 27400:2022 Information technology — Internet of things (IoT) — Security and privacy guidelines*. ISO.
- Congreso de la República de Colombia. (2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial*, 48.587.
- Ministerio de Tecnologías de la Información y las Comunicaciones. (2013). *Decreto 1377 de 2013: Reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial*, 48.830.
- Archivo General de la Nación. (2024). *Acuerdo 001 de 2024: Acuerdo único de la función archivística en el Estado colombiano.*
- Microsoft. (s.f.). *Microsoft 365*. Recuperado de https://www.microsoft.com
- Unión Europea. (2016). *Reglamento General de Protección de Datos (GDPR)*, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

ARTÍCULO TERCERO. La presente resolución rige a partir de la fecha de expedición y deroga todas las normas anteriores relacionadas con la materia o que le sean contrarias.

COMUNIQUESE Y CÚMPLASE

Dada en Bogotá D.C., a los trece días (13) del mes de mayo del año dos mil veinticinco (2025)

MARÍA SOLEDAD ARANGO MEJÍA
Presidente

Institución Universitaria Colegios de Colombia
unicoc
PRESIDENCIA

ANA MARÍA CUBILLOS HERANDEZ
Secretaria General

INSTITUCIÓN UNIVERSITARIA COLEGIOS DE COLOMBIA
unicoc
SECRETARÍA GENERAL

Institución Universitaria Colegios de Colombia
NIT: 860.045.054-1
Autopista Norte Km. 20, Campus Bogotá
Cr. 9 No. 12B-40, Bogotá, Centro
Cl. 13 Norte No 3N - 13, Cali