# MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DE ANTIOQUIA: ADAPTACIÓN DEL MARCO MINTIC.

**GESTIÓN DE TECNOLOGÍA Y MEDIOS AUDIOVISUALES.**

**INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DE ANTIOQUIA.**

**2026**

1. **Resumen Ejecutivo**

**Visión General del Modelo de Seguridad y Privacidad de la Información (MSPI) Propuesto para la Institución Universitaria Colegio Mayor de Antioquia**

El Modelo de Seguridad y Privacidad de la Información (MSPI) propuesto para la Institución Universitaria Colegio Mayor de Antioquia es un marco estratégico integral, meticulosamente diseñado para gestionar sistemáticamente los riesgos inherentes a la seguridad y privacidad de la información. Este modelo se construye sobre los cimientos del MSPI del Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) de Colombia, integrando de manera rigurosa las leyes nacionales de protección de datos, en particular la Ley 1581 de 2012 y su Decreto reglamentario 1377 de 2013. La adaptación del MSPI se ha personalizado para alinearse con el entorno académico, administrativo y de investigación único de una institución de educación superior. Su implementación efectiva no solo fortalecerá la resiliencia de la institución frente a las ciber amenazas en constante evolución, sino que también asegurará el cumplimiento normativo estricto y fomentará una cultura de confianza y responsabilidad en toda su comunidad universitaria.

**Beneficios Clave y Alineación Estratégica.**

La adopción e implementación de este MSPI generará beneficios sustanciales para el Colegio Mayor de Antioquia. Entre ellos se incluye una protección significativamente mejorada de los datos sensibles de estudiantes, personal y proyectos de investigación; el cumplimiento riguroso de la normativa nacional vigente en materia de seguridad y privacidad de la información; la mejora sustancial de la continuidad operativa de los servicios académicos y administrativos; la reducción del riesgo de incidentes cibernéticos y, consecuentemente, la minimización de los daños financieros y reputacionales asociados; y el fortalecimiento de una cultura organizacional proactiva en seguridad y privacidad en toda la universidad.

Desde una perspectiva estratégica, este MSPI soporta directamente los objetivos institucionales al salvaguardar los activos intelectuales, mantener la integridad académica y asegurar la entrega

ininterrumpida de servicios educativos en un panorama cada vez más digitalizado. La implementación del MSPI trasciende el mero cumplimiento normativo para consolidarse como un imperativo estratégico fundamental para el Colegio Mayor de Antioquia. Este enfoque no solo protege la información, sino que es crucial para mantener la reputación de la institución, un activo intangible de valor incalculable. Una postura de seguridad robusta es un factor decisivo para atraer y retener estudiantes y personal cualificado, quienes son cada vez más conscientes de la importancia de la protección de sus datos personales y académicos. Además, el modelo es vital para salvaguardar la propiedad intelectual generada en la investigación y asegurar la continuidad de la misión educativa central en un mundo digitalizado, donde la interrupción de servicios por incidentes de seguridad puede tener consecuencias devastadoras.

Un MSPI robusto y demostrablemente conforme puede conferir una ventaja competitiva significativa al Colegio Mayor de Antioquia. En el contexto actual, donde la confianza en el manejo de la información es un diferenciador clave, una institución que protege proactivamente los datos y cumple con estándares internacionales, como la ISO 27001 (referenciada por el MSPI en su Documento Maestro), puede construir una reputación más sólida. Esta reputación mejorada puede traducirse en una mayor atracción de estudiantes y profesores, especialmente aquellos preocupados por la privacidad de los datos y la seguridad digital en un entorno académico globalizado. La capacidad de demostrar un compromiso serio con la seguridad y la privacidad puede, a su vez, facilitar colaboraciones de investigación y desarrollo con otras instituciones y empresas, generando así una ventaja competitiva sostenible en el sector de la educación superior.



## 2. Introducción: La Importancia de la Seguridad y Privacidad en el Entorno Universitario.

### Contexto Global y Nacional de Ciberseguridad y Privacidad de la Información

La transformación digital ha posicionado la información como un activo crítico para todas las organizaciones, pero, paradójicamente, también la ha convertido en un objetivo principal para ataques maliciosos. A nivel global, los ciberataques están en un aumento constante, causando daños económicos significativos que, en algunos países, podrían sobrepasar el 1% del Producto Interno Bruto (PIB). América Latina, en particular, enfrenta un panorama de amenazas creciente, caracterizado por una notable brecha en el talento de ciberseguridad, estimada en 600,000

profesionales en la región, y un bajo nivel promedio de madurez en sus capacidades de ciberseguridad, que se sitúa entre los niveles 1 y 2 de un modelo de madurez.

Las universidades, al ser custodias de vastas cantidades de datos personales, académicos y de investigación sensibles, son cada vez más vulnerables a diversas ciber amenazas. Estas incluyen el *phishing* y los ataques de correo electrónico, que buscan engañar a los usuarios para obtener información confidencial o instalar *malware*; los ataques de *malware* y *ransomware*, que pueden cifrar datos y exigir rescates; los ataques de fuerza bruta, que intentan adivinar contraseñas; y los ataques a través de dispositivos móviles, que explotan aplicaciones maliciosas para obtener acceso no autorizado. La preocupación por la privacidad de los datos es creciente entre los usuarios, con menos del 50% confiando en que la tecnología mejorará sus vidas en este aspecto.

**Relevancia para la Institución Universitaria Colegio Mayor de Antioquia.**

Como institución pública de educación superior, el Colegio Mayor de Antioquia gestiona una diversidad de activos de información esenciales para sus funciones académicas, administrativas y de investigación. Esto incluye datos personales de estudiantes, profesores y personal administrativo, propiedad intelectual derivada de la investigación, registros académicos e información financiera. Proteger estos activos es fundamental para mantener la integridad institucional, asegurar la continuidad de los servicios y cumplir con las regulaciones nacionales como el MSPI del MinTIC y las leyes de protección de datos personales.

Las universidades, incluyendo el Colegio Mayor de Antioquia, enfrentan un perfil de amenazas cibernéticas único debido a sus entornos inherentemente abiertos y colaborativos. La gran y transitoria base de usuarios, compuesta por estudiantes que utilizan una diversidad de dispositivos personales y a menudo acceden a redes no seguras, amplía significativamente la superficie de ataque. Además, la presencia de valiosos datos de investigación y propiedad intelectual convierte a las instituciones académicas en objetivos particularmente atractivos para diversos actores maliciosos. Esta combinación de un entorno abierto y datos de alto valor crea desafíos de seguridad más complejos que en un entorno corporativo típico, lo que exige un enfoque de seguridad adaptado y robusto.

El "factor humano" se identifica consistentemente como una vulnerabilidad significativa en las universidades. Los estudiantes, profesores y empleados administrativos no siempre utilizan redes seguras para acceder a la información, y pueden ser susceptibles a ataques de

*phishing*. Esto sugiere que los controles técnicos por sí solos son insuficientes para garantizar una seguridad integral. Una implementación efectiva del MSPI debe, por lo tanto, poner un fuerte énfasis en programas continuos de concienciación y capacitación para toda la comunidad universitaria. Al educar a los usuarios sobre cómo reconocer y responder a las amenazas, y fomentar hábitos de protección, la institución puede construir una cultura de seguridad robusta, transformando a los individuos de posibles puntos débiles en una primera línea de defensa activa.

3. **Marco Normativo y Referencial**.



**El Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de las TIC de Colombia**

El Modelo de Seguridad y Privacidad de la Información (MSPI) es un marco integral desarrollado por el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) de Colombia. Su propósito fundamental es impartir lineamientos a las entidades públicas para la implementación y adopción de buenas prácticas en seguridad y privacidad de la información, tomando como referencia estándares internacionales. El objetivo principal del MSPI es orientar la gestión e implementación adecuada del ciclo de vida de la seguridad, ayudando a las entidades a identificar y gestionar los riesgos asociados con la información, asegurar el cumplimiento de la legislación vigente y optimizar sus procesos institucionales.

El MSPI contempla un ciclo de operación de cinco (5) fases, las cuales permiten a las entidades gestionar adecuadamente la seguridad y privacidad de su información, basándose en el ciclo Planificar-Hacer-Verificar-Actuar (PHVA).

- **Diagnóstico:** En esta fase, la entidad debe determinar el estado actual de la gestión de seguridad y privacidad de la información, identificar su nivel de madurez y evaluar el cumplimiento de la legislación vigente relacionada con la protección de datos personales y las

buenas prácticas en ciberseguridad.

- **Planificación:** Implica formular la política de seguridad y privacidad de la información de la entidad, definir roles y responsabilidades claras, elaborar un inventario y clasificar los activos de información, definir la gestión de riesgos y establecer indicadores de gestión para medir la eficiencia y eficacia del sistema.
- **Implementación/Operación:** Durante esta fase, se implementan los controles necesarios para mitigar los riesgos identificados, se establecen procedimientos operativos estándar (POE) y se gestionan los incidentes de seguridad y privacidad de la información.
- **Evaluación de Desempeño:** Consiste en definir métricas y criterios de evaluación para medir el progreso de la institución en la adopción efectiva del MSPI. Se realizan auditorías internas al modelo de seguridad y privacidad y revisiones periódicas por parte de la dirección para verificar el cumplimiento y la efectividad.
- **Mejora Continua:** En esta fase se establecen mecanismos para la identificación de no conformidades y la implementación de acciones correctivas, asegurando así la mejora continua del modelo en respuesta a los cambios en el entorno y las amenazas.

El MinTIC proporciona una serie de componentes clave y documentación oficial para guiar la implementación del MSPI. Estos incluyen el Documento Maestro MSPI, lineamientos sobre Roles y Responsabilidades, Indicadores de Gestión de Seguridad de la Información, Inventario y Clasificación de Activos de Información e Infraestructura Crítica Cibernética Nacional, el Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas, y guías sobre la Relación con Proveedores de Tecnologías de la Información y las Comunicaciones y la Seguridad de la información para el uso de servicios en la nube. Además, se ofrecen formatos como la Política general de seguridad, el Manual de políticas del MSPI y el Plan estratégico de seguridad, así como instrumentos de autodiagnóstico, gestión de activos y riesgos, y servicios en la nube.

Es importante destacar que el MSPI se alinea con estándares internacionales de seguridad de la información. El Documento Maestro del MSPI hace referencia explícita a la norma ISO/IEC 27001:2022 para la estructura de sus controles, lo que garantiza un enfoque reconocido globalmente para la gestión de la seguridad de la información.

**Marco Legal Colombiano de Protección de Datos Personales**

La implementación del MSPI en el Colegio Mayor de Antioquia debe estar firmemente anclada en el marco legal colombiano de protección de datos personales, que es fundamental para garantizar la privacidad y los derechos de los individuos.

**Ley 1581 de 2012 (Protección de Datos Personales)**

Esta ley estatutaria es el pilar fundamental del régimen general de protección de datos personales en Colombia. Reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.

- **Objeto y Alcance:** La ley busca desarrollar el derecho constitucional de *habeas data*.[3] Se aplica a datos personales registrados en cualquier base de datos que pueda ser objeto de tratamiento por entidades públicas o privadas, así como al tratamiento realizado en territorio colombiano o cuando la legislación colombiana sea aplicable. Excluye bases de datos para uso personal/doméstico, seguridad nacional, inteligencia, periodísticas y aquellas reguladas por leyes específicas.
- **Principios Rectores:** Establece principios fundamentales como la legalidad (el tratamiento debe sujetarse a la ley), finalidad (propósito legítimo informado al titular), libertad (consentimiento previo, expreso e informado), veracidad o calidad (información veraz, completa y actualizada), transparencia (derecho del titular a obtener información sobre sus datos), acceso y circulación restringida (límites al tratamiento y acceso solo por personas autorizadas), seguridad (medidas para proteger la información) y confidencialidad (obligación de garantizar la reserva de la información no pública).
- **Datos Sensibles:** Prohíbe el tratamiento de datos que afecten la intimidad del titular o cuyo uso indebido pueda generar discriminación (ej. origen racial, datos de salud, datos biométricos), con excepciones muy específicas, como el consentimiento explícito del titular o la necesidad de salvaguardar un interés vital.
- **Derechos de Niños, Niñas y Adolescentes:** Asegura el respeto de sus derechos prevalentes, generalmente prohibiendo el tratamiento de sus datos personales a menos que sean de naturaleza pública. Además, exige que el Estado y las entidades educativas proporcionen información y capacitación a los representantes legales sobre los riesgos y el uso responsable de sus datos.

- **Derechos de los Titulares:** Los titulares tienen derecho a conocer, actualizar y rectificar sus datos; solicitar prueba de autorización; ser informados sobre el uso de sus datos; presentar quejas ante la Superintendencia de Industria y Comercio (SIC); revocar la autorización y/o solicitar la supresión de sus datos; y acceder a sus datos tratados de forma gratuita.
- **Deberes de los responsables y Encargados:** La ley impone deberes específicos a los responsables (quienes deciden sobre el tratamiento) y encargados (quienes realizan el tratamiento por cuenta del responsable). Estos incluyen garantizar el pleno ejercicio de los derechos de *habeas data*, asegurar la seguridad de la información, actualizar y rectificar datos, tramitar consultas y reclamos, adoptar políticas internas y reportar brechas de seguridad.
- **Vigilancia y Sanciones:** La Superintendencia de Industria y Comercio (SIC), a través de su Delegatura para la Protección de Datos Personales, es la autoridad encargada de la vigilancia y puede imponer sanciones como multas, suspensión o cierre de actividades por incumplimiento.



**Decreto 1377 de 2013 (Reglamentación parcial de la Ley 1581)**

Este decreto reglamenta parcialmente la Ley 1581 de 2012, proporcionando disposiciones más detalladas para su aplicación.

- **Autorización:** Especifica los procedimientos para obtener el consentimiento previo, expreso e informado del titular, y la necesidad de conservar prueba de dicha autorización.
- **Políticas de Tratamiento:** Exige que los responsables desarrollen y pongan a disposición políticas claras de tratamiento de la información en lenguaje sencillo, incluyendo la finalidad, los derechos del titular y la información de contacto para consultas.
- **Aviso de Privacidad:** Define el contenido mínimo para informar a los titulares sobre el tratamiento de datos cuando las políticas completas no pueden ser proporcionadas de inmediato, asegurando que se les informe cómo acceder a la política completa.
- **Ejercicio de Derechos:** Detalla los mecanismos para que los titulares ejerzan sus derechos de acceso, actualización, rectificación, supresión y revocación de la autorización, incluyendo la designación de un área o persona responsable para tramitar estas solicitudes.
- **Responsabilidad Demostrada:** Manda que los responsables demuestren a la SIC que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones de la Ley 1581 y el decreto, de manera proporcional a la naturaleza y tamaño de la entidad, las características

de los datos y los riesgos potenciales.

- **Datos Recolectados Antes del Decreto:** Establece procedimientos para solicitar la autorización a los titulares de bases de datos existentes antes de la entrada en vigencia del decreto, permitiendo continuar el tratamiento si no hay solicitud de supresión en un plazo determinado.
- **Transferencias y Transmisiones Internacionales:** Aclara las reglas para el movimiento de datos personales a través de fronteras, distinguiendo entre transferencia (a un responsable) y transmisión (a un encargado), y los requisitos contractuales para estas últimas.

El MSPI no es solo un marco técnico, sino que está profundamente entrelazado con los requisitos legales de protección de datos en Colombia. El cumplimiento de la Ley 1581 y el Decreto 1377 es un pilar fundamental y un objetivo explícito del MSPI.[5] El modelo del MinTIC proporciona el "cómo" para cumplir con el "qué" exigido por la legislación, haciendo que la adhesión legal sea un componente central del modelo de seguridad, no un anexo. Esto significa que cada fase y componente del MSPI debe ser diseñado e implementado con una clara consideración de las obligaciones legales.

Al adoptar el MSPI, el Colegio Mayor de Antioquia puede pasar de un cumplimiento legal reactivo a un enfoque proactivo e integrado. Esto se logra aprovechando las fases estructuradas del MSPI, como la gestión de riesgos, la formulación de políticas y las auditorías, para abordar sistemáticamente las obligaciones legales y demostrar la "responsabilidad demostrada" exigida por el Decreto 1377. Por ejemplo, la fase de planificación del MSPI incluye la formulación de políticas de seguridad y privacidad, las cuales deben incorporar los requisitos de las políticas de tratamiento de datos personales exigidas por la ley. Las auditorías internas y los indicadores de gestión, parte de la fase de evaluación del desempeño del MSPI, sirven como mecanismos para verificar y documentar el cumplimiento continuo, lo que es esencial para la "responsabilidad demostrada". Esta integración asegura que las obligaciones legales estén incrustadas en los procesos operativos diarios de la institución, en lugar de ser una tarea separada y a menudo descuidada.

**4. Análisis del Contexto de la Institución Universitaria Colegio Mayor de Antioquia**

Para adaptar eficazmente el Modelo de Seguridad y Privacidad de la Información (MSPI), es crucial comprender en profundidad el contexto organizacional, tecnológico y de datos del Colegio Mayor de Antioquia.

**Estructura Organizacional y Procesos Clave.**

El Colegio Mayor de Antioquia posee una estructura administrativa definida, establecida por el Acuerdo 011 de 2022. Sus principales órganos de gobierno incluyen la Rectoría, el Consejo Superior Universitario (máximo órgano de dirección y gobierno), el Consejo Académico (máxima autoridad académica) y diversas Vicerrectorías, como la Administrativa y Financiera y la Académica. Dentro de esta estructura, el departamento de "Gestión de Tecnología e Informática" es un componente crítico, ubicado bajo la sección "Mi Colmayor" en el organigrama institucional.

La institución cuenta con un "Mapa de Procesos" que describe sus procesos estratégicos, misionales, de apoyo y de evaluación. Estos procesos abarcan una amplia gama de funciones, incluyendo la gestión académica (por ejemplo, programas de la Vicerrectoría Académica, subprocesos de formación para el trabajo y desarrollo humano, virtualidad, y aseguramiento de calidad académica), funciones administrativas (como planeación, gestión de tecnología e informática, control interno, comunicaciones y gestión documental), y la investigación. El desarrollo académico de la universidad se centra en tres grandes campos de conocimiento: turismo, gastronomía y gestión comercial/mercadeo. Esta especialización implica el manejo de tipos de datos y sistemas específicos relacionados con estas disciplinas, que deben ser considerados en el diseño del MSPI.

**Infraestructura Tecnológica Actual y Gestión de TI.**

El departamento de "Gestión de Tecnología e Informática" del Colegio Mayor de Antioquia es el actor principal en la administración de la seguridad de la información. Este departamento es responsable de la publicación y gestión de documentos clave como el plan de mantenimiento de servicios tecnológicos, los planes de seguridad y privacidad de la información, los planes de

tratamiento de riesgos de seguridad y privacidad, y el Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC). Además, este departamento es el encargado de informar sobre el progreso de la implementación del MSPI dentro de la institución.

La existencia de estos planes, particularmente un "PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN" y un "PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN" para varios años, incluyendo 2025, indica una comprensión fundamental y esfuerzos existentes en estas áreas. Estos documentos y la experiencia acumulada pueden servir como una línea de base sólida para la adaptación del MSPI, permitiendo que la implementación se enfoque en la mejora y estandarización en lugar de partir de cero.

Aunque no se proporcionan detalles específicos de la infraestructura tecnológica del Colegio Mayor de Antioquia posee una infraestructura universitaria típica incluye centros de datos con servicios de internet, servidores físicos y virtuales para sistemas críticos (bases de datos, aplicaciones, almacenamiento), equipos de red (firewalls para seguridad perimetral, routers, switches, puntos de acceso inalámbricos), segmentación de red (separación de redes administrativas y académicas) y una variedad de servicios (correo electrónico, software académico/administrativo/financiero, copias de seguridad automáticas, telefonía, red Wi-Fi extensa). Esta descripción proporciona una buena aproximación al tipo de infraestructura que el Colegio Mayor de Antioquia probablemente posee y que necesita ser protegida por el MSPI.



**Identificación de Activos de Información Críticos y Tipos de Datos Manejados.**

Basándose en las funciones académicas, administrativas y de investigación del Colegio Mayor de Antioquia, la identificación de los activos de información críticos es fundamental. Estos activos incluirían:

- **Datos Personales:** Registros de estudiantes (historial académico, admisiones, ayuda financiera), datos de recursos humanos de profesores y personal, información de exalumnos. Estos datos son altamente sensibles y están sujetos a la Ley 1581 de 2012 y el Decreto 1377 de 2013.
- **Datos Académicos:** Materiales de cursos, sílabos, calificaciones, contenido de sistemas de gestión del aprendizaje (LMS).

- **Datos de Investigación:** Datos generados por proyectos de investigación en turismo, gastronomía e ingeniería comercial. Esto puede incluir propiedad intelectual, datos sensibles de participantes y metodologías propietarias.
- **Datos Administrativos:** Registros financieros, información presupuestaria, contratos, documentos legales, políticas institucionales.
- **Infraestructura de TI:** Servidores, bases de datos, dispositivos de red, puntos finales, servicios en la nube utilizados por la institución.

La universidad maneja una combinación de datos públicos, privados y sensible Se requiere atención especial para los datos personales sensibles (por ejemplo, información de salud de estudiantes, datos biométricos para control de acceso) y datos de menores, cuyo tratamiento está sujeto a requisitos específicos y, en general, proscrito a menos que sean de naturaleza pública y con las debidas garantías.

El departamento de "Gestión de Tecnología e Informática" del Colegio Mayor de Antioquia ya cuenta con planes de seguridad y riesgos actuales. Esto representa una ventaja significativa, ya que la implementación del MSPI no debería ser una revisión completa, sino una integración y mejora de estos procesos y documentos establecidos, alineándolos más formalmente con el marco del MinTIC. La existencia de una base de trabajo, experiencia y procedimientos documentados permite que la adaptación del MSPI se enfoque en identificar brechas con el marco nacional y refinar o expandir lo existente, lo que resulta en una implementación más eficiente y menos disruptiva.

Dada la diversidad de campos académicos de la universidad (Ciencias de la salud, Ciencias Sociales, Arquitectura y Ciencias de la Educación) y sus múltiples funciones administrativas, la propiedad de los activos de información probablemente está altamente distribuida entre facultades, departamentos y grupos de investigación. Esta naturaleza distribuida exige una estructura de gobernanza centralizada y sólida para el MSPI, que emane de la alta dirección (Rectoría, Consejos), al tiempo que empodera a los "propietarios" locales de los activos con responsabilidades claras para su identificación, clasificación y protección. El departamento de "Gestión de Tecnología e Informática" deberá actuar como el coordinador central y facilitador, asegurando la coherencia y el cumplimiento en toda la institución.


*Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones*

**5. Propuesta del Modelo de Seguridad y Privacidad de la Información (MSPI) Adaptado**.

La propuesta del MSPI para la Institución Universitaria Colegio Mayor de Antioquia se estructura siguiendo las cinco fases del ciclo PHVA (Planificar-Hacer-Verificar-Actuar) del modelo del MinTIC, adaptadas a las particularidades del entorno universitario.

**Fase 1: Diagnóstico y Establecimiento del Contexto.**

En esta fase inicial, el Colegio Mayor de Antioquia realizará un autodiagnóstico exhaustivo de su estado actual en seguridad y privacidad de la información, utilizando el instrumento "Autodiagnóstico MSPI" provisto por el MinTIC. Este proceso permitirá identificar el nivel de madurez actual de la institución, que, a través de su diagnóstico, alcanzó el Nivel 3: Administrado. El diagnóstico debe abarcar una revisión detallada de las políticas, procedimientos, controles técnicos y factores humanos existentes.

Paralelamente, se involucrará activamente a las partes interesadas clave, incluyendo la Rectoría, Vicerrectorías, facultades, estudiantes, personal administrativo, el departamento de Gestión de Tecnología e Informática y socios externos, para identificar sus necesidades y expectativas específicas en materia de seguridad y privacidad de la información. Esto es fundamental para asegurar que el MSPI sea pertinente y responda a las realidades operativas y estratégicas de la universidad. Finalmente, se definirá claramente el alcance del MSPI dentro del Colegio Mayor de Antioquia, especificando qué activos de información, sistemas, procesos y personal están cubiertos.

Este alcance debe considerar las actividades académicas y de investigación únicas de la universidad, como las relacionadas con turismo, gastronomía e ingeniería comercial, y su naturaleza distribuida.

**Fase 2: Planificación del MSPI**

La fase de planificación sienta las bases para la implementación del MSPI.

**Política de Seguridad y Privacidad de la Información Institucional**

Se formulará una política de alto nivel que articule el compromiso de la institución con la seguridad y privacidad de la información. Esta política deberá ser aprobada por la máxima dirección institucional, como el Comité de Gestión y Desempeño Institucional o los Consejos Superior y Académico. La política debe alinearse con los lineamientos del MinTIC y los principios de la Ley 1581 de 2012, estableciendo el marco general, los objetivos y los requisitos legales.

Dentro del proceso de Tecnología y Medios Audiovisuales, se propuso una política global que abarca tanto lo referente a la seguridad digital, el gobierno digital, la adquisición, administración y desarrollo de software en los cuales se establecen los lineamientos para el manejo y la seguridad de la información de los sistemas institucionales.

**Roles y Responsabilidades**

Se definirán y asignarán claramente los roles y responsabilidades para la seguridad y privacidad de la información en toda la institución. Esto incluye la designación de un "Líder o encargado de Seguridad de la Información" o "responsable de Seguridad Digital", idealmente ubicado en el departamento de "Gestión de Tecnología e Informática", quien liderará el desarrollo e implementación del MSPI con el apoyo de toda la estructura organizacional. La siguiente tabla detalla los roles principales y sus responsabilidades clave:

**Tabla 1: Roles y Responsabilidades Clave para la Implementación del MSPI en Colmayor**

| Rol | Responsabilidades Clave |
|---|---|
| Rector/Comité de desempeño/Concejo Directivo | Aprobar la política de seguridad y privacidad, asignar los recursos necesarios, promover la cultura de seguridad, supervisar el cumplimiento general del MSPI. |

**Inventario y Clasificación de Activos de Información**

Se desarrollará un inventario exhaustivo de todos los activos de información de la institución, incluyendo hardware, software, datos, servicios, documentos y personal. Estos activos se clasificarán según su criticidad en términos de confidencialidad, integridad y disponibilidad (CIA). Para este proceso, se utilizará el instrumento "Activos de Información MSPI" del MinTIC. La clasificación permitirá priorizar los esfuerzos de protección.



**Tabla 2: Matriz de Activos de Información y su Clasificación (Ejemplo para Colmayor).**

| Nombre del Activo | Descripción | Propietario | Confidencialidad (C) | Integridad (I) | Disponibilidad (A) | Ubicación/ Sistema |
|---|---|---|---|---|---|---|
| Base de Datos de Estudiantes | Información personal y académica de estudiantes activos e inactivos. | Vicerrectoría Académica | Alta | Alta | Alta | Servidor de Aplicaciones Académicas |

| | | | | | | |
|---|---|---|---|---|---|---|
| Servidores de Investigación | Almacenamiento de datos y resultados de proyectos de investigación. | Vicerrectoría de Investigación | Alta | Alta | Media | Centro de Datos Principal |
| Plataforma LMS (Moodle) | Contenido de cursos, calificaciones, interacciones de estudiantes. | Vicerrectoría Académica | Media | Alta | Alta | Servidores en la Nube |
| Archivos de Admisiones | Documentos y datos de aspirantes a programas académicos. | Oficina de Admisiones y Registro | Alta | Media | Media | Servidor de Archivos Administrativos |
| Redes de Campus (Cableada/ Wi-Fi) | Infraestructura de comunicación para acceso a internet y | Gestión de Tecnología e Infor | Media | Alta | Alta | Edificios del Campus |

| | | | | | | |
|---|---|---|---|---|---|---|
| | recursos internos. | mática | | | | |
| Datos Financieros | Registros contables, presupuestos, nóminas, información de proveedores. | Vicerrectoría Administrativa y Financiera | Alta | Alta | Alta | Servidor de Aplicaciones Financieras |
| Equipos de Cómputo de Laboratorios | PC y estaciones de trabajo en laboratorios especializados (ej. Gastronomía, Turismo). | Decanatos de Facultades | Baja | Media | Media | Laboratorios |



**Modelo de Gestión de Riesgos de Seguridad de la Información Adaptado**

Se implementó una metodología de gestión de riesgos basada en el "Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas" del MinTIC, que se alinea con estándares como ISO/IEC 27000 y Magerit. Este proceso implica identificar, analizar, evaluar y tratar los riesgos. La valoración del riesgo combinará el impacto en la confidencialidad, integridad y disponibilidad del activo (CID), el nivel de amenaza y el nivel de vulnerabilidad.

Esta gestión de riesgos consiste entre otras cosas, en un procedimiento para la gestión de incidentes de seguridad que se encuentra cargado dentro del Sistema de Gestión Positiva G+, al

Plan de Tratamiento de Riesgos de Seguridad de la Información y al Plan de Continuidad del Negocio que han sido formulados por el proceso de Tecnología y Medios Audiovisuales.

**Plan Estratégico de Seguridad y Privacidad**

Se desarrollará un plan estratégico que describa los objetivos, iniciativas y recursos necesarios para la implementación y gestión continua del MSPI. Este plan se integrará con la planificación estratégica más amplia de la institución, asegurando que la seguridad y privacidad sean consideradas en todas las iniciativas institucionales.

**Fase 3: Operación e Implementación de Controles.**

En esta fase, los planes se traducen en acciones concretas mediante la implementación de controles y procedimientos.

**Implementación de Controles**.

Se aplicará una gama de controles técnicos, organizacionales y físicos para mitigar los riesgos identificados, alineados con los controles del Anexo A de ISO 27001. Ejemplos de estos controles incluyen:

- **Técnicos:** Implementación de autenticación multifactor (MFA), establecimiento de políticas de contraseñas robustas, segmentación de red para aislar sistemas críticos, despliegue de *firewalls* y sistemas antivirus actualizados, realización de copias de seguridad regulares y cifrado de datos sensibles, e implementación de sistemas de detección de intrusiones.
- **Organizacionales:** Desarrollo de políticas de control de acceso basadas en el principio de "necesidad de conocer", establecimiento de procedimientos claros de respuesta a incidentes, gestión de relaciones con proveedores de TI que incluya cláusulas de seguridad, y directrices específicas para la seguridad en el uso de servicios en la nube.
- **Físicos:** Aseguramiento de centros de datos con controles de acceso estrictos, restricción de acceso a áreas sensibles de la infraestructura de TI, y aplicación de controles ambientales

adecuados (temperatura, humedad) en salas de servidores.

**Gestión de Incidentes de Seguridad**.

Se establecerán procedimientos claros para identificar, reportar, analizar, responder y recuperarse de incidentes de seguridad de la información. Esto incluye la definición de roles y responsabilidades para un Equipo de Respuesta a Emergencias Cibernéticas (CERT) o una función similar, capaz de coordinar la gestión de incidentes de seguridad digital.

**Seguridad para el Uso de Servicios en la Nube y Relación con Proveedores**.

Se implementarán directrices claras para la adopción segura de servicios en la nube, asegurando que los datos alojados externamente cumplan con los mismos estándares de seguridad y privacidad que los datos internos. Adicionalmente, se establecerán requisitos de seguridad claros y cláusulas contractuales obligatorias para todos los proveedores externos que manejen información de la institución, incluyendo auditorías periódicas de cumplimiento.

La siguiente tabla presenta un ejemplo de plan de tratamiento de riesgos, ilustrando cómo se abordarán los riesgos identificados con controles y acciones específicas:

**Tabla 3: Plan de Tratamiento de Riesgos (Ejemplo de Controles y Acciones).**

| ID Riesgo | Nivel de Riesgo (Inicial) | Opción de Tratamiento | Control/Acción Específica | Área/Rol Responsable |
|---|---|---|---|---|
| R001 | Alto | Mitigar | Implementar autenticación multifactor (MFA) | Gestión de Tecnología e Informática |

| | | | | |
|---|---|---|---|---|
| | | | para todos los sistemas críticos. | |
| R002 | Alto | Mitigar | Realizar simulacros de *phishing* trimestrales y capacitación obligatoria. | Gestión de Tecnología e Informática |
| R003 | Medio | Mitigar | Implementar solución antivirus/antimalware centralizada y actualizada. | Gestión de Tecnología e Informática |
| R004 | Alto | Mitigar | Establecer políticas de contraseñas complejas y rotación periódica. | Gestión de Tecnología e Informática |
| R005 | Medio | Mitigar | Cifrado de bases de datos sensibles (estudiantes, financieros, investigación). | Gestión de Tecnología e Informática, Dueños de Activos/Proveedores |
| R006 | Alto | Mitigar | Realizar copias de seguridad diarias de datos críticos con almacenamiento fuera de sitio. | Gestión de Tecnología e Informática |

| | | | | |
|---|---|---|---|---|
| R007 | Medio | Reducir | Implementar políticas de seguridad para dispositivos móviles institucionales y personales. | Gestión de Tecnología e Informática |
| R008 | Alto | Mitigar | Auditorías internas de cumplimiento de la Ley 1581 y Decreto 1377. | Control Interno, Gestión de Tecnología e Informática |

**Fase 4: Evaluación del Desempeño.**

La evaluación del desempeño es crucial para medir la efectividad del MSPI.

**Definición de Indicadores de Gestión**.

Se tienen establecidos los indicadores dentro del Plan de Privacidad y Seguridad de la Información para medir la efectividad, eficiencia y eficacia del MSPI. Estos indicadores tienen como función rastrear el cumplimiento normativo, las tasas de incidentes de seguridad, la participación en capacitaciones de concienciación y la efectividad de los controles implementados. Ejemplos incluyen el porcentaje de cumplimiento de las políticas, el número de incidentes de seguridad por mes, el tiempo promedio de respuesta a incidentes, y el porcentaje de personal capacitado.

**Auditorías Internas y Revisiones por la Dirección**

Se realizarán auditorías internas regulares del MSPI para verificar su cumplimiento con las políticas establecidas y los requisitos del MinTIC. Estas auditorías serán complementadas con revisiones periódicas por parte de la dirección institucional. Estas actividades son esenciales para asegurar el

cumplimiento continuo, identificar áreas de mejora y mantener el compromiso del liderazgo con la seguridad de la información.

**Fase 5: Mejora Continua**

La seguridad de la información es un proceso dinámico que requiere una mejora constante.

**Mecanismos para No Conformidades y Acciones Correctivas**

Se implementará un proceso formal para identificar no conformidades con el MSPI, analizar la causa raíz de los incidentes o fallas, y diseñar e implementar acciones correctivas y preventivas eficaces. Esto asegurará que las lecciones aprendidas de los incidentes y auditorías se traduzcan en mejoras tangibles.

**Ciclo de Mejora Continua**

El ciclo PHVA (Planificar, Hacer, Verificar, Actuar) se integrará como la metodología fundamental para la gestión del MSPI, asegurando su adaptación y mejora continua en respuesta a las amenazas cambiantes, los avances tecnológicos y los cambios institucionales. Este enfoque iterativo reconoce que la seguridad de la información no es un proyecto puntual con una fecha de finalización, sino un proceso continuo y evolutivo. Esto implica que el Colegio Mayor de Antioquia necesita asignar recursos de manera continua para la capacitación, las actualizaciones tecnológicas y las auditorías regulares, fomentando una cultura de vigilancia y adaptación constantes.

Alcanzar niveles de madurez superiores (por ejemplo, más allá del "Nivel 3: debería ser un objetivo estratégico a largo plazo. Este modelo de madurez puede guiar futuras inversiones en ciberseguridad y la priorización de iniciativas, permitiendo a la institución medir su progreso de manera objetiva y planificar estratégicamente el desarrollo de capacidades de seguridad avanzadas. Por ejemplo, el paso del Nivel 3 (Administrado) a niveles superiores implicaría una mayor integración de la seguridad en el diseño de nuevos sistemas, la automatización de controles y una gestión de riesgos más predictiva.

**6. Gestión de Riesgos de Seguridad de la Información en el Entorno Universitario**

La gestión de riesgos es el pilar central del MSPI, permitiendo a la institución identificar, evaluar y mitigar proactivamente las amenazas a sus activos de información.

**Metodologías de Evaluación de Riesgos Aplicables.**

El MSPI del MinTIC hace referencia explícita al "Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas". Este modelo se integra con las fases de planificación e implementación del MSPI, proporcionando una guía detallada para la gestión de riesgos. Define conceptos clave como "Riesgo de Seguridad de la Información" como la posibilidad de que una amenaza explote una vulnerabilidad para causar daño a un activo de información, siendo una combinación de probabilidad y consecuencias. Además, enfatiza la importancia de identificar a los propietarios de los activos ya que, sin un dueño claro, nadie se hará responsable de su protección.

Otras metodologías reconocidas, como Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) e ISO/IEC 27005 (implícita por la alineación del MSPI con ISO 27001), son altamente relevantes y complementarias para un análisis detallado de riesgos en un contexto universitario. El proceso de gestión de riesgos implica varias actividades clave:

- **Identificación de activos:** Reconocer todos los elementos de valor que manejan información (hardware, software, datos, personas, servicios).
- **Identificación de amenazas:** Determinar qué puede provocar pérdidas a la institución, incluyendo amenazas y sus orígenes.
- **Identificación de vulnerabilidades:** Reconocer las debilidades en la tecnología, personas o procedimientos que pueden ser explotadas por las amenazas.
- **Identificación de controles existentes:** Evaluar las medidas de seguridad ya implementadas.
- **Valoración del riesgo:** Cuantificar el riesgo combinando el impacto del activo (Confidencialidad, Integridad, Disponibilidad - CID), el nivel de amenaza y el nivel de vulnerabilidad. La fórmula general para el nivel de riesgo es: Nivel de Riesgo = VA(CID) * Nivel de Amenaza * Nivel de Vulnerabilidad.

**Riesgos Específicos para Instituciones de Educación Superior**

Las universidades, por su naturaleza abierta y la diversidad de datos que manejan, enfrentan riesgos de seguridad de la información particulares:

- **Phishing y Ataques de Correo Electrónico:** Son una de las formas más comunes de ciberataques, donde los atacantes utilizan correos falsos para engañar a los destinatarios y robar información confidencial o instalar *malware*.
- **Malware y Ransomware:** Software malicioso que puede cifrar datos y exigir un rescate. Requieren soluciones antivirus robustas y copias de seguridad regulares para minimizar el impacto.
- **Ataques de Fuerza Bruta:** Intentos automatizados de adivinar contraseñas, lo que exige políticas de contraseñas fuertes y mecanismos de bloqueo de cuentas tras intentos fallidos.
- **Ataques a través de Dispositivos Móviles:** El creciente uso de dispositivos móviles aumenta la amenaza de aplicaciones maliciosas que pueden obtener acceso no autorizado a los sistemas universitarios o robar información. Se necesitan políticas de seguridad para dispositivos móviles y concienciación.
- **Uso de Redes Inseguras y Software Desactualizado/Pirata:** Gran parte de estudiantes, profesores y personal administrativo no siempre utilizan redes seguras para acceder a recursos institucionales, y el uso de software desactualizado o no licenciado aumenta la vulnerabilidad.
- **Protección de Datos de Investigación:** Los datos de investigación, especialmente la información sensible o propietaria generada en los campos de especialización del Colegio Mayor de Antioquia (turismo, gastronomía, ingeniería comercial [14]), requieren salvaguardas específicas para proteger la propiedad intelectual y la confidencialidad de los participantes.
- **Falta de Talento Humano Calificado:** Existe una brecha significativa de habilidades en ciberseguridad en América Latina, lo que afecta la capacidad de las instituciones para gestionar y responder eficazmente a las amenazas.

**Estrategias de Tratamiento de Riesgos.**

Una vez identificados y valorados los riesgos, se deben definir estrategias de tratamiento:

- **Reducción/Mitigación:** Implementación de controles para disminuir la probabilidad de ocurrencia o el impacto de un riesgo. Esto incluye la aplicación de autenticación multifactor, cifrado de datos, capacitación en concienciación sobre seguridad y el mantenimiento de software actualizado.
- **Aceptación:** Decisión consciente de aceptar un riesgo, generalmente cuando su impacto o probabilidad es bajo, o cuando el costo de mitigación supera el beneficio esperado.
- **Evitación:** Eliminación del riesgo al cesar la actividad que lo genera. Esta opción se considera cuando los riesgos son muy altos y los costos de los controles superan los beneficios.
- **Transferencia:** Trasladar el riesgo a un tercero, por ejemplo, a través de pólizas de seguros de ciberseguridad o mediante la subcontratación de servicios a proveedores especializados que asumen parte del riesgo.

Dada la prevalencia de ataques de *phishing*, ataques a dispositivos móviles y el uso de redes inseguras en las universidades, el plan de tratamiento de riesgos para el Colegio Mayor de Antioquia debe priorizar fuertemente los controles centrados en el factor humano. Esto significa una inversión significativa en programas continuos de concienciación sobre seguridad y la implementación de políticas de uso aceptable robustas, además de las salvaguardas técnicas. La evidencia demuestra que, a pesar de los avances tecnológicos, el eslabón más débil en la cadena de seguridad suele ser el usuario. Por lo tanto, la educación y el entrenamiento constante de toda la comunidad universitaria son tan críticos como la implementación de

*firewalls* o sistemas de detección de intrusiones.

Los datos de investigación, particularmente en campos especializados como el turismo, la gastronomía y la ingeniería comercial, representan un objetivo de alto valor para el robo de propiedad intelectual o el espionaje competitivo. A diferencia de los datos personales genéricos, que están protegidos por la Ley 1581, los datos de investigación pueden contener información propietaria, metodologías innovadoras o resultados con un valor comercial o estratégico significativo. Por lo tanto, el MSPI debe incluir controles específicos y mejorados para la confidencialidad e integridad de los datos de investigación. Esto podría requerir una clasificación de datos más granular, políticas de acceso separadas para proyectos de investigación, el uso obligatorio de cifrado para datos en reposo y en tránsito, la implementación de entornos de investigación seguros con acceso restringido y la aplicación de protocolos de acceso rigurosos para la propiedad intelectual.

**7. Protección de Datos Personales: Cumplimiento de la Ley 1581 y Decreto 1377**

El cumplimiento de la Ley 1581 de 2012 y el Decreto 1377 de 2013 es un componente ineludible del Modelo de Seguridad y Privacidad de la Información para el Colegio Mayor de Antioquia. La institución, como responsable del tratamiento de datos personales de su comunidad (estudiantes, docentes, personal administrativo, egresados, etc.), debe asegurar el respeto de los derechos de los titulares y la adecuada gestión de la información.

Los requisitos clave para el tratamiento de datos personales en el Colegio Mayor de Antioquia, en consonancia con la normativa, son los siguientes:

- **Autorización Previa e Informada:** Es imperativo obtener el consentimiento explícito, previo e informado de los titulares de los datos para cualquier operación de tratamiento de datos personales.[3] Esta autorización debe ser demostrable y se debe informar claramente el propósito y el alcance del tratamiento.
- **Finalidad Legítima:** Toda recolección, almacenamiento, uso o circulación de datos personales debe obedecer a un propósito legítimo y claramente definido, el cual debe ser comunicado al titular. Los datos solo pueden ser tratados durante el tiempo razonable y necesario para la finalidad.
- **Principios de Calidad y Veracidad:** La institución debe garantizar que los datos personales sean precisos, completos, actualizados, verificables y comprensibles, prohibiendo el tratamiento de datos parciales o que induzcan a error.
- **Seguridad y Confidencialidad:** Se deben implementar medidas técnicas, humanas y administrativas necesarias para proteger los datos personales de accesos no autorizados, pérdida, alteración o uso fraudulento. La confidencialidad debe mantenerse incluso después de que cese la relación con el tratamiento.
- **Políticas de Tratamiento de la Información:** El Colegio Mayor de Antioquia debe desarrollar y mantener políticas de tratamiento de la información claras y accesibles, que incluyan la identificación del responsable, la finalidad del tratamiento, los derechos de los titulares y los procedimientos para ejercerlos.
- **Aviso de Privacidad:** En los casos en que no sea posible poner a disposición las políticas completas al momento de la recolección, se debe utilizar un aviso de privacidad que contenga

la información mínima requerida, incluyendo cómo el titular puede acceder a la política completa.

- **Derechos de los Titulares:** La institución debe garantizar el pleno y efectivo ejercicio de los derechos de los titulares a conocer, actualizar, rectificar, suprimir sus datos y revocar la autorización. Se deben establecer mecanismos sencillos y gratuitos para la atención de consultas y reclamos.
- **Deberes de los responsables y Encargados:** El Colegio Mayor de Antioquia, como responsable del tratamiento, y cualquier tercero que actúe como encargado, deben cumplir con los deberes establecidos en la ley, como conservar la prueba de la autorización, garantizar la seguridad de la información, tramitar solicitudes y reportar incidentes de seguridad.
- **Datos de Menores de Edad:** Se debe asegurar el respeto a los derechos prevalentes de los niños, niñas y adolescentes. El tratamiento de sus datos personales está generalmente proscrito, salvo que sean de naturaleza pública y cumplan con el interés superior del menor y el respeto de sus derechos fundamentales. La autorización debe ser otorgada por el representante legal, valorando la madurez del menor.
- **Responsabilidad Demostrada:** La institución debe ser capaz de demostrar, a petición de la Superintendencia de Industria y Comercio, que ha implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 y el Decreto 1377, de manera proporcional a su naturaleza, tamaño, características de los datos y riesgos potenciales.
- **Transferencias y Transmisiones Internacionales:** Cualquier transferencia o transmisión de datos personales a otros países debe cumplir con los requisitos establecidos en la ley, especialmente la prohibición de transferencias a países que no proporcionen niveles adecuados de protección, salvo excepciones específicas.

**8. Conclusiones y Recomendaciones**.

**Síntesis de la Adaptación del MSPI.**

La elaboración de un Modelo de Seguridad y Privacidad de la Información (MSPI) adaptado para la Institución Universitaria Colegio Mayor de Antioquia, tomando como referencia el MSPI del Ministerio de las TIC colombiano, representa un paso estratégico fundamental para la institución. Este modelo proporciona un marco integral y sistemático para la gestión de los riesgos de seguridad y privacidad de la información, integrando los requisitos normativos de la Ley 1581 de 2012 y el Decreto 1377 de 2013, y personalizándolos para las particularidades del entorno universitario.[1]

La adaptación del MSPI reconoce la naturaleza única de una institución de educación superior, caracterizada por un entorno abierto, una gran y transitoria base de usuarios, y la gestión de datos de alto valor, como la propiedad intelectual de la investigación. Al aprovechar los planes y la experiencia existente del departamento de Gestión de Tecnología e Informática, el MSPI se convierte en una mejora e integración de procesos, no en una reformulación completa. La estructura del MSPI, basada en el ciclo PHVA (Diagnóstico, Planificación, Operación, Evaluación de Desempeño y Mejora Continua), asegura que la seguridad de la información sea un proceso dinámico y en constante evolución, capaz de adaptarse a las amenazas cambiantes y a los desarrollos institucionales.

**Recomendaciones Clave para la Implementación Exitosa**

Para asegurar una implementación exitosa y sostenible del MSPI en el Colegio Mayor de Antioquia, se formulan las siguientes recomendaciones clave:

1. **Liderazgo y Compromiso Continuo de la Alta Dirección:** El éxito del MSPI depende fundamentalmente del compromiso visible y continuo de la Rectoría, los Consejos y las Vicerrectorías.[5] Esto implica no solo la aprobación formal de políticas, sino también la asignación sostenida de recursos financieros, tecnológicos y humanos. La seguridad de la información debe ser vista como una inversión estratégica que protege la misión y la reputación de la institución, no como un mero costo.
2. **Fomento de una Cultura de Seguridad y Privacidad:** Dada la identificación del factor humano como una vulnerabilidad crítica [8], es imperativo priorizar programas continuos y obligatorios de concienciación y capacitación en seguridad y privacidad para toda la comunidad universitaria: estudiantes, profesores, personal administrativo y directivos. Estos programas deben ser interactivos, relevantes para sus roles y actualizados periódicamente para abordar las amenazas emergentes.
3. **Implementación de un Enfoque Basado en Riesgos Robusto e Iterativo:** La gestión de riesgos debe ser el motor del MSPI, con una metodología clara para la identificación, análisis, evaluación y tratamiento de riesgos. Se recomienda prestar especial atención a la protección de los datos de investigación, implementando controles mejorados como el cifrado y entornos de acceso restringido para salvaguardar la propiedad intelectual y la información sensible generada en las facultades especializadas. Este proceso debe ser iterativo, permitiendo la reevaluación y ajuste de los controles a medida que evolucionan las amenazas y el entorno institucional.

4. **Integración y Aprovechamiento de Procesos y Documentos Existentes:** En lugar de crear un sistema completamente nuevo, el MSPI debe integrarse y mejorar los planes y procedimientos de seguridad y privacidad ya existentes en el departamento de Gestión de Tecnología e Informática. Esto optimizará el uso de recursos, capitalizará la experiencia interna y facilitará una transición más fluida hacia el nuevo modelo.
5. **Establecimiento de un Marco de Monitoreo y Mejora Continua:** Se deben definir indicadores clave de rendimiento (KPIs) claros y medibles para evaluar la efectividad y eficiencia del MSPI. La realización de auditorías internas periódicas y revisiones por la dirección es fundamental para identificar no conformidades, analizar causas raíz y aplicar acciones correctivas y preventivas oportunas. Este ciclo de verificación y actuación es esencial para la adaptación constante del modelo a un panorama de amenazas dinámico.
6. **Gobernanza de Datos Distribuida con Responsabilidades Claras:** Dada la dispersión de activos de información en una universidad con diversas facultades y departamentos, es crucial establecer un marco de gobernanza que defina claramente los "propietarios" de los activos de información. Estos propietarios deben ser empoderados y responsabilizados por la seguridad y privacidad de sus datos, bajo la coordinación central del Líder de Seguridad de la Información y el departamento de Gestión de Tecnología e Informática. Esto asegura que la seguridad sea una responsabilidad compartida en toda la organización.



*Obras citadas*

1. Política de Protección de Datos Personales -, fecha de acceso: julio 1, 2025, https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/
2. Decreto 1377 de 2013 - Biblioteca Digital CCB, fecha de acceso: julio 1, 2025, https://bibliotecadigital.ccb.org.co/items/9d7cd427-3a10-4dd8-b45b-a5780dcc616f
3. LEY ESTATUTARIA 1581 DE 2012 (octubre 17) Reglamentada ..., fecha de acceso: julio 1, 2025, https://esdegue.edu.co/sites/default/files/Normatividad/LEY%20TRATAMIENTO%20DE%20DATOS%20-%20LEY%201581%20DE%202012.pdf

4. Decreto 1377 de 2013 - Gestor Normativo - Función Pública, fecha de acceso: julio 1, 2025, https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646
5. IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) EN EL INVÍAS – VIGENCIA 2024 1. INTRODUCCIÓN., fecha de acceso: julio 1, 2025, https://www.invias.gov.co/index.php/archivo-y-documentos/hechos-de-transparencia/16731-implementacion-modelo-de-seguridad-y-privacidad-de-la-informacion-mspi-2024/file
6. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - Agencia de Desarrollo Rural, fecha de acceso: julio 1, 2025, https://www.adr.gov.co/wp-content/uploads/2021/07/Plan-de-Seguridad-y-Privacidad-de-la-Informacio%CC%81n_Comite_24082020.pdf
7. Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe, fecha de acceso: julio 1, 2025, https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf
8. Seguridad de los datos en las universidades - Vínculo TIC, fecha de acceso: julio 1, 2025, https://vinculotic.com/educacion/seguridad-datos-universidades/
9. Principales amenazas de ciberseguridad que enfrentan las Universidades de Latinoamérica hoy en día - BEXTechnology, fecha de acceso: julio 1, 2025, https://www.bextsa.com/blog-actualidad/principales-amenazas-de-ciberseguridad-que-enfrentan-las-universidades-de-latinoamerica-hoy-en-d%C3%ADa
10. MSPI - Gobierno digital - MinTIC, fecha de acceso: julio 1, 2025, https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/
11. Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información - Gobierno digital - MinTIC, fecha de acceso: julio 1, 2025, https://gobiernodigital.mintic.gov.co/692/articles-401770_recurso_1.pdf
12. Organigrama institucional - Colegio Mayor de Antioquia, fecha de acceso: julio 1, 2025, https://www.colmayor.edu.co/institucional/micolmayor/organigrama-institucional/
13. Mapa de procesos - Colegio Mayor de Antioquia, fecha de acceso: julio 1, 2025, https://www.colmayor.edu.co/institucional/mapa-de-procesos/
14. Facultad de Administración - Colegio Mayor de Antioquia, fecha de acceso: julio 1, 2025, https://www.colmayor.edu.co/facultad-de-administracion/
15. Ciberseguridad en instituciones de educación superior: un análisis desde la perspectiva de la teoría de la motivación de pro - REDIECH, fecha de acceso: julio 1, 2025, https://www.rediech.org/ojs/2017/index.php/ie_rie_rediech/article/download/2271/2212
16. Modelo de Seguridad y Privacidad de la Información - DIAN, fecha de acceso: julio 1, 2025, https://www.dian.gov.co/atencionciudadano/LMDP/Informacion-Innovacion-y-Tecnologia/Seguridad-de-la-Informacion/Otros-Documentos/OD-IIT-0001.pdf
17. Untitled - Umayor, fecha de acceso: julio 1, 2025,

https://umayor.edu.co/files/tecnologia/MSPI.pdf
18. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI - Alcaldía de Cajicá, fecha de acceso: julio 1, 2025, https://www.cajica.gov.co/docdown/archi/2022/Instructivo/MODELO%20DE%20SEGURIDAD%20Y%20PRIVACIDAD%20DE%20LA%20INFORMACION-%20MSPI%202022%20.pdf
19. MNGRSI - Gobierno digital - MinTIC, fecha de acceso: julio 1, 2025, https://gobiernodigital.mintic.gov.co/692/articles-237907_maestro_mspi.pdf
20. Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - Gobierno digital - MinTIC, fecha de acceso: julio 1, 2025, https://gobiernodigital.mintic.gov.co/portal/Biblioteca/237907:Modelo-Nacional-de-Gestion-de-Riesgo-de-Seguridad-de-la-Informacion-en-Entidades-Publicas
21. Protección de datos personales | MINCIT - Ministerio de Comercio, Industria y Turismo, fecha de acceso: julio 1, 2025, https://www.mincit.gov.co/minindustria/estrategia-transversal/regulacion/proteccion-de-datos-personales
22. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO DECRETO NÚMERO DE 2012 () - MinTIC, fecha de acceso: julio 1, 2025, https://mintic.gov.co/images/documentos/documentos_comentarios/proyecto_decreto_ley_1581_de_2012_proteccion_datos.pdf
23. Protección de Datos Personales - Ministerio de Educación Nacional, fecha de acceso: julio 1, 2025, https://www.mineducacion.gov.co/portal/micrositios-institucionales/Modelo-Integrado-de-Planeacion-y-Gestion/Data/387771:Proteccion-de-Datos-Personales
24. Decreto 1377 de 2013 Nivel Nacional - Secretaría General de la Alcaldía Mayor de Bogotá, fecha de acceso: julio 1, 2025, https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646
25. Universidad de Antioquia - Wikipedia, la enciclopedia libre, fecha de acceso: julio 1, 2025, https://es.wikipedia.org/wiki/Universidad_de_Antioquia
26. Gestión de Tecnología e informática - Colegio Mayor de Antioquia, fecha de acceso: julio 1, 2025, https://www.colmayor.edu.co/institucional/micolmayor/gestion-de-tecnologia-e-informatica/
27. GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN - Gobierno Electrónico, fecha de acceso: julio 1, 2025, https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf
28. MANUAL DE POLÍTICAS Y GUÍA DE SEGURIDAD DE INFORMÁTICA PARA LAS Y LOS USUARIOS DE LA UNIVERSIDAD INTERCULTURAL DEL ESTADO DE - Periódico Oficial Gaceta del Gobierno y LEGISTEL, fecha de acceso: julio 1, 2025, https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/gct/2021/agosto/ago251/ago251b.pdf

29. GUÍA METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN - Gobernación de Nariño, fecha de acceso: julio 1, 2025, https://narino.gov.co/wp-content/uploads/2025/01/ANEXO-1.-GUIA-METODOLOGIA-GESTION-DEL-RIESGO-DE-SEGURIDAD-DE-LA-INFORMACION.pdf
30. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método - CCN-CERT, fecha de acceso: julio 1, 2025, https://www.ccn-cert.cni.es/es/documentos-publicos/1789-magerit-libro-i-metodo/file?format=html
31. Política de Seguridad de la Información para la Universidad Nacional de Córdoba, fecha de acceso: julio 1, 2025, https://www.unc.edu.ar/sites/default/files/PoliticadeSeguridad08.pdf
32. Protección de datos - Universidad Piloto de Colombia, fecha de acceso: julio 1, 2025, https://www.unipiloto.edu.co/proteccion-de-datos/
33. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025 - Gobernación de Antioquia, fecha de acceso: julio 1, 2025, https://antioquia.gov.co/images/PDF2/Transparencia/2025/01/plan-de-tratamiento-de-riesgos-de-seguridad-y-privacidad-informacion-gob-22012025-v1.pdf
34. Protección de Datos Personales - U Cundinamarca, fecha de acceso: julio 1, 2025, https://www.ucundinamarca.edu.co/index.php/proteccion-de-datos-personales