



**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACIÓN EN LA INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR
DE ANTIOQUIA.**



1. INTRODUCCIÓN

La institución Universitaria Colegio Mayor de Antioquia implementa un método lógico y sistemático en busca de la mejora continua, que posibilite la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los riesgos asociados al manejo de la información institucional, con el fin de prevenir y controlar la aparición de los mismos.

En las diferentes actividades y quehacer diario, la institución utiliza las TIC para la captura de información, al igual que su procesamiento y reporte de información en el ámbito interno y externo, con la intención de entregarse de forma segura y oportuna, lo cual posibilita la vulneración de la misma frente ataques, mala manipulación llegando así a problemas de carácter legal, económico y administrativo por lo cual se pretende con éste documento establecer una línea de trabajo para lograr la seguridad y correcta manipulación de datos almacenados en las diferentes bases de datos institucionales.

2. ALCANCE

La vigencia del presente plan es 2021-2023 y aplica para los procesos evidenciados en el Mapa de Procesos Institucional.

3. OBJETIVO

3.1 GENERAL

Elaborar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información alineado con la guía metodológica para la gestión del riesgo del Departamento Administrativo de la Función Pública y las disposiciones de la Ley 1581 de 2012, decreto 1377 de 2013 y el decreto 886 de 2014.

3.2. ESPECÍFICOS

- Lograr un diagnóstico real de la situación actual de la Institución Universitaria Colegio Mayor de Antioquia referente a los riesgos de seguridad y privacidad de la información.
- Aplicar metodologías, recomendaciones y mejores prácticas enunciadas por el DAFP y Min Tic para el tratamiento de riesgos de seguridad y privacidad de la información.
- Aportar avances al modelo integrado de planeación y gestión en sus políticas de Gobierno Digital, Seguridad Digital, Transparencia, Acceso a la Información Pública y Lucha contra la Corrupción.
- Integrar en el mapa de riesgos institucional los riesgos de seguridad y privacidad de la información.



4. RECURSOS

- **Humano:** La Alta Dirección, oficina de control interno, equipo MIPG, líderes de proceso y líder del proceso de tecnología.
- **Físico:** Infraestructura tecnológica, controles de acceso físico.

5. RESPONSABLES

- La Alta Dirección
- Oficina Gestión Documental
- Equipo MIPG
- Oficina de Control Interno
- Talento Humano
- Líderes de Proceso
- Líder de Tecnología
- Equipo de Comunicaciones

6. MARCO CONCEPTUAL

- **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.
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **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.
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
- **Ciberespacio:** Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua Española). 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 salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la



organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

- 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.
- Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.
- 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.
- 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 interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) 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.
- Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.
- Parte interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

7. MARCO NORMATIVO

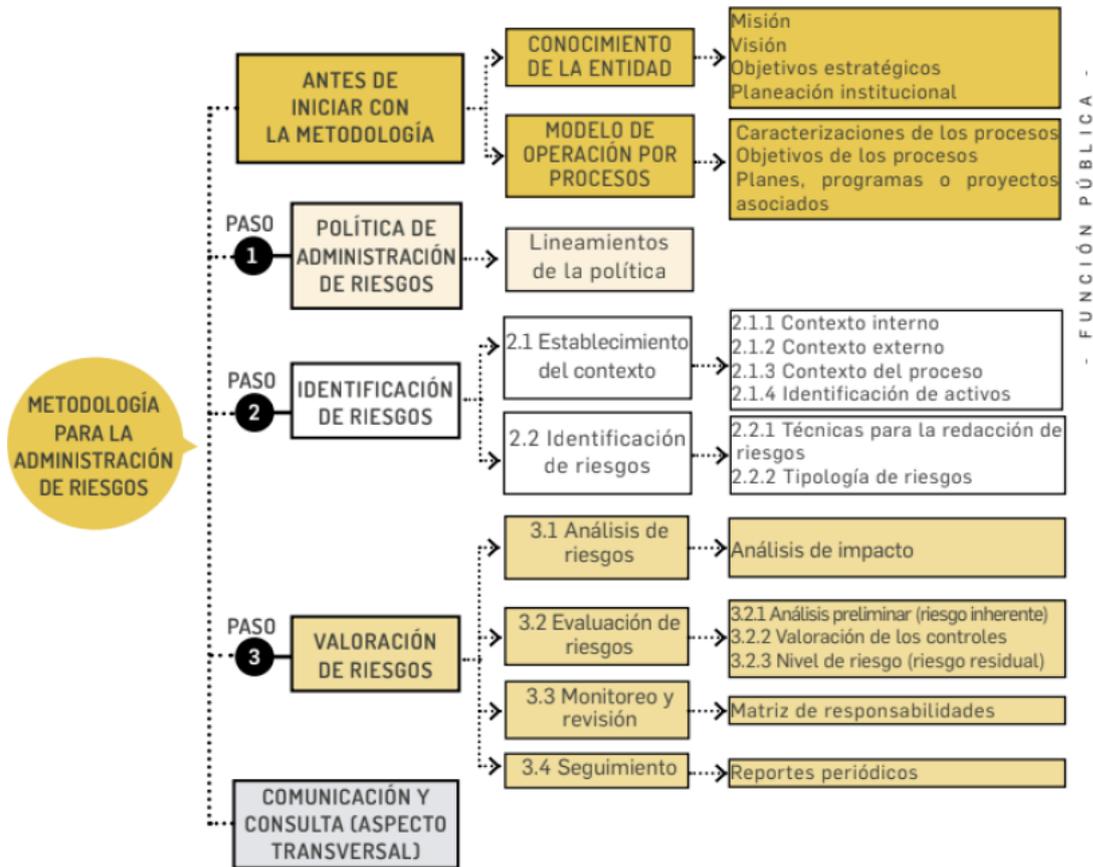
- Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública
- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública
- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales
- Ley 594 de 2000 - Ley General de Archivos
- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática



- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad
- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo
- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos
- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública
- Decreto 2364 de 2012 - Firma electrónica
- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos
- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales
- Ley 527 de 1999 - Ley de Comercio Electrónico
- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
- Ley Estatutaria 1581 de 2012 - Protección de datos personales
- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información
- Decreto 1759 de 8 de noviembre de 2016 por el cual se modifica el artículo 2.2.2.26.3.1 del Decreto 1074 de 2015. Decreto Único Reglamentario del Sector Comercio, Industria y Turismo
- Resolución 670 de 14 de diciembre de, 2017 de la Procuraduría General de la Nación, por medio de la cual se adopta el manual de políticas y procedimientos para la protección de datos personales.
- Ley 1915 de 12 de julio 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.
- Ley 1928 de 24 de julio de 2018, por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest.
- Proyecto de ley 300 de 2020, del 11 de marzo de 2020, por medio de la cual se dictan disposiciones generales para el fortalecimiento de la protección de datos personales, con relación al reconocimiento de las garantías de los derechos digitales, y se dictan otras disposiciones.
- Decreto 1287 de 24 de septiembre de 2020, por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.



8. METODOLOGÍA DE IMPLEMENTACIÓN



Fuente: Cartilla de administración de riesgos del DAFP ISO 31000:2018

8.1. ACTIVIDADES Y ENTREGABLES DE LAS FASES DE LA METODOLOGÍA DE IMPLEMENTACIÓN

8.1.1. Fase I – Caracterización de los sistemas de gestión y de los procesos de la Entidad

Dentro de esta fase se realizan las siguientes actividades:

- Listado Maestro de Registros en el SIG Actualizado
- Identificación de procedimientos actualizados
- Inventario de activos de información

8.1.2. Fase II – Identificación de riesgos

Dentro de esta fase se realizan las siguientes actividades:



- Identificación de causas
- Identificación de riesgo.
- Establecer las consecuencias
- Tipificar y valorar el riesgo
- Determinar el impacto
- Determinar la probabilidad
- Determinar el nivel de riesgo inherente y residual

8.1.2 Fase III – Valoración de controles

- Calculo estimado del riesgo residual
- Selección de la opción de tratamiento
- Determinar las acciones de mitigación del riesgo

8.1.5. Fase V – Seguimiento y Evaluación.

- Realizar seguimiento a la autoevaluación de la gestión por áreas
- Realizar monitoreo de los riesgos a través de la evaluación independiente que realiza la Entidad y el líder del sistema de gestión de seguridad y privacidad de la información.
- Determinar las alertas que se generen a partir de los resultados de las mediciones anteriores
- Aplicar acciones de mejora continua resultado de las auditorias, de los mapas de riesgos y planes de acción.
- Socialización de resultados

9. DESARROLLO DEL PLAN

El seguimiento del presente plan se realiza conforme a los diferentes informes y tiempos establecidos en el Plan de Acción por proceso, y es registrado en un documento de control de avance del mismo, y a su vez quedará registrado el resultado en el mapa de riesgos institucional con su debida identificación como “Riesgo de Seguridad y Privacidad de la Información”.