INSTITUCIÓN UNIVERSITARIA
MAYOR DE CARTAGENA

AVANZA
HACIA LA EXCELENCIA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Contenido

1. INTRODUCCION

El Plan de seguridad de la información constituye una parte fundamental del Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno Digital y se convierte en la base para la implementación de los controles, procedimientos y estándares definidos.

En la actualidad, la información se considera uno de los activos más valiosos y esenci ales para cualquier organización. La Institución Universitaria Mayor de Cartagena (UNI MAYOR) no es la excepción. La gestión adecuada de la información es fundamental p ara asegurar su confidencialidad, integridad, disponibilidad y privacidad.

El Desarrollo de este plan está basado en el Modelo de Seguridad y Privacidad de la Información expuesto por el Ministerio de la Tecnologías de la Información y las Comunicaciones, el cual recopila las mejores prácticas para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo. Lo anterior teniendo en cuenta las necesidades, objetivos, los requisitos de seguridad y los procesos misionales en la INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA. De esta forma estamos dando cumplimiento al decreto único reglamentario 1078 de 2015 en el componente de seguridad y privacidad de la Información como parte integral de la estrategia de Gobierno Digital.

2. MARCO LEGAL

NORMA	DESCRIPCIÓN
Decreto1078de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
NTC/ISO27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
NTC/ISO 27002:2013	Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.

3. ALCANCE

El presente Plan de Seguridad y Privacidad de la Información se aplica a toda la información gestionada por la Institución Universitaria Mayor de Cartagena **UMA YOR**, abarcando tanto datos digitales como físicos. Este plan es relevante para todas las áreas y departamentos de la institución, así como para todos los miem bros de la comunidad universitaria, incluyendo directivos, docentes, estudiantes, personal administrativo y cualquier tercero que tenga acceso a la información de **UMAYOR.**

EL ALCANCE DE ESTE PLAN INCLUYE:

- **Protección de la Información**: Establecer medidas de seguridad para as egurar la confidencialidad, integridad y disponibilidad de la información.
- **Cumplimiento Normativo**: Asegurar el cumplimiento de leyes y regulacio nes locales e internacionales relacionadas con la seguridad y privacidad d e la información.
- **Gestión de Riesgos**: Identificar y mitigar riesgos asociados con la gestió n de la información.
- **Capacitación y Concienciación**: Proveer formación continua y programa s de concienciación para todos los miembros de la comunidad universitari a.
- **Respuestas a Incidentes**: Definir procedimientos para la gestión de incid entes de seguridad y la recuperación ante desastres.

4. DIRECCIONAMIENTO ESTRATÉGICO

MISIÓN

Somos, desde el Caribe colombiano, una institución universitaria de carácter público, que asume la formación de ciudadanos integrales como un proyecto de trasformación humana y social, consecuente con las necesidades del entorno y el desarrollo sostenible, con perspectiva y proyección internacional.

VISIÓN

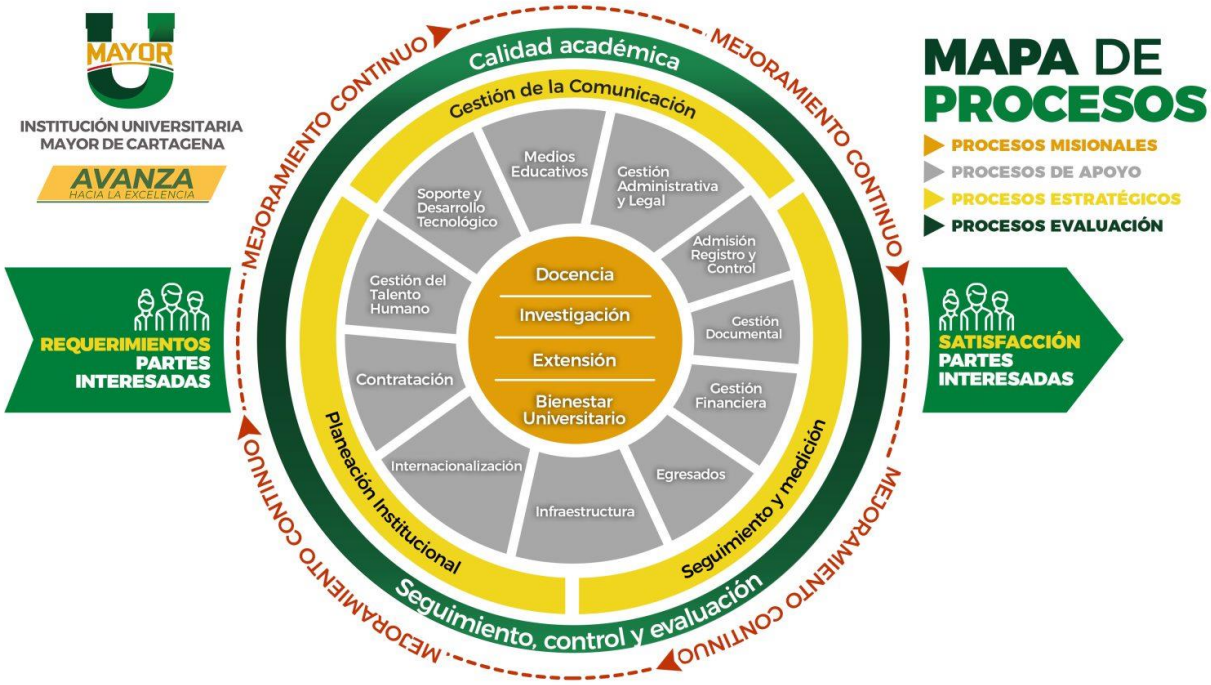
Ser reconocida a 2033, en el marco de los 500 años de Cartagena, como una institución universitaria de alta calidad, proyectada a la comunidad a través de la excelencia e integralidad de sus egresados, del compromiso con el desarrollo sostenible y del aporte al desarrollo económico y social en el contexto local, nacional e internacional.

5. POLÍTICA SISTEMA INTEGRADO DE GESTIÓN

La Institución Universitaria mayor de Cartagena reestructuró e implementó el Sistema Integrado de Gestión –SIG – con el propósito de mejorar su desempeño y su capacidad de proporcionar productos y servicios que respondan a las necesidades y expectativas de sus estudiantes y partes interesadas.

Cartagena de Indias - Centro Histórico
K3 # 36-95 Calle de la Factoría
umayorctg

6. MAPA DE PROCESOS



7. TÉRMINOS Y DEFINICIONES

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultadque tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de Información:** cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de UMAYOR y, en consecuencia, debe ser protegido. Se refiere al activo que contiene información publica que el sujeto obligado genere, obtenga, adquiera, transforme o controle.
- **Amenaza:** es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los elementos de información. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de riesgos de seguridad de la información:** proceso sistemático de identificación de fuentes, estimación de impactos, probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.
- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soportematerial, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como lainstitución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

- **Autenticación:** es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar acabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales software, redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.
- **Confidencialidad:** es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguardar o contramedida. En una definición más simple, es una medida que modifica el riesgo
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o

reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3)

- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contienedatos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación,tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición,
  así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. Decreto 1377 de 2013, art 3
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural Jurisprudencia Corte Constitucional.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012)
- **Disponibilidad:** es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública oprivada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3).
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar,reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada:** Es aquella información que estando en poder ocustodia de un sujeto obligado en su calidad de tal, pertenece al

ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de losrequisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014,art 6).
- **Integridad:** es la protección de la exactitud y estado completo de los activos de información.
- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anónimos o cifrado.
- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del manual de la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Propietarios de los activos de información:** son los responsables de cada uno de los activos de información (archivos, bases de datos, contratos y acuerdos, documentación del sistema, manuales de usuario, material de formación, aplicaciones, software del sistema, equipos informáticos, equipos de comunicaciones, servicios informáticos y de comunicaciones, las personas, etc. Esta persona se hará cargo de mantener la seguridad del activo.
- **Recursos tecnológicos:** son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información.
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos yrecursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.
- **Sistema de información (SI)**: es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo. Dichos elementos pueden ser personas, actividades o técnicas de trabajo, datos y recursos materiales en general

- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento.
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

8. OBJETIVO GENERAL

Establecer las políticas de seguridad de la información para la institución universitaria mayor de Cartagena, con el fin de cumplir con los requisitos de seguridad, definidos en el MSPI que ayudarán, mediante su implementación, a preservar la Confidencialidad, Integridad y Disponibilidad de la información. De acuerdo a los lineamientos de buenas prácticas en Seguridad y Privacidad para las entidades del Estado, con el fin de regular la gestión de la seguridad de la información al interior de la entidad.

9. PARTES INTERESADAS

Todos los funcionarios, contratistas, proveedores, entes de control, entidades gubernamentales del orden nacional, departamental y local, y ciudadanía en general que accedan a los sistemas de información e instalaciones físicas de la Administración Municipal.

10. ESQUEMA DEL PLAN

El Plan de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la **INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA** con respecto a la protección de los activos de información que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

11. DESARROLLO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La **INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA**, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y las acciones a implementar son:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el modelo de seguridad y privacidad de la información **(MSPI)**.
- Diligenciamiento de instrumento
- Proteger los activos de información.
- Establecer, e implementar las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, practicantes y ciudadanía en general.
- Garantizar la continuidad de los procesos frente a incidentes.

La Política de Seguridad que soportan el SGSI, considera los siguientes aspectos:

- La **INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA**, ha decidido **definir, implementar,operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de **UMAYOR**, y a los requerimientos regulatorios que le aplican a su naturaleza.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados y proveedores de la comunidad **UMAYOR**.

- La institución universitaria mayor de Cartagena protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- Protegerá su información de las amenazas originadas por parte del personal.

- Protegerá las instalaciones de procesamiento y la infraestructura tecnológicaque soporta sus procesos críticos.

- Controlará la operación de los procesos de **LA INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA** garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- Implementará control de acceso a la información, sistemas y recursos dered.

- Garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- Garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- Garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

12. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Entregable	Responsable de actividad	Actividad	Periodicidad
Usuario- Clave	Desarrollo y soporte Tecnológico	Creación, activación e inactivaciónde usuarios	A solicitud del área de Talento Humano
Contratos	Desarrollo y soporte Tecnológico	Renovación de licenciamiento	Anual
Backups o copias de seguridad	Desarrollo y soporte Tecnológico	Realizar backups diarios automatizados por herramienta Google Drive, realizar Backups a servidores de una manera programada.	Diario y eventos programados
Evidencia del seguimiento	Desarrollo y soporte Tecnológico	Configuración y seguimiento a la Seguridad perimetral y consola antivirus.	Diariamente
Desarrollo o actualización de sistemas de información	Desarrollo y soporte Tecnológico	Implementación o actualización de sistemas de información	A solicitud de requerimiento
Plan de Mantenimiento preventivo Informe de la mesade ayuda	Desarrollo y soporte Tecnológico	Mantenimiento preventivo y/o correctivo a equipos de cómputo y demás elementos tecnológicos	Evento programado, teniendo en cuenta el cronograma de mtto.

13. SEGUIMIENTO DEL PLAN

- Desde el área de Talento Humano se informará al Departamento de soporte y desarrollo tecnológico de la institución universitaria mayor de Cartagena acerca de las novedades de ingreso, retiro temporal o definitivo del personal que labora en la entidad, con el fin de asignar o eliminar los usuarios de red y sus respectivos permisos de acceso a la información. De igual manera, impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.

- En cuanto al Software, se garantiza la continuidad de los aplicativos que requieren renovación anual, con el fin de tener el licenciamiento legal y vigente.

- Programar y realizar mantenimientos periódicos preventivos a los equipos de cómputo y demás elementos tecnológicos de la entidad, así como los mantenimientos correctivos a los que haya lugar.

- Restringir los permisos de instalación, cambio o eliminación de aplicativos, fondos de pantallas que no sean de identidad **UMAYOR**, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica.

Este seguimiento se hace a través de reportes generados por la plataforma de seguridad perimetral y consola antivirus.

- Generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores, cuando es solicitado a través de la mesa de ayuda o solicitud realizada desde el área de Talento Humano

- Monitorear constantemente los aplicativos de seguridad de la información, Fortinet y Antivirus, con el fin de detectar y corregir cualquier anomalía en nuestros sistemas de información.

- Garantizar la disponibilidad de la red de datos, realizando control de tráfico y estableciendo políticas que garanticen la integridad y confidencialidad de la información.