INSTITUCIÓN UNIVERSITARIA
MAYOR DE CARTAGENA

AVANZA
HACIA LA EXCELENCIA

MSPI
2022 - 2026

MODELO DE SEGURIDAD
Y PRIVACIDAD DE LA INFORMACIÓN

2022 - 2026

Cartagena de Indias - Centro Histórico
Cra3 # 36-95 Calle de la Factoría.
www.umayor.edu.co

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Institución Universitaria Mayor de Cartagena, consciente de los desafíos actuales en materia de seguridad y privacidad de la información en el entorno digital, reconoce la importancia de salvaguardar sus activos de información para garantizar el funcionamiento eficiente de sus servicios y el resguardo de la confianza de la comunidad universitaria y la sociedad en general. En línea con esta premisa, la institución ha adoptado el Modelo de Seguridad y Privacidad de la Información (MSPI) promovido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

El MSPI se erige como un marco estratégico integral que permite a UMAYOR establecer y operar un Sistema de Gestión de Seguridad de la Información (SGSI) y seguridad digital. Este sistema, fundamentado en el ciclo PHVA (Planear, Hacer, Verificar y Actuar), se estructura en cinco fases, cada una diseñada para abordar aspectos clave en la gestión de la seguridad y privacidad de la información:

Diagnóstico: Inicia el proceso mediante la identificación del estado actual de la institución en relación con la adopción del MSPI, proporcionando un análisis GAP como base para la planificación y la mejora continua.

Planificación: Define las necesidades y objetivos de seguridad y privacidad de la información, considerando el contexto interno y externo de UMAYOR, así como su mapa de procesos. Esta fase destaca la elaboración del plan de valoración y tratamiento de riesgos como elemento central del proceso.

Operación: Implica la implementación de controles destinados a mitigar el impacto o la probabilidad de ocurrencia de los riesgos identificados en la etapa de planificación.

Evaluación de desempeño: Establece los criterios para evaluar la adopción efectiva del modelo, permitiendo a UMAYOR monitorear y medir su progreso en términos de seguridad y privacidad de la información.

Mejoramiento Continuo: Define procedimientos para identificar desviaciones en las normas establecidas en el modelo y para tomar las acciones correctivas necesarias, asegurando así un proceso de mejora continua en la gestión de la seguridad y privacidad de la información.
Mediante la implementación del MSPI, UMAYOR busca fortalecer su capacidad para gestionar y proteger adecuadamente sus activos de información, asegurando la

continuidad de sus operaciones y el cumplimiento de las expectativas de seguridad y privacidad de la comunidad universitaria y demás partes interesadas.

2. OBJETIVO GENERAL

El objetivo de un modelo de seguridad y privacidad de la información es garantizar la protección adecuada de los datos sensibles y confidenciales de la INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA, así como de los sistemas que los procesan, al tiempo que se preserva la integridad, la disponibilidad y la confidencialidad de la información.

Un modelo de seguridad y privacidad de la información busca establecer un marco integral de controles y procesos para proteger la información de manera efectiva, minimizando los riesgos de exposición, pérdida o compromiso de datos sensibles.

3. OBJETIVOS ESPECÍFICOS

1: Consolidar los procesos pedagógicos desarrollados dentro de la institución mediante evaluación, control y mejoramiento continuo en la calidad de los servicios ofrecidos a la comunidad educativa

2: Incrementar el nivel de impacto en la comunidad educativa a nivel local y regional mediante la formulación de proyectos de investigación en ciencia, tecnología e innovación que permitan la construcción de nuevo conocimiento

3: Fortalecer el sistema de seguimiento a egresados mediante la actualización constante de base de datos, identificación de la situación laboral actual y el impacto social en el mercado laboral como herramienta de monitoreo de la oferta académica institucional

4: Fortalecer de manera integral los mecanismos de participación docentes y estudiantil con el fin de mejorar los procesos democráticos de la institución

5: Mejorar la calidad del cuerpo docente en aras de la formación integral de nuestros estudiantes

6: Ofertar programas académicos de calidad con factores innovadores, incluyentes y flexibles que permitan la formación integral de la ciudadanía, comprometida con el medio ambiente, derechos humanos y valores éticos

7: Generar impactos positivos y sostenible en las personas comunidades y organizaciones a través de soluciones enfocadas a problemas sociales concretos

8: Garantizar una mejora significativa en las condiciones laborales, salariales, de bienestar y mejora de incentivos

9: Desarrollar programas para promover la formación integral desde la cultura, la salud física, salud mental, el deporte y el desarrollo humano

4. ALCANCE DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Con la implementación de este modelo en UMAYOR es garantizar la protección adecuada de los datos sensibles y confidenciales dentro de la organización, establecimiento en cada área controles de seguridad teniendo en cuenta los siguientes aspectos

USUARIOS Y ROLES: en UMAYOR se tiene especificado los usuarios que están sujetos a las políticas, controles de seguridad y privacidad.

ÁREAS Y DEPARTAMENTOS

Todas las áreas están cubiertas por el modelo, las cuales tendrán control total de la información sensible que se lleve dentro de las mismas.

RIESGOS Y AMENAZAS:

Analizar los riesgos y las amenazas que está expuesta la información y los sistemas de la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA, así como las posibles consecuencias de una brecha de seguridad o violación de privacidad.

CONTROLES DE SEGURIDAD Y PRIVACIDAD

Los modelos, controles y medidas de seguridad que se implementaran para proteger la información y los sistemas contra las amenazas identificadas, políticas de acceso, cifrado, autenticación y auditorias en UMAYOR.

Este modelo de seguridad y privacidad de la información define el ámbito y las áreas específicas que se abordarán para garantizar la protección adecuada de los datos sensibles y confidenciales dentro de UMAYOR

5. LÍMITES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Identificar y abordar estos límites con la finalidad de mejorar la resiliencia y robustez de los programas de seguridad y privacidad de la información, protegiendo así los datos sensibles y confidenciales de manera efectiva en la entidad UMAYOR. Los límites más comunes incluyen

FACTORES HUMANOS: en UMAYOR se concientiza a los empleados de los errores humanos, como la falta de conciencia de seguridad, negligencia o el comportamiento malicioso de los empleados, esto con el fin de minimizar los antes mencionados.

TECNOLOGÍA OBSOLETA O INADECUADA: UMAYOR dispone de software de seguridad actualizado, controles de seguridad para disminuir los riesgos de vulnerabilidad en los sistemas de la institución, cuentan con la última actualización de seguridad para optimizar la seguridad.

6. IDENTIDAD DE UMAYOR

La Institución Universitaria Mayor de Cartagena, con sede en la ciudad de Cartagena de Indias, recibió la categoría de establecimiento público del orden nacional por medio del decreto 758 de 1988. Es actualmente un organismo con Personería Jurídica, autonomía administrativa y patrimonio independiente, adscrito al Ministerio de Educación nacional.

Por ser un establecimiento público, su desarrollo ha estado orientado por la normatividad colombiana. Así se inicia con la Ley 48 de 1945 que autorizó la apertura de instituciones de educación superior femenina iniciando labores en marzo de 1947. El decreto 257 de 1970 elevó el nivel de estudios de los Colegios Mayores al de educación superior y los puso bajo la supervisión del Instituto Colombiano para el Fomento de la Educación Superior ICFES, ofreciendo la titulación de expertas.

Más tarde, la Ley 80 de 1980, dio base para la transformación en institución tecnológica y con la Ley 83 de 1980 el Colegio logró esta transformación iniciando nuevos ajustes y revisiones curriculares que finalmente culminaron con la aprobación de todos los programas ante el ICFES.

La Ley 24 de 1988, convirtió en establecimientos públicos oficiales a los Colegios mayores e instituciones técnicas y tecnológicas, con todas las exigencias de orden administrativo y presupuestal, condición requerida para transformarse en un ente autónomo, modificando su condición de unidad especial adscrita al Ministerio de Educación nacional. Esto permitió la reforma de los estatutos y la estructura, los cuales fueron aprobados por el Consejo Directivo mediante los Acuerdos 01 de 1988 y 07 de 1989 respectivamente y luego ratificados por el Gobierno nacional mediante los Decretos 1095 y 1127 de 1989.

7. GLOSARIO

ACCIÓN CORRECTIVA: Conjunto de acciones tomadas para eliminar la (s) causa (s) de una no conformidad detectada u otra situación no deseable.

ACCIÓN PREVENTIVA: Conjunto de acciones tomadas para eliminar la (s) causa (s) de una no conformidad potencial u otra situación potencial no deseable.

ACREDITACIÓN: Es un testimonio que da el Estado sobre la calidad de un programa o institución académica con base en un proceso de evaluación en el cual intervienen la institución, las comunidades académicas y el Consejo Nacional de Acreditación.

Por lo tanto, es un acto de reconocimiento público de una institución o de sus programas académicos en tanto cumplan ciertas condiciones y estándares generales de excelencia establecidos como producto de su Autoevaluación.

ADMITIDO: Persona que obtuvo el puntaje exigido en las pruebas aplicadas por la institución.

ADQUISICIÓN DE BIENES Y SERVICIOS: Cualquier modalidad de contratación, convenio, concesión, o provisión de bienes y/o servicios, inherentes al cumplimiento de la función de la entidad.

ALTA DIRECCIÓN: Persona o grupo de personas, del máximo nivel jerárquico que dirigen o controlan la entidad.

ASPIRANTE: Persona que solicita ingreso formalmente a un programa académico.

AUDITORÍA INTERNA: Proceso sistemático, independiente y documentado para obtener evidencias que, al evaluarse de manera objetiva, permiten determinar la conformidad del Sistema de Gestión de la Calidad con los requisitos establecidos y que se ha implementado y se mantiene de manera eficaz, eficiente y efectiva.

AUTOEVALUACIÓN: La Autoevaluación se ha definido como un proceso permanente y participativo, mediante el cual la institución obtiene, registra y analiza información útil, confiable y apropiada, para la identificación de aciertos y debilidades en función de una toma de decisiones eficientes que contribuyen a la efectividad de los procesos de planeación y cambio para lograr el desarrollo institucional.

COBERTURA: Estrategia que se concreta en el proceso de matrícula y asignación de cupos. Porcentaje de alumnos en un ciclo educativo o en todo el sistema, calculado respecto al número de personas en edad de estudiar dicho ciclo.

CALIDAD: Se define calidad como las políticas, los sistemas y los procesos que apuntan a asegurar la preservación y el mejoramiento de la calidad de los productos de la educación propuestos por una institución.
– Grado en el que un conjunto de características inherentes cumplen con los requisitos.
-El concepto de calidad aplicado al servicio público de la Educación Superior, hace referencia a la síntesis de características que permiten reconocer un programa académico específico o una institución de determinado tipo y hacer un juicio sobre la distancia relativa sobre el modo como en esa institución o en ese programa académico se presta dicho servicio y el óptimo que corresponde a su naturaleza.

CARACTERÍSTICAS: Atributos que pueden adquirir diferentes magnitudes y valores. Son definidos por la institución de acuerdo con su naturaleza e intereses particulares. Están representadas en 8 factores y 53 características de cualidades agrupadas

CLIENTE: Organización, entidad o persona que recibe un producto y/o servicio.

COMITÉ CENTRAL DE AUTOEVALUACIÓN: Es la máxima autoridad de la institución que traza los lineamientos concernientes al proceso de Autoevaluación institucional.

COMITÉ OPERATIVO DE AUTOEVALUACIÓN: Es responsable de implementar y operacionalizar las acciones del proceso de Autoevaluación dispuestas por el Comité Central

CNA: Consejo Nacional de Acreditación.

CONCESIÓN: Autorización para utilizar o liberar un producto y/o servicio que no es conforme con los requisitos especificados.

CONFORMIDAD: Cumplimiento de un requisito.

CONTROL DE CALIDAD: Parte de la gestión de la calidad orientada a la verificación y al cumplimiento de los requisitos de la calidad.

CONVENIENCIA: Grado de alineación o coherencia del objetivo de revisión con las metas y políticas organizacionales.

CORRECCIÓN: Acción tomada para eliminar una no conformidad detectada.

DESERCIÓN: Proceso de abandono, voluntario o forzoso, del programa académico en el que se matriculó un estudiante. Este fenómeno obedece a causas, internas y externas, que involucran factores personales, familiares, socioeconómicos, culturales e institucionales. Se relaciona también con aspectos como el ausentismo, el retiro forzoso y la repitencia, la cual, cuando es recurrente, conduce al abandono definitivo de los estudios.

DISEÑO Y DESARROLLO: Conjunto de procesos que transforma los requisitos de una política, programa, proyecto o cliente en características especificadas o en la especificación de un proceso o sistema, producto y/o servicio.

EFECTIVIDAD: Medida del impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles.

EFICACIA: Grado en el que se realizan las actividades planificadas y se alcanzan los resultados planificados.

EFICIENCIA: Relación entre el resultado alcanzado y los recursos utilizados.

ENFOQUE BASADO EN PROCESOS: Gestión sistemática de la interacción e interrelación entre los procesos empleados por las entidades para lograr un resultado deseado.

EQUIPO DE MEDICIÓN: Instrumento. Software, patrón, material de referencia o equipos auxiliares, o combinación de ellos necesarios para llevar a cabo un proceso de medición.

ESPECIFICACIÓN: Documento que establece requisitos.

ESTRUCTURA DE LA ENTIDAD: Distribución de las diferentes unidades o dependencias con sus correspondientes funciones generales, requeridas para cumplir la función de la entidad dentro del marco de la Constitución y la Ley.

ESTUDIANTE: Persona que ha sido admitido en alguno de los programas académicos que ofrece una institución y que se matricula cumpliendo con los requisitos que se establecen.

EVALUACIÓN: Proceso cuyo objetivo es la realización de un estudio de una institución o programa, que concluye con la emisión de un juicio o diagnóstico, tras el análisis de sus componentes, funciones, procesos y resultados, para posibles cambios de mejora. Una evaluación incluye la recopilación sistemática de datos y estadísticas relativos a la calidad de la institución o del programa. Las agencias de calidad suelen dividir su actuación en dos tareas relacionadas: la evaluación y la acreditación (RIACES, 2007).

EVALUACIÓN INSTITUCIONAL: Supone el examen integral de la organización entera: abarca la misión y el proyecto institucional; la comunidad académica (estudiantes, profesores e investigadores); los procesos académicos (docencia, investigación, extensión o proyección social); el bienestar institucional; la pertinencia y el impacto social; los procesos de autoevaluación y autorregulación; la organización, la administración y la gestión; la planta física y los recursos de apoyo académico; los recursos financieros.

EVALUACIÓN EXTERNA O EVALUACIÓN POR PARES: Utiliza como punto de partida la autoevaluación, verifica sus resultados, identifica las condiciones internas de operación de la institución o de los programas y concluye en un juicio sobre la calidad de una u otros.

EVALUACIÓN FINAL: Que realiza el Consejo Nacional de Acreditación a partir de los resultados de la autoevaluación y de la evaluación externa.

EVALUACIÓN DEL CNA: Estará centrada en el análisis de la eficacia y eficiencia del trabajo realizado para llevar a cabo los fines y propósitos para el cumplimiento de la misión establecida por Ley.

EVALUACIÓN DE LA CALIDAD: Correspondiente a la acreditación institucional se centra en el cumplimiento de los objetivos de la educación superior que incluyen naturalmente, como elementos universales, la formación integral, la creación, el desarrollo y la transmisión del conocimiento y la contribución a la formación de profesionales y consolidación de las comunidades académicas. Se centra, además, en el logro de los postulados de las misiones y proyectos institucionales y en la pertinencia social, cultural y pedagógica de esas misiones y proyectos; además, atiende a la manera como la institución afronta el cumplimiento de sus funciones básicas en los distintos campos de acción de la educación superior, al clima institucional, a los recursos con que cuenta y a su desempeño global. Cuando se habla de instituciones resulta necesario enfatizar el vínculo entre pertinencia y calidad: a la exigencia académica sobre la calidad de los programas, que también resulta ser esencial cuando se juzga sobre la institución como un todo, se añade, en este caso, una exigencia particular relacionada con su papel social.

EVALUACIÓN PARA LA ACREDITACIÓN: Es la que hace la institución siguiendo un Modelo de Autoevaluación y los lineamientos de Consejo Nacional Acreditación y tiene como fin lograr la acreditación de un programa o una institución.

EVALUACIÓN PARA LA MEJORA: Es el proceso de evaluación permanente que realiza internamente la institución con el fin de no perder de vista todos sus procesos y propender por mejorar la calidad de la institución.

GESTIÓN: Actividades coordinadas para planificar, controlar, asegurar y mejorar la entidad.

GESTIÓN DOCUMENTAL: Conjunto de actividades administrativas y técnicas tendientes a la planificación, manejo y organización de la documentación producida y revisada por las entidades, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación.

HABILIDAD: Capacidad para aplicar apropiadamente atributos o comportamientos personales para desempeñar una actividad.

INDICADORES: Referentes empíricos de las variables posibles, valores de desempeño o comportamiento de las variables de la dinámica cotidiana, pueden ser cualitativos y cuantitativos.

INDUCCIÓN: Jornada de apertura e introducción a los estudiantes de primer semestre de lo que es el sistema educativo que se lleva en una institución de educación superior.

INFRAESTRUCTURA: Sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de la entidad.

INSCRITO: Persona que cumple con los requisitos de inscripción exigidos por la institución.

INSCRIPCIÓN: Es el acto que realizan todas las personas que aspiren a ingresar por primera vez o por transferencia a cualquiera de los programas regulares y cursos especiales ofrecidos por una institución.

MANUAL DE CALIDAD: Documento que describe y especifica el Sistema de Gestión de la Calidad de una entidad.

MATRÍCULA: Acto que vincula al estudiante con la institución.

MEJORA CONTINUA: Acción permanente realizada con el fin de aumentar la capacidad para cumplir los requisitos y optimizar el desempeño.

MODELO DE ACREDITACIÓN: Documento elaborado por el Consejo parte de un ideal de Educación Superior y busca articular referentes universales con los referentes específicos definidos por la misión y el proyecto institucional.

MODELO DE AUTOEVALUACIÓN INSTITUCIONAL: Es una guía que busca orientar los procesos de evaluación y acreditación de programas, de la Institución Universitaria Mayor de Cartagena, pretende dar respuesta a las inquietudes fundamentales que se plantea la institución para llevar a cabo el proceso de Autoevaluación en forma organizada, eficiente y efectiva.

NO CONFORMIDAD: Incumplimiento de un requisito.

OBJETIVO DE CALIDAD: Algo ambicionado o pretendido, relacionado con la calidad.

PARTE INTERESADA: Organización, persona o grupo que tiene un interés en el desempeño o éxito de una entidad.

PERMANENCIA: Estudiante que realiza estudios por períodos secuenciales en una institución de educación superior

PLANIFICACIÓN DE LA CALIDAD: Parte de la gestión de la calidad enfocada al establecimiento de los objetivos de la calidad y a la especificación de los procesos operativos necesarios y de los recursos relacionados, para cumplir los objetivos de la calidad.

8. ANÁLISIS DE LA SITUACIÓN ACTUAL

La Institución Universitaria Mayor de Cartagena UMAYOR enfrenta los desafíos de seguridad y privacidad de la información en el entorno digital actual con determinación y compromiso. Reconociendo la importancia de proteger sus activos de información para mantener la confianza de su comunidad universitaria y de la sociedad en general, UMAYOR ha adoptado el Modelo de Seguridad y Privacidad de la Información MSPI promovido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). A continuación, se describe la situación actual de seguridad de la información de UMAYOR.

Situación Actual de Seguridad de la Información en UMAYOR

UMAYOR ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) y seguridad digital basado en el MSPI, que se fundamenta en el ciclo PHVA (Planear, Hacer, Verificar y Actuar) y se estructura en cinco fases clave:

Diagnóstico:

UMAYOR ha llevado a cabo un diagnóstico exhaustivo de su situación actual en relación con la adopción del MSPI.

El análisis GAP ha permitido identificar brechas y áreas de mejora, proporcionando una base sólida para la planificación y el desarrollo de estrategias de seguridad y privacidad de la información.

Planificación:

Se han definido necesidades y objetivos claros de seguridad y privacidad de la información, considerando el contexto interno y externo de la institución.

UMAYOR ha elaborado un plan de valoración y tratamiento de riesgos que se ha convertido en el eje central de sus estrategias de seguridad.

Operación:

UMAYOR ha implementado controles de seguridad adecuados para mitigar los riesgos identificados en la fase de planificación.

Estos controles incluyen medidas técnicas, administrativas y físicas diseñadas para proteger la confidencialidad, integridad y disponibilidad de los activos de información de la institución.

Evaluación de Desempeño:

Se han establecido criterios y métodos para evaluar la adopción efectiva del MSPI.

UMAYOR monitorea y mide su progreso en términos de seguridad y privacidad de la información, asegurando el cumplimiento de sus objetivos y la eficacia de sus controles.

Mejoramiento Continuo:

UMAYOR ha implementado procedimientos para identificar y corregir desviaciones en las normas establecidas en el MSPI.

El proceso de mejora continua permite a la institución adaptar y fortalecer constantemente sus estrategias de seguridad de la información. UMAYOR ha demostrado un compromiso sostenido con la protección de sus activos de información y con el cumplimiento de las expectativas de seguridad y privacidad de la comunidad universitaria y de las partes interesadas. Mediante la implementación eficaz del MSPI, la institución busca garantizar la continuidad de sus operaciones y ofrecer un entorno seguro para sus estudiantes, docentes

y personal administrativo. Este enfoque proactivo en la gestión de la seguridad de la información refleja la dedicación de UMAYOR a mantener los más altos estándares de calidad en la educación superior y en la administración de su información.

9. JUSTIFICACIÓN

La Institución Universitaria Mayor de Cartagena (**UMAYOR**) es una entidad educativa comprometida con la excelencia académica y la formación de profesionales de calidad. En el contexto actual, donde el entorno digital juega un papel fundamental en la vida cotidiana y en el desarrollo de las instituciones, es esencial que UMAYOR adopte un enfoque proactivo para proteger sus activos de información y garantizar la privacidad y seguridad de sus procesos.

El manejo adecuado de la seguridad y privacidad de la información no solo es una necesidad técnica, sino también una responsabilidad con la comunidad universitaria y la sociedad en general. UMAYOR reconoce que la confianza en la institución está directamente relacionada con su capacidad para proteger datos sensibles y garantizar la confidencialidad, integridad y disponibilidad de la información.

En respuesta a estos desafíos, **UMAYOR** ha adoptado el Modelo de Seguridad y Privacidad de la Información (MSPI) promovido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Este modelo ofrece un marco estratégico integral para establecer y operar un Sistema de Gestión de Seguridad de la Información (SGSI) y seguridad digital, basado en el ciclo PHVA (Planear, Hacer, Verificar y Actuar).

El MSPI proporciona a UMAYOR un enfoque estructurado y escalable para abordar los aspectos clave de la gestión de la seguridad y privacidad de la información:

10. PROCEDIMIENTO GESTIÓN DOCUMENTAL MSPI

El procedimiento de control documental del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Institución Universitaria Mayor de Cartagena está elaborado de la siguiente manera, tomando en consideración las cinco fases del ciclo PHVA (Planear, Hacer, Verificar y Actuar) del MSPI:

Diagnóstico:

- Se realizó una revisión exhaustiva de la situación actual de la institución en cuanto a la adopción del MSPI, identificando fortalezas, debilidades y áreas de mejora.
- Fue documentado los resultados del análisis GAP para establecer la base sobre la cual se planificaron las acciones futuras.
- Se genera un informe detallado que incluya las conclusiones del diagnóstico y las recomendaciones para la implementación del MSPI.

Planificación:

- Se elaboró un plan detallado que define las necesidades y objetivos de seguridad y privacidad de la información de la institución.
- Se documenta el proceso de valoración y tratamiento de riesgos, identificando los activos críticos, las amenazas potenciales y las medidas de control necesarias.
- Fueron definidos roles y responsabilidades dentro del proceso de implementación del MSPI, asignando tareas específicas a los miembros del equipo.

Operación:

- Se documentan los controles necesarios para mitigar los riesgos identificados durante la fase de planificación, incluyendo medidas técnicas, organizativas y de procedimiento.
- Fueron establecidos procedimientos operativos estándar (SOP) para la implementación de los controles, asegurando su consistencia y eficacia.
- Se registran incidentes relacionados con la seguridad y privacidad de la información, y documentar las acciones correctivas correspondientes.

Evaluación de desempeño:

- Se definen métricas y criterios de evaluación para medir el progreso de la institución en la adopción efectiva del MSPI.
- Está establecido un programa de auditoría interna para verificar el cumplimiento de los estándares de seguridad y privacidad de la información.
- Se documentan los resultados de las evaluaciones periódicas y utilizarlos como base para la toma de decisiones y la mejora continua.

Mejoramiento Continuo:

- Se implementaron procedimientos para identificar y documentar desviaciones en las normas establecidas en el MSPI.
- Se documentaron las acciones correctivas y preventivas tomadas para abordar las desviaciones identificadas, asegurando la corrección oportuna de los problemas.
- Como plan de mejora se revisará periódicamente el MSPI y actualizar la documentación según sea necesario para reflejar cambios en el entorno operativo o en los requisitos regulatorios.

Este procedimiento de control documental proporciona una estructura sistemática para la implementación y gestión efectiva del MSPI en la Institución Universitaria Mayor de Cartagena, asegurando la protección adecuada de los activos de información y el cumplimiento de las expectativas de seguridad y privacidad de la comunidad universitaria y demás partes interesadas.

11. METODOLOGÍA GESTIÓN DE RIESGO

Por medio de la implementación de esta metodología la **Institución Universitaria Mayor de Cartagena** logró identificar, evaluar y gestionar de manera efectiva los riesgos asociados a la seguridad y privacidad de la información, en línea con los principios y objetivos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI).

Identificación de Activos de Información:

- Fue realizado inventario de todos los activos de información relevantes para la institución, incluyendo datos sensibles, sistemas, redes, aplicaciones, recursos físicos y humanos asociados.

Evaluación de Amenazas y Vulnerabilidades:

- Se identifican las posibles amenazas y vulnerabilidades que podrían afectar a los activos de información, considerando tanto amenazas internas como externas, así como los riesgos asociados a cada una.

Análisis y Evaluación de Riesgos:

- Es evaluado el impacto potencial y la probabilidad de ocurrencia de cada riesgo identificado, utilizando matrices de riesgos o métodos similares para clasificar y priorizar los riesgos según su nivel de riesgo.

Tratamiento de Riesgos:

- Se desarrollan estrategias de tratamiento de riesgos para mitigar, transferir, evitar o aceptar los riesgos identificados, asegurando que cada riesgo sea abordado de manera adecuada y eficiente.

Implementación de Controles:

- Se implementan controles de seguridad y medidas preventivas para reducir el impacto o la probabilidad de ocurrencia de los riesgos identificados, asegurando que se apliquen de manera consistente en toda la institución.

Monitoreo y Revisión Continua:

- En **UMAYOR** fue establecido un proceso de monitoreo continuo para supervisar la efectividad de los controles implementados y detectar cualquier cambio en el entorno de riesgo que pueda requerir ajustes en la estrategia de gestión de riesgos.
- Se realizan revisiones periódicas del análisis de riesgos y de las medidas de control, actualizando la evaluación de riesgos según sea necesario para reflejar cambios en el entorno operativo o en las amenazas y vulnerabilidades identificadas.

Documentación y Comunicación:

- Son documentados todos los aspectos del proceso de gestión de riesgos, incluyendo los resultados del análisis de riesgos, las estrategias de tratamiento de riesgos y los controles implementados.

- A todas las dependencias se les comunica de manera efectiva los riesgos identificados, las medidas de control y las responsabilidades correspondientes a todas las partes interesadas relevantes dentro de la institución.

  Con esta metodología de gestión de riesgos, **la Institución Universitaria Mayor de Cartagena** podrá identificar, evaluar y gestionar de manera efectiva los riesgos asociados a la seguridad y privacidad de la información, en línea con los principios y objetivos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI).

12. RIESGOS IDENTIFICADOS Y VALORADOS DE ACUERDO A LA METODOLOGÍA

Estos riesgos representan algunas de las posibles amenazas que la institución podría enfrentar en relación con la seguridad y privacidad de la información. Implementar estrategias de tratamiento de riesgos adecuadas, monitorear de manera continua y mantener una comunicación efectiva ayudará a mitigar estos riesgos y garantizar la protección de los activos de información de la Institución Universitaria Mayor de Cartagena.

Acceso no autorizado a sistemas y datos:

- Descripción: Posibilidad de que personas no autorizadas obtengan acceso a sistemas o datos sensibles de la institución.
- Evaluación de riesgos: Impacto alto debido a la potencial exposición de información confidencial. Probabilidad media debido a la implementación de controles de acceso.
- Estrategia de tratamiento de riesgos: Implementación de autenticación multifactor, monitoreo de acceso y revisión periódica de permisos de usuario.

Ataques de malware y ransomware:

- Descripción: Exposición a virus informáticos, ransomware y otros tipos de malware que podrían comprometer la integridad y disponibilidad de sistemas y datos.
- Evaluación de riesgos: Impacto medio-alto debido a la posibilidad de interrupción de servicios y pérdida de datos sensibles. Probabilidad media debido a las medidas de seguridad implementadas.
- Estrategia de tratamiento de riesgos: Implementación de software antivirus actualizado, educación sobre conciencia de seguridad y respaldos regulares de datos.

Violación de la confidencialidad de datos personales:

- Descripción: Posibilidad de divulgación o compromiso de datos personales de estudiantes, profesores y personal administrativo.

- Evaluación de riesgos: Impacto alto debido al incumplimiento de regulaciones de protección de datos y

  daño a la reputación. Probabilidad media debido a la implementación de medidas de seguridad.
- Estrategia de tratamiento de riesgos: Implementación de políticas de privacidad robustas, encriptación de datos personales y acceso restringido a información confidencial.

Falta de cumplimiento normativo:

- Descripción: Riesgo de no cumplir con las regulaciones y normativas relacionadas con la protección de datos.
- Evaluación de riesgos: Impacto alto debido a posibles sanciones legales y daño a la reputación. Probabilidad media debido a la implementación de procesos de cumplimiento normativo.
- Estrategia de tratamiento de riesgos: Implementación de procesos de cumplimiento normativo, revisión periódica de políticas y procedimientos, y seguimiento de cambios en la legislación.

13. PLANES DE TRATAMIENTO DE LOS RIESGOS

Estos planes de tratamiento de riesgos están diseñados para abordar los riesgos identificados de manera efectiva, asegurando que la Institución Universitaria Mayor de Cartagena pueda gestionar sus riesgos de seguridad y privacidad de la información de manera proactiva y en línea con los objetivos del Modelo de Seguridad y Privacidad de la Información (MSPI).

Acceso no autorizado a sistemas y datos

- Estrategia de tratamiento:
- Mitigación: en UMAYOR se implementó autenticación multifactor en todos los sistemas y aplicaciones críticas.
- Responsable: Equipo de Seguridad de la Información.
- Monitoreo: se creó cronograma de revisión mensual de registros de acceso y auditorías de seguridad.

Ataques de malware y ransomware

- Estrategia de tratamiento:
- Mitigación: en UMAYOR se mantiene actualizado software antivirus en todos los dispositivos de la red.
- Prevención: se realizan simulacros de phishing y se proporciona capacitación regular sobre conciencia de seguridad.
- Responsable: Equipo de TI y Seguridad de la Información.
- Monitoreo: Escaneos diarios de malware, respaldos regulares y auditorías de seguridad trimestrales.

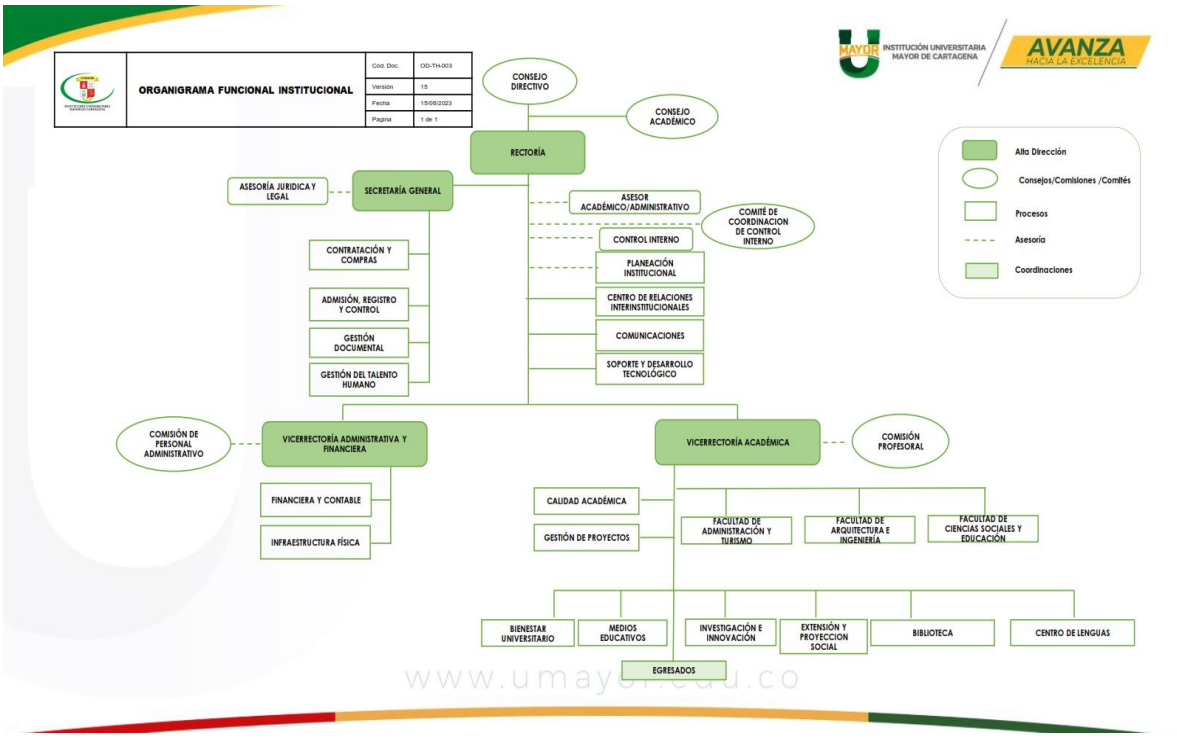
Violación de la confidencialidad de datos personales

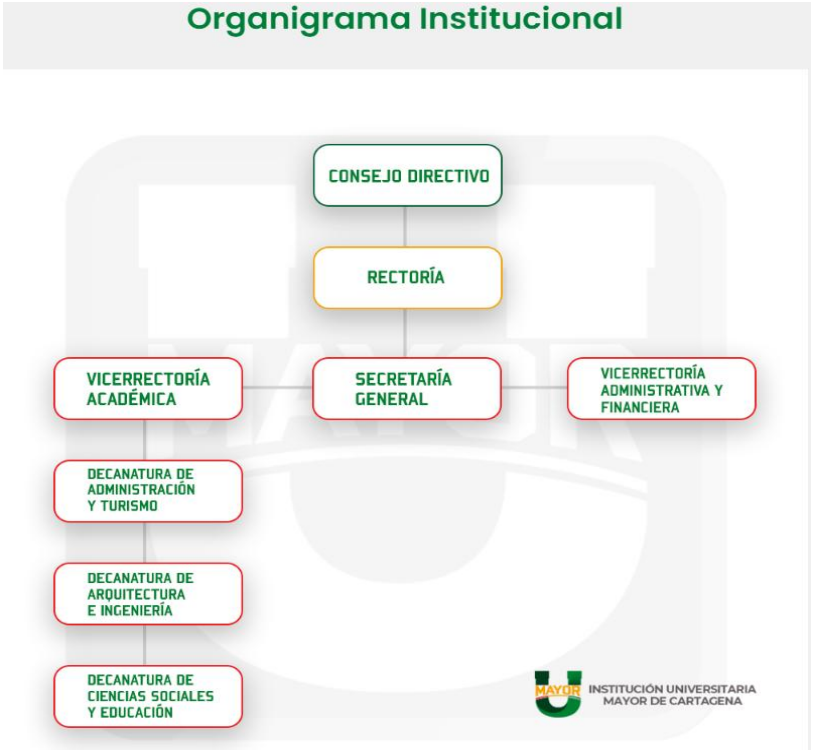
- Prevención: Implementar políticas de acceso basadas en roles y realizar capacitaciones sobre manejo de datos sensibles.
- Responsable: Equipo de Cumplimiento Normativo y Protección de Datos.
- Fecha de implementación: Dentro de los próximos 2 meses.

- Monitoreo: Auditorías internas de cumplimiento, revisiones trimestrales de políticas de privacidad.

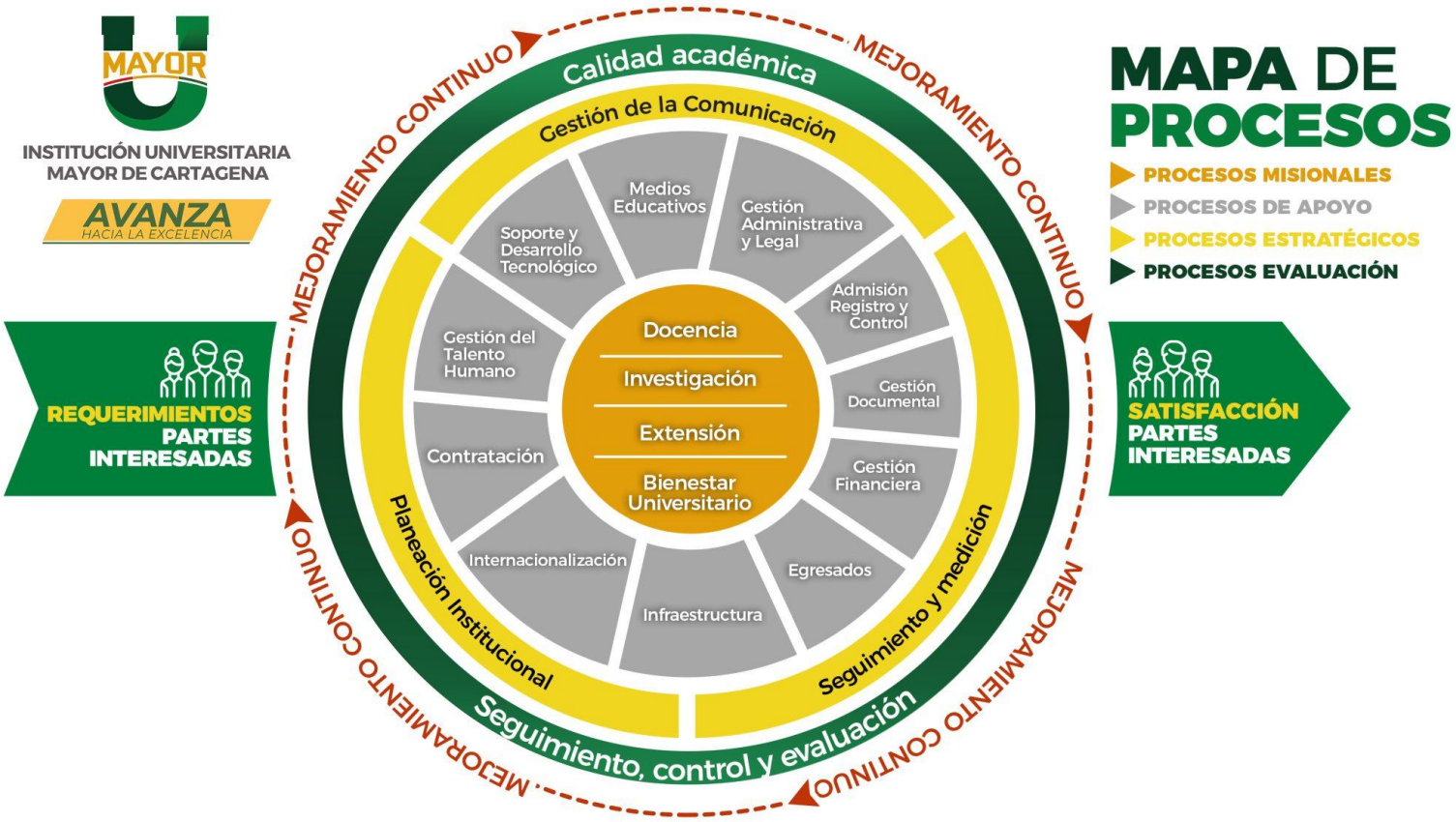
Estos planes de tratamiento de riesgos están diseñados para abordar los riesgos identificados de manera efectiva, asegurando que la Institución Universitaria Mayor de Cartagena pueda gestionar sus riesgos de seguridad y privacidad de la información de manera proactiva y en línea con los objetivos del Modelo de Seguridad y Privacidad de la Información (MSPI).

14. ORGANIGRAMA FUNCIONAL INSTITUCIONAL





15. MAPA DE PROCESOS



16. PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN

	MATRIZ DE CAPACITACIÓN														Codigo	FT-TH-031
															Versión	3
															Fecha	12/04/2023
	Contenido de la capacitación			Estatus	Cronograma Capacitación	No. Horas	Indicador Cobertura			¿La capacitación requiere evaluación? (Marque con una x)		Indicador Eficacia				
	Lineas programáticas	Nombre de la capacitación	Objetivo de la capacitación	Estatus	Fecha de realización	Horas de duración de la capacitación	Numero de asistentes a capacitación	Numero total de trabajadores programados	% Cobertura	SI	No	Numero trabajadores evaluados	Numero de evaluaciones eficaces	% de evaluaciones eficaces	Observaciones
1	5. Transformación Digital	Capacitaciones BASES DE DATOS DIGITALIA	Capacitar a la comunidad academica sobre el uso y acceso a la base de datos Digitalia	Programada	27/02/2023	1		50	0%		x				
2	7. Seguridad y Salud en el Trabajo	Inducción/Reinducción	Buscar de acciones para la conservación de la salud de los trabajadores y el mantenimiento de ambientes saludables, procurando la mejora continua	Ejecutada	30/01/2023	2		120	0%	x		101,00	101,00	100,00%	
2	7. Seguridad y Salud en el Trabajo	Investigaciones de Accidentes	Socializar con los miembros del COPASST y líderes de proceso la metodología para la investigación de accidentes.	Programada	28/02/2023	2		20	0%		x				
3	3. Gestión del Conocimiento y la Innovación	Seminario Teórico práctico de Escritura Científica	Fortalecer el proceso de formación en escritura científica de los docentes de la Institución Universitaria Mayor de Cartagena	Programada	Inauguración: Lunes 27 de febrero de 2023 de 8:00 am a 12:00 m (Actividad presencial. Por confirmar sitio). Sesión 1. Viernes 3 de marzo de 2023 (Actividad virtual) Sesión 2. Sábado 4 de marzo de 2023 (Actividad virtual) Sesión 3. Viernes 10 de marzo de 2023 (Actividad virtual) Sesión 4. Sábado 11 de marzo de 2023 (Actividad virtual) Sesión 5. Viernes 17 de marzo de 2023 (Actividad virtual) Sesión 6. Sábado 18 de marzo de 2023 (Actividad virtual) Sesión 7. Viernes 24 de marzo de 2023 (Actividad virtual) Sesión 8. Sábado 25 de marzo de 2023 (Actividad virtual)	50		52	0%		x				
4	6. Probidad y ética de lo público	Lenguaje Claro Grupo 1	Brindar herramientas para mejorar la comunicación personal e institucional, a la vez que busca organizar y diseñar mejores comunicaciones escritas, para que la información se pueda encontrar, entender y usar.	Programada	Virtual, Desarrollo autonomo del colaborador.	35		50	0%		x				
5	7. Seguridad y Salud en el Trabajo	Riesgo Químico	Brindar orientación sobre la comprensión de los peligros, el control y la prevención de la exposición a sustancias químicas, logrando la participación de los trabajadores efectiva, evitando accidentes, al igual que promocionar las prácticas adecuadas de uso, manejo y almacenamiento de las sustancias químicas empleadas; mediante actividades de vigilancia, promoción y prevención a los sujetos que manejan sustancia químicas, para minimizar los riesgos que afecten la salud de las personas que trabajen o viven	Programada	15/03/2023	2		10	0%		x				
6	5. Transformación Digital	Socialización y definición propuesta para Opencomas	Socialización y definición para el software de Comercio Exterior	Programada	22/03/2023	1		10	0%		x				
7	5. Transformación Digital	Socialización de Recursos Digitalia que posee la red cultural del banco de la republica.	Socializar los servicios del comercio interbibliotecario que ofrece la red del banco de la republica	Programada	22/03/2023	1		50	0%		x				
8	5. Transformación Digital	Confidencialidad de la información	Socializar con los diferentes grupos de interes de la Institución, la importancia de la confidencialidad y no divulgacion de la información reservada.	Programada	12/04/2023 21/04/2023	2		200	0%		x			#¡DIV/0!	
9	7. Seguridad y Salud en el Trabajo	Inspecciones de seguridad (COPASST, Servicios Generales)	Capacitar a los miembros del COPASST y Servicio	Programada	18/04/2023	2		12	0%		x				
10	5. Transformación Digital	Base de datos E-libro	Capacitar a los docentes y estudiantes sobre el uso de las base de datos	Programada	19/04/2023	1		50	0%		x				

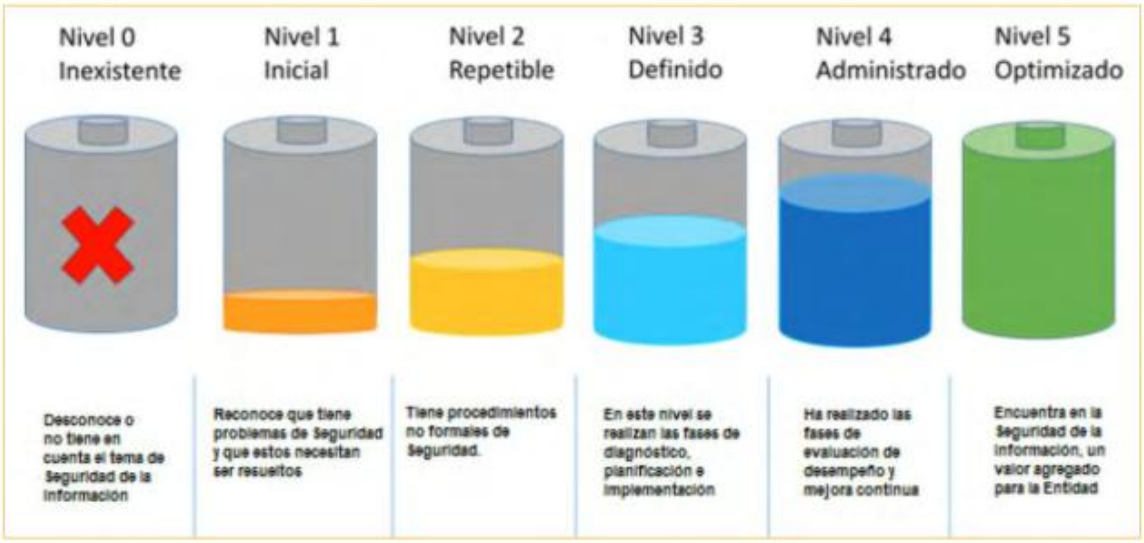
11	3. Gestión del Conocimiento y la Innovación	Conversatorio Vida de Gabriel Garcia Marquez	Fomentar el hábito de la lectura y escritura a través de los espacios lúdicos-pedagógicos que resitalen la vida de Gabriel Garcia Marquez	Programada	19/04/2023	2		20	0%		x				
12	3. Gestión del Conocimiento y la Innovación	Herramientas Pearson	Socializar las herramientas pearson con profesores del Centro de Idiomas-programas de turismo	Programada	22/04/2023	2		25	0%		x				
13	5. Transformación Digital	Taller Teorico- Practico Base de datos EBSCO	Capacitar a la comunidad academica sobre el uso y acceso a la base de datos EBSCO	Programada	24/04/2023	2		50	0%		x				
14	5. Transformación Digital	Capacitación Base de Datos Digitalia	Capacitar a la comunidad academica sobre el uso y acceso a la base de datos Digitalia	Programada	24/04/2023	2		50	0%		x				
15	7. Seguridad y Salud en el Trabajo	Orden y aseo: Metodologia de las 5S	Socializar la mmetodologia de las 5S en el desarrollo de actividades.	Programada	24/04/2023	3		50	0%		x				
16	7. Seguridad y Salud en el Trabajo	Prevención de caidas a nivel I	Brindar herramientas de prevención para evitar la ocurrencia de las caidas a nivel.	Programada	27/04/2023	2		50	0%		x				
17	7. Seguridad y Salud en el Trabajo	Estilos de vida saludable	Socializar con el personal la importancia de tener habitos y estilos de vida saludables	Programada	27/04/2023	1		35	0%		x				
18	7. Seguridad y Salud en el Trabajo	Prevención de Riesgos Cardiovasculares	Crear conciencia de la importancia del cuidado al momento de ejecutar las actividades laborales e implementación de los habitos saludables	Programada	9/05/2023	2		50	0%		x				
19	7. Seguridad y Salud en el Trabajo	Prevención de enfermedades laborales	Prevención de enfermedades laborales	Programada	19/05/2023	2		8	0%						

20	3. Gestión del Conocimiento y la Innovación	Capacitación Herramientas de Google (Workspace)	Fomentar el uso de las herramientas de google, que se encuentran disponibles en la institución.	Programada	30/06/2023	2		40	0%		x				
21	3. Gestión del Conocimiento y la Innovación	Taller Indicadores de Gestión para Lideres	Fortalecer los procesos de medición a traves de los indicadores de gestión	Programada	26/06/2026	2		25	0%		x				
22	7. Seguridad y Salud en el Trabajo	Pausas Activas	Promover conciencia en la salud respecto al autocuidado de la comunidad UMAYOR	Programada	2/06/2023	3		60	0%		x				
23	4. Creación de valor público.	En el lugar de trabajo ¿Cómo me proyecto?	Fortalecer la imagen y proyección de todos los colaboradores de la institución	Programada	26/06/2023	2		60	0%		x				
24	6. Probidad y ética de lo público	Capacitación de ética en lo público	Buen comportamiento de funcionarios público con probidad	Programada	27/06/2023	40		6	0%		x			x/xxxx	
25	4. Creación de valor público.	Gestión Documental	Fortalecer los conocimientos de todo el personal en materia de gestión documental	Programada	12/07/2023	2		120	0%		x				
26	7. Seguridad y Salud en el Trabajo	Prevención de caidas a nivel II	Brindar herramientas de prevención para evitar la ocurrencia de las caidas a nivel.	Programada	9/08/2023	2		60	0%		x				
27	1. Gestión del cambio – cultura organizacional	Seminario de Alta Gerencia y Liderazgo	Capacidad de direccion y fortalecimiero en el liderazgo para la productividad con el fin de lograr las metas que involucre a los egresados y el poder	Programada	9/08/2023	120		20	0%		x			x/xxxx	
28	2. Institucionalidad para la paz	Educación Inclusiva	Preparar a la comunidad para atender las necesidades de los estudiantes con especial énfasis en aquellos que son vulnerables a la marginalidad y la	Programada	9/08/2023	120		150	0%		x			x/xxxx	
29	2. Institucionalidad para la paz	**Diplomado para la Paz** con enfoque diferencial, Violencia de genero, cultura de paz e identidad, posteuerdo para la construccion de paz y liderazgos locales.	adpatacion de las necesidades de las diferentes poblaciones a intervenir y poder motivar e influir en un liderazgo local basado en la construccion de paz.	Programada	9/08/2023	120		15	0%		x			x/xxxx	
30	3. Gestión del Conocimiento y la Innovación	Elaboración y gestion de informes ejecutivos	Brindar herramientas realizar informes ejecutivos de impacto	Programada	9/08/2023	120		40	0%		x			x/xxxx	
31	7. Seguridad y Salud en el Trabajo	Capacitación en manejo de Riesgo Público	Brindar herramientas para dar manejo a situaciones de atención al usuario que se salgan de control	Programada	10/08/202	30		20	0%		x			x/xxxx	
32	1. Gestión del cambio – cultura organizacional	Gestión del cambio organizacional	Logran aprehender estilos de liderazgo organizacional para la transformación estilosa	Programada	10/08/2023	120		80	0%		x			x/xxxx	
33	7. Seguridad y Salud en el Trabajo	Manejo del Estrés	Entrenar en habilidades de control de las emociones que permitan proveer a los participantes de herramientas para enfrentar situaciones que perciben	Programada	25/08/2023	2		90	0%		x				
34	7. Seguridad y Salud en el Trabajo	Seguridad Basada en comportamientos	Lograr el cambio de conducta de los trabajadores. En particular, minimizar los comportamientos inseguros, germen de la mayoría de los accidentes.	Programada	31/08/2023	2		50	0%		x				

35	7. Seguridad y Salud en el Trabajo	Tre Charla Conservacion de la Voz	Capacitar a los docentes sobre los mecanismos de la producción vocal normal y los factores que la modifican. - Prevenir las alteraciones de la voz a partir del conocimiento y adopción de hábitos saludables.	Programada	08/09/2023	2		50	0%		x				
36	7. Seguridad y Salud en el Trabajo	Prevención del Riesgo Psicosocial	Identificar, evaluar y valorar los riesgos psicosociales presentes en el entorno laboral para, con la intención de eliminarlos o reducirlos, establecer las medidas preventivas que resulten oportunas.	Programada	15/09/2023	2		80	0%		x				
38	3. Gestión del Conocimiento y la Innovación	Herramientas Ofimaticas	Aprender el uso de las herramientas informaticas para automatizar, optimizar y compartir informacion en las tareas administrativas. Manejo de bases de datos	Programada	Proyectada para Septiembre			40	0%		x			x/xxxx	
39	7. Seguridad y Salud en el Trabajo	Taller: Prevención de Riesgos laborales	Tener conocimiento de cuales son los factores de riesgos laboraly asi prevenir enfermedades	Programada	Proyectada para Septiembre			2	0%		x			x/xxxx	
40	1. Gestión del cambio – cultura organizacional	Curso Logistica y Organización de Eventos	Planificar encuentros y reuniones de manera organizada Teniendo la coordinación de la logistica interna y externa.	Programada	Proyectada para Octubre			15	0%		x			x/xxxx	
41	1. Gestión del cambio – cultura organizacional	Comunicación Organizacional	Lograr el fortalecimiento del clima organizacional a traves de la comunicación.	Programada	Proyectada para Octubre	2		40	0%		x			x/xxxx	
42	3. Gestión del Conocimiento y la Innovación	Gestión de la permanencia estudiantil	Identificar los lineamientos desde el Ministerio de Educación Nacional para la Gestión de la permanencia estudiantil.	Programada	En el marco del convenio UDC			42	0%		x			x/xxxx	
43	3. Gestión del Conocimiento y la Innovación	Gestión del conocimiento como integrador para la innovación	Capacitar al equipo de Calidad Académica sobre las particularidades de la gestión del conocimiento para aplicación de estrategias innovadoras en los procesos	Programada	Proyectada para Septiembre			4	0%		x			x/xxxx	
45	1. Gestión del cambio – cultura organizacional	Gestión Ambiental	Capacitar a toda la comunidad Umayor sobre el sistema de gestión ambiental y su importancia a nivel institucional	Programada	En el marco del convenio UDC			40	0%		x			x/xxxx	
46	3. Gestión del Conocimiento y la Innovación	Diseño e implementación de Estrategias pedagógicas	Identificar e implementar estrategias pedagógicas ajustada al contexto actual.	Programada	En el marco del convenio UDC			50	0%		x			x/xxxx	
47	3. Gestión del Conocimiento y la Innovación	Normatividad adscrita a la Educación Superior en Colombia	Conocer e interpretar el marco legal asociado a la educación superior en Colombia	Programada	En el marco del convenio UDC			50	0%		x			x/xxxx	
48	3. Gestión del Conocimiento y la Innovación	Estrategias internacionalización del currículo	Identificar e implementar estrategias que fomenten la internacionalización del currículo	Programada	En el marco del convenio UDC			50	0%		x			x/xxxx	
49	7.Seguridad y Salud en el Trabajo	Inpeecciones de Siguridad	Detectar y controlar los peligros potenciales susceptibles de ocasionar pérdidas que afecten a las personas o a la propiedad. Identificar las situaciones laborales que puedan causar accidentes de trabajo y definir las medidas correctivas necesarias	Programada	19/04/2023	2		11	0%		x			x/xxxx	
50	7.Seguridad y Salud en el Trabajo	Seguridad Basada en comportamientos	Es una herramienta de gestión que se rige por la observación de las conductas seguras en el lugar de trabajo. Su finalidad es reforzar y mejorar el desempeño o comportamiento seguro de toda la plantilla de una organización	Programada	31/08/2023	2		30	0%		x				
51	7.Seguridad y Salud en el Trabajo	Salud Mental	Fomentar la cultura de la salud mental mediante actuaciones con individuos, grupos y comunidades. Prevenir la aparición de trastornos de salud mental en el país. Recrientar y mejorar la calidad de la prestación del servicios en salud mental, en el contexto del Sistema General de Seguridad Social en Salud.	Programada	28/11/2023	2		30	0%						
52	7.Seguridad y Salud en el Trabajo	Capacitación Manejo Sustancia Quimica	El manejo adecuado de sustancias químicas permite incrementar la seguridad, reducir las emergencias químicas, el impacto ambiental, social y económico de las mismas	Programada	15/03/2023	2		4	0%						

17. MODELO DE MADUREZ

Este modelo permite identificar el modelo de madurez del MSPI en el que se encuentra la **INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA,** midiendo la brecha entre el nivel actual de la entidad y el nivel optimizado. A continuación, la figura muestra diferentes niveles que hacen parte del modelo de madurez.



De acuerdo a la figura del **MODELO DE SEGURIDAD y PRIVACIDAD DE LA INFORMACIÓN** el nivel de madurez en el que se encuentra la **INSTITUCIÓN UNIVERSITARIA MAYOR DE CARTAGENA** es el nivel 3, el cual explica lo siguiente:

		NIVEL DE CUMPLIMIENTO
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Inicial	SUFICIENTE
	Repetible	INTERMEDIO
	Definido	INTERMEDIO
	Administrado	INTERMEDIO
	Optimizado	CRÍTICO

NIvel	Descripción
Administrado	La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información. ● Se revisa y monitorea periódicamente los activos de información de la Entidad. ● Se utilizan indicadores para establecer para el cumplimiento de las políticas de seguridad y privacidad de la información ● Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro ● La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.

18. PLAN DE TRANSICIÓN DE IPV4 A IPV6

19. DESCRIPCIÓN DE LA INFRAESTRUCTURA ACTUAL DE LA ENTIDAD

La Institución Universitaria Mayor de Cartagena, dispone de un Data Center con un servicio de internet dedicado por fibra óptica, con IPS Movistar a una velocidad simétrica de 300Mbps para dar cobertura de internet a toda las áreas administrativas y académicas.

Un Data Center equipado con servidores físicos y virtuales para alojar sistemas críticos, bases de datos, aplicaciones y almacenamiento de datos. Asimismo, dispone una UPS y un conjunto de equipos de red activos, que van desde la seguridad perimetral de un firewall hasta router, switch y punto de acceso inalámbricos con velocidades desde 1Gbps, combinando así las redes cableadas y Wi-Fi que conectan todas las dependencias, salones, salas de informática proporcionando acceso a Internet a personal administrativos, docentes y estudiantes.

La infraestructura de red de datos, está segmentada y conformada con un conjunto de servidores virtualizados con diferentes servicios entorno a los sistemas de información académico y administrativos, directorio activo, servidor de gestión centralizada de seguridad informática Eset Protect, servicio de aplicativo Zeus Hotel.....

Dispone de equipos activos de red, que van desde firewall imponiendo la seguridad perimetral hasta router, switch y puntos de acceso inalámbrico con velocidades de 1Gbps.

UMAYOR dispone de una de una arquitectura de servicios tecnológicos para una adecuada operación de los procesos de la entidad, provisto de una suscripción con Movistar como Proveedor del Servicio de Internet - IPS a velocidad simétrica de 100Mbps con medio de transmisión fibra óptica, un sistema PBX y firewall fortinet.

Seguidamente desde el centro de datos propiamente, consta con una gran capacidad de almacenamiento necesario donde se albergan una amplia variedad de bases de datos, archivos, aplicaciones y espacio para un entorno de servidores virtualizados desde donde se administra la infraestructura tecnológica de UMAYOR y todo ello bajo un respaldo de un sistema de alimentación ininterrumpida – UPS.

Desde el centro de datos se proporciona el servicio de Internet y de Intranet a todos los equipos de cómputos administrativos y académicos de la institución mediante conexión guiada por cable UTP categoría 6 llegando a velocidades en la LAN de 1Gbps, gozando de servicios como Firewall, Controlador de Dominio, Software Académico, administrativo y Financiero, Chat Institucional, Copias de Seguridad Automáticas, Centro de Comunicación de Telefonía, Sistemas de Información Académico y Administrativo, servicio de impresora en la red.

Cabe aclarar que la red administrativa y la red académica están en segmentos total mente diferentes tal que los hosts de una red y otra no se alcanzan.

Así mismo, en lo que corresponde a la conexión no guiada, la institución cuenta con un despliegue de redes wifi en toda el área geográfica de la institución atendiendo a cabalidad la cobertura inalámbrica, protegida con un tipo de seguridad WPA PSK2 en todos sus puntos de acceso wireless.

20. PERSONAL, PROCESOS, NORMAS Y POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

- **Servicios de Operación:**

  Se catalogan como servicios de operación aquellos que garantizan la operación, mantenimiento y soporte de la plataforma tecnológica; de las aplicaciones, de los sistemas de información y de los servicios informáticos.

  En **UMAYOR** se realizan programas de mantenimiento preventivo y correctivo a los equipos de cómputo de la institución. No obstante, existen algunos retos para optimizar la calidad y seguridad de los servicios.

  Los servicios que el grupo de sistemas presta en primera instancia para cubrir, desde el punto de vista técnico las necesidades de las áreas de la institución se describen a continuación.

Servicios	Disponibilidad	Horario de soporte	Tiempo de respuesta	Responsable
❖ Servicios de Contexto: ➢ Servicio de Red. ➢ Servicios de Comunicaciones. ➢ Servicios de Accesibilidad. ➢ Servicios de seguridad. ➢ Servicios de gestión de accesos.	99 %	L - V de 7:00 a.m. a 9:00 p.m.	Todas las solicitudes que recibimos son atendidas inmediatamente, pero dependiendo de la solicitud y del área al cual pertenece, el tiempo de respuesta podría variar. Por ejemplo, si pertenece al área de Redes y Comunicación y no hay insumos dependemos del tiempo de respuesta de Recursos Físicos.	Grupo de Sistemas
❖ Servicios de Productividad: ➢ Servicios de correo electrónico. ➢ Servicios ofimáticos.	99 %	L - V de 7:00 a.m. a 9:00 p.m.		Grupo de Sistemas
❖ Servicios de Soporte: ➢ Servicios de salidas: ▪ Portales web. ➢ Servicios de almacenamiento:	99 %	L - V de 7:00 a.m. a 9:00 p.m.		Grupo de Sistemas

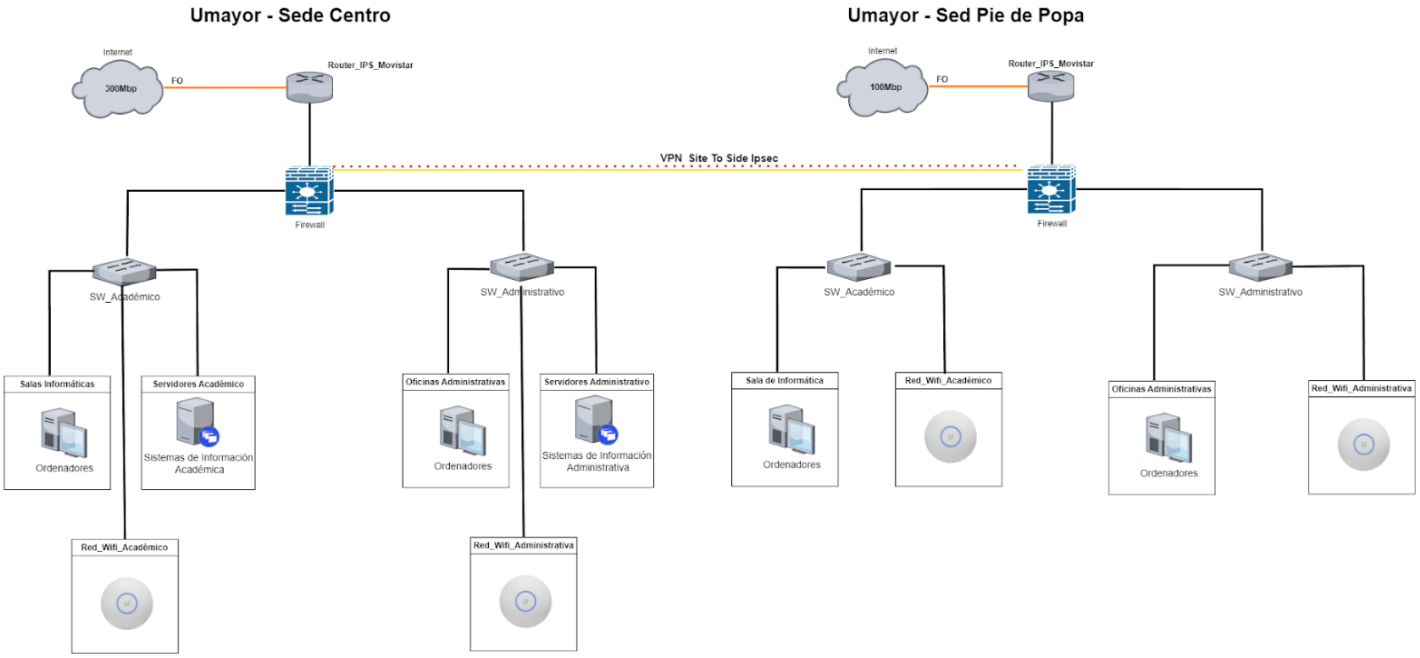
▪ Backup Freenas ➢ Servicios Remotos: ▪ Acceso remoto VNC ❖ Hardware ➢ Computadores y portátiles. ➢ Periféricos.				
❖ Sistemas de Información: ➢ S. I. Synersis ➢ S. I. WAS ➢ S. I. Plataforma Virtual	99 %	L - V de 7:00 a.m. a 9:00 p.m.		Grupo de Sistemas

- **PR-ST-001 PROCEDIMIENTO DE MANTENIMIENTO:** Proporcionar y coordinar los servicios que en materia de mantenimiento preventivo requiere la Institución universitaria mayor de Cartagena, prolongando la vida útil de la infraestructura tecnológica informática, garantizando el buen funcionamiento de la misma.
-
- **PR-ST-004-PROCEDIMIENTO ADMINISTRACIÓN COPIAS DE SEGURIDAD:** Planear, desarrollar y controlar las actividades relacionadas con las copias de seguridad de la información de la Institución Tecnológica Colegio Mayor de Bolívar, para garantizar la integridad y seguridad de los datos.

- **PR-ST-006 ADMINISTRACIÓN DE LICENCIAS:** Describir en forma clara las diferentes actividades que se realizan en el procedimiento de Administración de Licencias con el fin de garantizar el manejo adecuado de las mismas dentro de la Institución Tecnológica Colegio Mayor de Bolívar.

PR-ST-007 DESARROLLO Y SOPORTE DE SOFTWARE INSTITUCIONAL: Diseñar, desarrollar y mantener los diferentes aplicativos creados a medida para la institución, Mejorando así el desarrollo tecnológico de la institución por medio de la sistematización de procesos y procedimiento que se realizan en el colegio mayor de Bolívar.

21. DIAGRAMA DE LA RED DE UMAYOR



22. MARCO NORMATIVO

Conforme con lo establecido en la normatividad vigente el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación del MSPI en la Entidad UMAYOR:

- Constitución Política de Colombia. Artículos 15, 209 y 269.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. • Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1080 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.
- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.