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 ha adoptado un enfoque metódico y estructurado con el propósito de optimizar de manera continua la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los riesgos vinculados a la gestión de la información institucional. Esta estrategia se implementa con el fin de prevenir, controlar e incorporar medidas que mitiguen los riesgos y su posible aparición. En todas las actividades y tareas cotidianas, la institución recurre a las Tecnologías de la Información y la Comunicación (TIC) para la captura, procesamiento y reporte seguro y oportuno de información, tanto interna como externa. De este modo, se previene la vulneración de la información ante eventuales ataques o manipulaciones inadecuadas, lo que podría acarrear problemas legales, económicos y administrativos.

Con este documento, se pretende definir un marco de trabajo que asegure la protección y la adecuada gestión de la información contenida en las diversas bases de datos institucionales.

2. ALCANCE

La vigencia del presente plan es 2025-2027 y aplica para los procesos evidenciados en el Mapa de Procesos Institucionales.

3. OBJETIVO

3.1 GENERAL

Desarrollar el Plan de Tratamiento de Riesgos en materia de Seguridad y Privacidad de la Información, conforme a la guía metodológica para la gestión del riesgo del Departamento Administrativo de la Función Pública, así como a lo establecido en la Ley 1581 de 2012, el decreto 1377 de 2013 y el decreto 886 de 2014.

3.2. ESPECÍFICOS

- Realizar un diagnóstico certero sobre la situación presente de la Institución Universitaria Colegio Mayor de Antioquia en lo que respecta a los riesgos asociados a la seguridad y la privacidad de la información.

- Aplicar las metodologías, sugerencias y mejores prácticas definidas por el DAFP y Min Tic con el fin de gestionar de manera eficaz los riesgos relacionados con la seguridad y la privacidad de la información.

- Colaborar en el crecimiento y solidificación del modelo integral de planificación y gestión dentro de las políticas de Gobierno Digital, Seguridad Digital, Transparencia, Acceso a la Información Pública y Combate a la Corrupción, a través de la ejecución de medidas y acciones específicas.

- Incorporar en el mapa de riesgos institucional los riesgos asociados a la seguridad y la protección de la información.

4. RECURSOS

RECURSOS	VARIABLE
Humanos	• El Grupo Interno de Trabajo de Seguridad y Privacidad de la Información • Profesional de riesgos del Grupo Interno de Trabajo de Transformación Organizacional • Líderes y gestores de procesos • Dimensión de Seguridad informática de la Oficina de TI • Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia - COLCERT • Equipo de Trabajo de Seguridad y Privacidad de la Información de la Dirección de Gobierno Digital.
Técnicos	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital del DAFP Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI)
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías en el GIT de Seguridad y Privacidad de la Información

5. RESPONSABLES

A. Alta Dirección

- **Rol:** Aprobación del plan y aseguramiento de recursos necesarios (financieros, humanos y tecnológicos).
- **Responsabilidades:**

- Garantizar que el tratamiento de riesgos esté alineado con los objetivos estratégicos de la organización.
- Establecer una cultura de seguridad y cumplimiento.
- Supervisar los resultados y desempeño del plan a través de reportes periódicos.

B. Oficial de Seguridad de la Información (CISO o equivalente)

- **Rol:** Líder principal del plan, responsable de supervisar su diseño e implementación.
- **Responsabilidades:**

- Coordinar los análisis de riesgos y definir las estrategias de mitigación.
- Supervisar las auditorías y revisiones de cumplimiento.
- Garantizar que las políticas y procedimientos estén alineados con las normativas aplicables.

C. Equipo de Tecnologías de la Información (TI)

- **Rol: Implementación técnica de controles de seguridad y privacidad.**
- **Responsabilidades:**

- Gestionar los sistemas de autenticación, firewalls, antivirus y demás herramientas tecnológicas.
- Realizar copias de seguridad periódicas y verificar su recuperación.
- Implementar actualizaciones de seguridad y monitorear vulnerabilidades.

D. Oficial de Cumplimiento o responsable Legal

- **Rol:** Garantizar el cumplimiento normativo en temas de privacidad y protección de datos (por ejemplo, GDPR, ISO 27001, Ley de Protección de Datos).
- **Responsabilidades:**

- Identificar y comunicar requisitos regulatorios relevantes.
- Realizar evaluaciones de impacto de privacidad (PIAs o DPIAs).
- Velar por que la organización documente y respalde cada control implementado.

E. Dueños de Procesos

- **Rol:** Responsables de los procesos internos donde se identificaron riesgos específicos.
- **Responsabilidades:**

- Asegurar que sus procesos cumplan con las políticas de seguridad y privacidad.
- Colaborar en la identificación de riesgos y ejecución de controles.
- Monitorear los indicadores relacionados con los riesgos de su área.

F. Comité de Seguridad y Privacidad

- **Rol:** Grupo interdisciplinario encargado de monitorear, asesorar y ajustar el plan.
- **Responsabilidades:**

- Revisar y priorizar los riesgos identificados.
- Alinear las acciones del plan con los objetivos de la organización.
- Proponer actualizaciones según los cambios del entorno interno o externo.

G. Auditores Internos/Externos

- **Rol:** Evaluar la efectividad del plan y sus controles implementados.
- **Responsabilidades:**

- Identificar desviaciones y proponer medidas correctivas.
- Verificar el cumplimiento de estándares internacionales, normativas y políticas internas.
- Emitir reportes sobre los hallazgos de auditoría.

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.
Criticidad: Ej. Catastrófico, Mayor, Moderado, Menor, Insignificante.
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.
Eficacia: Grado en el que se realizan las actividades planificadas y se logran los resultados planificados. NTC ISO 9000: 2015.
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.
Gestión o Administración del riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
Impacto: consecuencias que puede ocasionar a la organización la materialización del riesgo.
Parte interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
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.
Política de administración del riesgo: Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.
Revisión: Acción para determinar la idoneidad, conveniencia y eficacia de la gestión del riesgo.
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.
Riesgo inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de dirección para modificar su probabilidad o impacto. (primer análisis).
Riesgo residual: Nivel de riesgo que permanece luego de tomar medidas (dirección) de tratamiento del riesgo. (análisis final/permanece).
Riesgo de Seguridad de la Información: 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. (ISO/IEC 27000).
Seguimiento: Asegurar que las acciones establecidas se están llevando a cabo.
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.

7. MARCO NORMATIVO

LEY	DEFINICIÓN
Constitución Política de Colombia Art. 15 y 74	Establece el derecho a la intimidad, protección de datos personales y habeas data, así como el derecho de acceso a la información pública con garantías de confidencialidad.
Ley 527 de 1999	Ley de Comercio Electrónico
Decreto 1747 de 2000	Entidades de certificación, los certificados y las firmas digitales
Ley 594 de 2000	Ley General de Archivos.

Decreto 1537 de 2001 Artículo 4	La administración de los riesgos, como parte integral del fortalecimiento de los sistemas de control interno en las entidades publicas
Ley 962 de 2005	Racionalización de trámites y procedimientos administrativos procedimientos administrativos. que los afectan. Literal f) Definir y aplicar medidas para prevenir los riesgos, detectar y corregir desviaciones que se presentan en la organización y que puedan afectar el logro de los objetivos.
Ley 1266 de 2008	Enfocada en la protección de información financiera, crediticia y comercial, estableciendo medidas para garantizar integridad y confidencialidad.
Circular Única de la SIC	Dicta lineamientos técnicos para la gestión de riesgos en protección de datos personales e implementación de sistemas de gestión de seguridad de la información (SGSI).
Ley 1474 de 2011 Estatuto anticorrupción Art. 73.	"Plan anticorrupción y atención al ciudadano" que debe elaborarse anualmente, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar riesgos, las estrategias anti- trámites y los mecanismos para mejorar la atención al ciudadano.
Ley 1581 de 2012	Regula el tratamiento de datos personales, estableciendo principios clave (legalidad, finalidad, transparencia, seguridad, entre otros) y medidas para proteger los datos.
Decreto 019 de 2012	Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
Decreto 2364 de 2012	Firma electrónica
Ley estatutaria 1618 de 2013	Ejercicio pleno de las personas con discapacidad
Decreto 1377 de 2013	Reglamenta la Ley 1581, definiendo disposiciones sobre autorización, uso y transferencia de datos personales y medidas de seguridad específicas para datos sensibles.
Ley 1712 de 2014	Conocida como la Ley de Transparencia, regula el acceso

	a la información pública, garantizando medidas de confidencialidad y protección de datos personales.
Decreto 886 de 2014	Detalla la obligación de actualizar y gestionar las bases de datos en el Registro Nacional de Bases de Datos (RNBD), incluyendo medidas para prevenir riesgos en su manejo.
Decreto Ministerial 1078 de 2015:	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
Decreto Presidencial 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".
Acuerdo 03 de 2015	Del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos
Circular Externa 005 de 2017	Lineamientos de la SIC para proteger datos personales y realizar evaluaciones de impacto de privacidad (PIAs), con controles específicos en entidades públicas y privadas.
ISO/IEC 27001 (Referencia Internacional)	Estándar para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), utilizado como base para controles técnicos y organizativos.
ISO/IEC 27701 (Referencia Internacional)	Extensión de ISO 27001, que integra la gestión de la privacidad de los datos personales en los sistemas de información.
NIST SP 800-53 (Referencia Internacional)	Ofrece un conjunto de controles para la seguridad y privacidad de sistemas de información, utilizado en algunos sectores especializados.
Sector Financiero (Normas Específicas)	La Superintendencia Financiera regula la gestión de riesgos operativos en el sector financiero a través de circulares y directrices específicas.
Sector Salud (Normas Específicas)	Ley 23 de 1981 (secreto profesional) y Resolución 1995 de 1999, que regula la protección de la historia clínica como dato confidencial.
Sector Gobierno	Decreto 2609 de 2012 sobre gestión documental,

(Normas Específicas)	incluyendo la seguridad y protección de archivos gubernamentales.
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 generale 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.
Resolución Ministerial 00500 de 2021:	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital".
Decreto Presidencial 767 de 2022:	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

8. TRATAMIENTO DE RIESGOS SEGURIDAD DE LA INFORMACIÓN.

Una vez se conocen todos los activos de información, así como su nivel de importancia, y las posibles repercusiones económicas, legales y reputacionales que pueden derivarse de cualquier afectación a la disponibilidad, integridad y confidencialidad de la información. Por lo tanto, es necesario implementar ciertas medidas para gestionar adecuadamente el riesgo asociado.

a. Identificación del riesgo

- Fuentes de riesgo: Identificar qué activos, vulnerabilidades, amenazas y consecuencias están implicados.
- Contexto: Evaluar el entorno interno y externo que influye en los riesgos.

b. Evaluación del riesgo

La evaluación comprende:

- Análisis de riesgo: Determinar la probabilidad de que ocurran los riesgos identificados y sus impactos potenciales.
- Valoración: Clasificar los riesgos según su nivel (alto, medio, bajo) basándose en criterios definidos previamente.

c. Selección de opciones de tratamiento.

Existen cuatro opciones principales para tratar un riesgo:

- Mitigar: Reducir el riesgo implementando controles de seguridad o medidas correctivas.
- Transferir: Delegar el riesgo a terceros (seguros, contratos con proveedores, etc.).
- Evitar: Eliminar el riesgo al no realizar ciertas actividades asociadas a este.
- Aceptar: Reconocer el riesgo, sin tomar medidas adicionales, si está dentro de los niveles tolerables.

d. Plan de tratamiento de riesgos

Se elabora un plan que debe incluir:

- Controles específicos: Acciones o herramientas diseñadas para reducir riesgos a niveles aceptables.
- Responsables: Quiénes ejecutarán e implementarán cada control.
- Tiempos: Calendario para implementación.
- Recursos necesarios: Materiales, humanos y financieros.

e. Implementación de controles

Algunos ejemplos de controles pueden ser:

- Medidas técnicas (firewalls, cifrado, control de accesos).
- Políticas y procedimientos (gestión de contraseñas, clasificación de la información).
- Capacitación y concientización del personal.

f. Monitoreo y revisión

- Realizar revisiones periódicas para asegurarse de que los controles implementados son efectivos.
- Actualizar el análisis de riesgos para adaptarse a cambios en el entorno o en los sistemas de la organización.

g. Documentación

- Registro: Mantener un registro actualizado de los riesgos, decisiones y acciones tomadas.
- Auditorías: Facilitar inspecciones internas y externas para evaluar la conformidad y eficacia del tratamiento.

Este enfoque estructurado permite gestionar los riesgos de manera continua, asegurando que las amenazas se mitiguen adecuadamente y los objetivos de la seguridad de la información se cumplan.

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

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.

8.1.1. 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

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

8.1.3. 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 auditorías, de los mapas de riesgos y planes de acción.
- Socialización de resultados

9. METODOLOGÍA DE IMPLEMENTACIÓN

Esta metodología ofrece un esquema organizado para la administración de riesgos en organizaciones públicas, con el objetivo de identificar, evaluar y reducir los riesgos de forma eficiente.

Paso	Descripción
Política de administración del riesgo	Declaración de la Dirección y las intenciones generales de una organización con respecto a la administración del riesgo [2].
Identificación del riesgo	Proceso de encontrar, reconocer y describir los riesgos que podrían afectar la consecución de los objetivos de la organización [2].
Valoración del riesgo	Evaluar la probabilidad y el impacto de cada riesgo identificado [2].

La metodología de implementación del tratamiento de riesgos en seguridad de la información consta de un conjunto de pasos estructurados, enfocados en gestionar de manera efectiva los riesgos que afectan a la confidencialidad, integridad y disponibilidad de la información. Esta metodología generalmente sigue un enfoque alineado con normas como ISO/IEC 27001 e incluye las siguientes fases:

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

9.1. Metodología para la administración del riesgo

9.1.2. Etapas de metodología

I. Contexto y Alcance

Definir el marco y los límites de la gestión del tratamiento de riesgos.

Actividades clave:

- Establecer el alcance del sistema de gestión (activos, procesos, áreas).
- Identificar objetivos y criterios para la evaluación y tratamiento de riesgos.
- Determinar las partes interesadas y sus expectativas (clientes, reguladores, empleados).

Entregables:

- Documento de alcance y objetivos de gestión de riesgos.
- Identificación de partes interesadas.

II. Identificación de Riesgos

Descubrir las posibles amenazas, vulnerabilidades y sus consecuencias sobre los activos de información.

Actividades clave:

- Realizar un inventario de activos.
- Identificar vulnerabilidades en los activos.
- Determinar las amenazas y evaluar las posibles consecuencias.

Entregables:

- Lista de activos de información.
- Mapa de amenazas y vulnerabilidades.

III. Análisis y Evaluación de Riesgos

Medir los riesgos en función de su probabilidad e impacto para priorizarlos.

Actividades clave:

- Estimar el impacto financiero, operacional, legal o reputacional de un riesgo.
- Calcular la probabilidad de que ocurra cada riesgo.
- Clasificar y priorizar riesgos según su nivel crítico (alto, medio o bajo).

Entregables:

- Matriz de evaluación de riesgos.
- Registro priorizado de riesgos.

IV. Definición de Estrategias de Tratamiento

Seleccionar y justificar las acciones que se tomarán para gestionar los riesgos identificados.

Opciones de tratamiento:

- Mitigar: Reducir la probabilidad o impacto del riesgo.
- Evitar: Eliminar la actividad que genera el riesgo.
- Transferir: Delegar el riesgo a terceros (seguros, contratos, etc.).
- Aceptar: Tolerar el riesgo si es bajo y manejable.

Entregables:

- Documentación de decisiones estratégicas de tratamiento.

V. Plan de Tratamiento de Riesgos

Desarrollar un plan detallado para implementar los controles necesarios.

Actividades clave:

- Seleccionar controles de seguridad (por ejemplo, basados en ISO/IEC 27002).
- Definir responsables y recursos para la ejecución del plan.
- Establecer cronogramas y plazos de implementación.

Entregables:

- Plan de tratamiento de riesgos.
- Lista de controles de seguridad seleccionados.

VI. Implementación de Controles

Aplicar las medidas necesarias para tratar los riesgos.

Actividades clave:

- Establecer políticas y procedimientos.
- Configurar herramientas técnicas (firewalls, cifrado, autenticación).
- Capacitar al personal en los controles implementados.

Entregables:

- Controles operativos.
- Procedimientos documentados.
- Evidencias de formación del personal.

VII. Supervisión y Mejora Continua

Garantizar la efectividad de los controles implementados y actualizar la gestión de

riesgos.

Actividades clave:

- Realizar auditorías internas sobre los controles implementados.
- Monitorear los riesgos residuales y nuevos.
- Incorporar ajustes o mejoras basados en incidentes y cambios en el entorno.

Entregables:

- Informes de auditoría y monitoreo.
- Actualizaciones del registro de riesgos.

VIII. Comunicación y Documentación

Mantener un registro claro y comunicar los avances a las partes interesadas.

Actividades clave:

- Generar informes periódicos sobre el estado de los riesgos y controles.
- Documentar las acciones realizadas y los resultados obtenidos.
- Informar a la alta dirección y a los equipos relevantes.

Entregables:

- Informe final de gestión de riesgos.
- Evidencias de cumplimiento para auditorías.

10. Clasificación de riesgos.

La **clasificación de riesgos** en la seguridad de la información es una etapa clave dentro del proceso de gestión de riesgos y consiste en categorizar y priorizar los riesgos en función de su probabilidad de ocurrencia y su impacto. Esta clasificación facilita la toma de decisiones sobre cómo tratarlos.

10.1. Criterios para la clasificación de riesgos

Los riesgos generalmente se evalúan considerando dos factores principales:

a. Probabilidad

Evalúa la posibilidad de que un evento o amenaza ocurra. Se puede clasificar en niveles como:

- **Alta**: La amenaza es muy probable y podría ocurrir frecuentemente.
- **Media**: La amenaza puede ocurrir en ciertas circunstancias.
- **Baja**: Es poco probable que la amenaza ocurra.

b. Impacto

Refleja la gravedad de las consecuencias si el evento ocurre. Se considera el efecto sobre:

- Confidencialidad (exposición o acceso indebido a datos).
- Integridad (alteración de información).
- Disponibilidad (interrupción de servicios).

Clasificaciones comunes:

- **Alto**: Impacto significativo sobre los procesos, finanzas, reputación u obligaciones legales.
- **Medio**: Consecuencias gestionables que podrían afectar temporalmente la operación.
- **Bajo**: Consecuencias menores con poco efecto sobre el negocio.

10.2. Clasificación basada en el nivel de riesgo

Para combinar probabilidad e impacto, se utiliza una **matriz de riesgos**, que cruza ambos criterios y clasifica los riesgos en niveles. Por ejemplo:

	Bajo impacto	Medio impacto	Alto impacto
Baja probabilidad	Riesgo Bajo	Riesgo Bajo	Riesgo Medio
Media probabilidad	Riesgo Bajo	Riesgo Medio	Riesgo Alto
Alta probabilidad	Riesgo Medio	Riesgo Alto	Riesgo Crítico

Clasificaciones típicas de niveles:

- **Riesgo bajo:** Riesgo aceptable sin necesidad de acciones adicionales. Se puede monitorear.
- **Riesgo medio:** Puede requerir medidas para reducirlo si los recursos están disponibles.
- **Riesgo alto:** Debe tratarse prioritariamente con controles de seguridad específicos.
- **Riesgo crítico:** Acciones inmediatas son necesarias, ya que representa una amenaza grave para la organización.

10.3. Categorías de riesgos

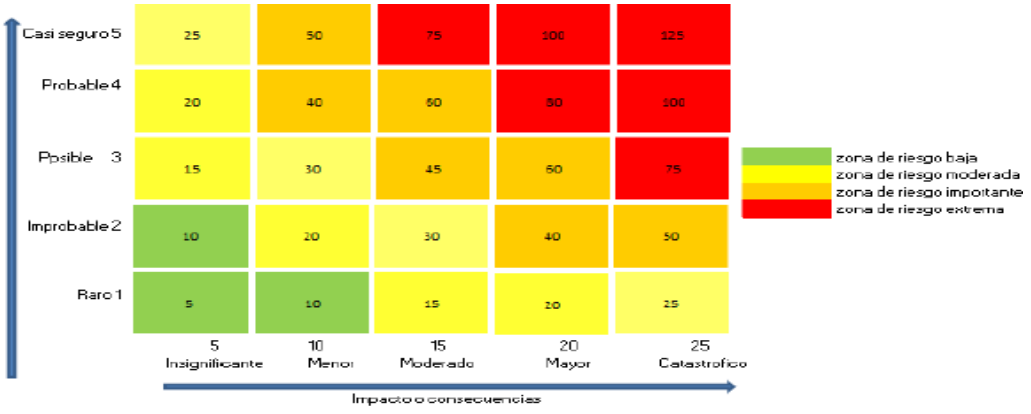
Además de clasificar por nivel, los riesgos pueden categorizarse según su naturaleza:

- **Riesgos tecnológicos:** Fallos en software, ataques cibernéticos, pérdida de datos.
- **Riesgos humanos:** Errores, negligencia, o falta de capacitación.
- **Riesgos físicos:** Daños por desastres naturales, robos o interrupción de servicios eléctricos.
- **Riesgos regulatorios:** Incumplimiento de leyes y normativas.
- **Riesgos operativos:** Interrupción de procesos críticos.

10.4. Priorización

Con base en la clasificación, los riesgos se priorizan para determinar el orden en el que se deben abordar:

- **Riesgos críticos y altos:** Requieren atención inmediata y controles estrictos.
- **Riesgos medios:** Se tratan si los recursos lo permiten, ajustándose al nivel aceptable de la organización.
- **Riesgos bajos:** Se monitorean, pero no suelen implicar acciones inmediatas.



Ejemplo Niveles del Calificación Riesgo

11. Evaluación del riesgo

La evaluación de riesgos en la seguridad de la información es una parte esencial del proceso de gestión de riesgos. Consiste en analizar, medir y priorizar los riesgos identificados para determinar su nivel y planificar las medidas de tratamiento adecuadas. Este proceso debe ser sistemático, objetivo y basado en criterios claros. Acciones para valorar el riesgo

- Identificar los controles existentes.
- ¿Quién lleva a cabo el control? Responsable.
- ¿Qué busca hacer el control? Objetivo.
- ¿Cómo se lleva a cabo el control? Procedimiento.
- Evidencia de la ejecución del control
- ¿Tipo de control? Manual o automático.
- ¿Cuándo se realiza el control? Periodicidad.
-

11.1 Objetivo de la evaluación de riesgos

El objetivo principal es:

- Determinar el nivel de riesgo para cada activo identificado.
- Priorizar los riesgos según su importancia.
- Proporcionar la información necesaria para decidir el tratamiento adecuado.

11.2 Naturaleza del control

- **Preventivo:** Evitan que el evento suceda. Ej.: Capacitación del personal, evitar la producción de errores.
- **Detectivo:** Permiten registrar un evento después de que ha sucedido. Ej.: Programa de auditoría, para evidenciar errores que no fueron corregidos con controles preventivos**.**
- **Correctivo:** No prevén que un evento suceda, pero permiten enfrentar la situación una vez ha sucedido. Ej.: Pólizas de seguro, recuperar la operación.

11.3 Revisión y seguimiento.

Determinar Eficacia de la implementación, realizar revisiones periódicas, lecciones aprendidas, detectar cambios en el contexto externo e interno, criticidad de los riesgos, acciones de tratamiento.

11.4 Fases de la evaluación de riesgos

La evaluación consta de tres etapas clave:

a. Análisis de riesgos

Se centra en comprender los riesgos y calcular su nivel combinando los factores de

b. probabilidad e impacto:

Identificar factores:

- **Amenazas:** Eventos que podrían explotar vulnerabilidades.
- **Vulnerabilidades:** Debilidades que podrían ser explotadas.
- **Impactos:** Consecuencias sobre los activos si se materializan las amenazas.

1. **Cuantificar probabilidad:** Determinar la posibilidad de que el riesgo ocurra.
2. **Evaluar impacto:** Analizar las consecuencias que tendría un incidente en aspectos como confidencialidad, integridad y disponibilidad.

c. Medición del nivel de riesgo

Se utiliza una fórmula básica para calcular el nivel de riesgo:

Riesgo = Probabilidad × Impacto

Según la metodología, la medición puede ser:

- **Cualitativa:** Usa términos subjetivos como bajo, medio o alto para la probabilidad e impacto.
- **Cuantitativa:** Usa valores numéricos para calcular el nivel de riesgo con mayor precisión (por ejemplo, de 0 a 10 para probabilidad e impacto).

12. 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