PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EMPRESA DE SERVICIOS PÚBLICOS DE VALLEDUPAR – EMDUPAR S.A. ESP

VIGENCIA 2026

ELABORO:	***REVISO:***	***APROBO:***
FAUSE RIZCALA MUVDI	FAUSE RIZCALA MUVDI	EDUARDO MESA BUITRAGO
Jefe División Sistemas de Información	***Jefe División Sistemas de Información***	***Agente Especial***

TABLA DE CONTENIDO

INTRODUCCIÓN 3

GLOSARIO DE TÉRMINOS Y DEFINICIONES 4

1. OBJETIVOS ---------- 6
1.1. OBJETIVO GENERAL 6
1.2. OBJETIVOS ESPECIFICOS 6
2. NORMATIVIDAD 6
3. PLAN DE ACCIÓN PARA TRATAMIENTO DE RIESGOS 7
3.1. Identificación y valoración riesgos en activos de información 8
3.2. Tratamiento de riesgos 11
3.2.1. Materialización 11
3.3. Seguimiento y control 12
4. CRONOGRAMA 15
5. RECURSOS 15
6. INDICADORES 17

INTRODUCCION

La información que gestiona, custodia y preserva EMDUPAR S.A. ESP para el cumplimiento de sus objetivos estratégicos es un activo valioso fundamental para crecer, innovar y ser competitiva. Por esta razón se requiere que la información sea protegida de manera adecuada y que sea resguardada de cualquier posibilidad de alteración, mal uso o perdida.

Dentro del modelo de Seguridad y Privacidad de la información (MSPI), un tema fundamental es la Gestión de riesgos que tiene como objetivo identificar, analizar, medir y encargarse de los riesgos asociados a la seguridad de la información y establecer controles de forma preventiva contra las amenazas que se puedan encontrar y además conseguir reducirlas.

Para el desarrollo del Plan de tratamiento de Riesgos se utilizó la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la función Pública DAFP en su versión No. 6.

Es importante resaltar que para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA. Mediante la definición del Plan de Tratamiento de Riesgos se busca establecer medidas para mitigar los riesgos presentes en su análisis (perdida de confidencialidad, perdida de integridad y perdida de disponibilidad de los activos de información) evitando situaciones que generen incertidumbre en el cumplimiento de los objetivos de EMDUPAR S.A. ESP.

GLOSARIO DE TERMINOS Y DEFINICIONES

Activo: cualquier elemento que tenga valor para la organización. Sin embargo, en el contexto de seguridad digital, son activos elementos tales como: aplicaciones, servicios web, redes, información física o digital, tecnologías de información TI y tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital.

Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Análisis del riesgo: Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.

Causa: Elemento específico que origina el evento.

Controles o Medida: protección o contramedida que permite reducir o mitigar un riesgo. Pueden ser procesos, políticas y/o actividades que pueden modificar el riesgo.

Criterios de riesgos: Términos de referencia frente a los cuales se evaluará la importancia del riesgo.

Evaluación del Riesgo: Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.

Evento: Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Identificación del riesgo: Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos del mismo

Impacto: consecuencias que puede ocasionar a la organización la materialización del riesgo.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

Riesgo: Efecto que se causa sobre los objetivos de las organizaciones debido a eventos potenciales.

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).

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Establecer el Plan de Tratamiento para los riesgos de seguridad y privacidad de la información identificados en los procesos de la Universidad Popular del Cesar.

1.2. OBJETIVOS ESPECIFICOS

- Identificar los activos de información de cada proceso y los riesgos presentes en cada uno de ellos: pérdida de la confidencialidad, pérdida de la integridad y pérdida de la disponibilidad.
- Establecer el nivel de riesgo
- Definir el Plan de tratamiento
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos formulado.

2. NORMATIVIDAD

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 1008 de 2018: 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.

Manual para la Implementación de la Política de Gobierno Digital: Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2)

Versión 7, abril de 2019

Modelo de Seguridad y privacidad de la información - MSPI Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta

transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales

NTC / ISO 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).

NTC/ISO 31000:2009 Gestión del Riesgo. Principios y directrices.

Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 6 Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública, noviembre de 2022.

3. PLAN DE ACCION PARA TRATAMIENTO DE RIESGOS

El plan propuesto en este documento comprende, como se detallará más adelante, las siguientes actividades principales: identificación y valoración de riesgos, evaluación de riesgos, tratamiento de riesgo y aceptación del riesgo, guardando coherencia con la Guía para la administración del riesgo y el diseño de controles en entidades públicas V6, emitida por el Departamento Administrativo de la Función Pública.

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2013):

Ciclo PHVA y la Gestion de riesgos

3.1. Identificación y valoración de riesgos en activos de información

Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información de cada proceso. La institución debe saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

La Universidad realizará los siguientes pasos para la identificación de los activos de información y organizará la información de acuerdo a lo establecido en la sección 3.1.6. del anexo 4 *"Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas"* que hace parte de los anexos de la *"Guía para la Administración del Riesgo y el diseño de controles en entidades públicas"*, del Departamento Administrativo de la Función Pública (DAFP) en su versión no. 6.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

Dentro de la Identificación del riesgo, se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- ✓ Pérdida de la confidencialidad ✓
  Pérdida de la integridad
- ✓ Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Para este efecto se recomienda, consultar el Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas donde se encuentran las siguientes tablas necesarias para el análisis: tabla de amenazas comunes, tabla de amenazas dirigida por el hombre y tabla de vulnerabilidades comunes.

Valoración del riesgo: Para esta etapa se asociarán las siguientes tablas de probabilidad e impacto:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Tabla de Criterios para definir el nivel de probabilidad

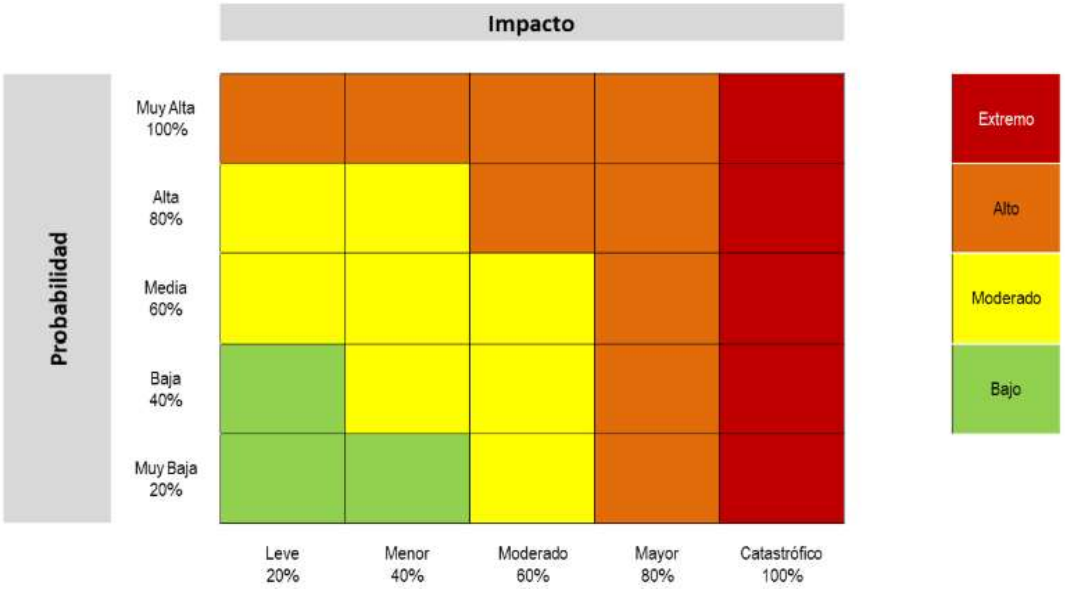
	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Tabla de criterios para definir el nivel de impacto

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto se busca determinar la zona de riesgo inicial (RIESGO INHERENTE). Para el análisis preliminar (riesgo inherente), en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello, se aplica la matriz de calor

Para ello se aplica la siguiente matriz de calor:

Matriz de calor niveles de severidad del riesgo



El proceso de identificación y evaluación de los riesgos de seguridad de la información está compuesto por las siguientes actividades:

1) **Programación de entrevistas con líderes de procesos:** en esta actividad se seleccionan los procesos incluidos en el alcance del SGSI de la Universidad popular del Cesar y se procede a programar y a agendar a los líderes de las dependencias y grupos internos de trabajo que conforman los procesos, para la identificación de riesgos.
2) **Entrevistas:** Se entrevista a cada líder de dependencia o grupo, se presenta la metodología y en conjunto se procede a realizar la identificación de los riesgos sobre los activos de información, los cuales se consignan en la Matriz de Riesgos.
3) **Identificación y Calificación de Riesgos:** En esta etapa, el líder de proceso evalúa el nivel de impacto vs. Probabilidad y los controles existentes para calcular el nivel de riesgo.
4) **Valoración del Riesgo Residual**: en esta fase se hace una proyección de la eficacia de los controles para calcular el riesgo residual.

5) **Mapas De Calor:** se procede a ubicar los riesgos en el mapa de calor para visualizar su comportamiento a medida que se van aplicando los controles.

3.2. Tratamiento de riesgos

Una vez ejecutadas las etapas de análisis y valoración de riesgos, y con base en los resultados obtenidos en la determinación real de riesgos, es necesario tomar decisiones aplicando el apetito de riesgos definido por la Universidad.

Si el riesgo se ubica en una zona no aceptable, cada líder responsable de los riesgos identificados con el apoyo de la Oficina de Informática y sistemas, debe definir e implementar los controles necesarios para llevar el riesgo a un nivel aceptable a través del plan de tratamiento de riesgos. A continuación, se definen las siguientes estrategias de tratamiento, asumir los riesgos bajos y moderados y gestionar el riesgo alto y extremo. En el anexo No, 1 se muestra la estrategia para abordar los riesgos y establecer su tratamiento.

3.2.1. Materialización

En el caso de materializarse un riesgo, este debe ser reportado de acuerdo con el procedimiento de gestión de incidentes de seguridad y privacidad de la información. Así mismo se deberá analizar el riesgo y validar en qué nivel queda posterior a la materialización, registrando los cambios respectivos en el mapa de riesgos. En caso de que se materialice un riesgo que no esté identificado, deberá ser reportado para que se inicie su correspondiente identificación en el mapa de riesgos.

La Universidad Popular del Cesar no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades de mejora. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

3.3. Definición de atributos del control en la gestión de riesgos

En el marco de la gestión institucional del riesgo de seguridad de la información, la identificación, valoración y tratamiento de los riesgos requiere no solo el planteamiento de controles adecuados, sino también la caracterización formal de sus atributos. Estos atributos permiten evaluar la eficacia, trazabilidad, aplicabilidad y sostenibilidad de cada control implementado, conforme a las directrices establecidas por el **Modelo de Seguridad y Privacidad de la Información (MSPI)**, la **ISO/IEC 27001:2013**, la **ISO/IEC 27005** y las buenas prácticas de gestión de riesgos del sector público colombiano.

A continuación, se detallan **los atributos asociados a los controles**, utilizados en la matriz de riesgos de la Universidad. Cada atributo se define con base en estándares internacionales y se acompaña de los valores posibles que pueden adoptarse en su aplicación práctica. Esta estandarización contribuye a la uniformidad del lenguaje técnico, la claridad en los procesos de auditoría interna, y el fortalecimiento del sistema de control interno institucional.

Variables de Atributos del Control

1. Tipo

Descripción:

Define la naturaleza funcional del control según el momento en que actúa frente al riesgo: antes, durante o después del evento.

Valores posibles:

- **Preventivo:** Actúa antes de que ocurra el evento de riesgo. Busca evitar que suceda (ej. autenticación, capacitación).
- **Detectivo:** Identifica o alerta cuando el evento está ocurriendo o ha ocurrido (ej. monitoreo, revisión de logs).
- **Correctivo:** Mitiga el impacto después de que se ha materializado el riesgo (ej. restauración, respuesta ante incidentes).

2. Implementación

Descripción:

Indica si el control se ejecuta automáticamente mediante sistemas, o si requiere intervención humana.

Valores posibles:

- **Automático:** Se ejecuta por medio de sistemas o herramientas tecnológicas sin intervención manual (ej. bloqueo automático, auditoría SIEM).
- **Manual:** Requiere acción humana para su ejecución (ej. revisión de procedimientos, validación por otro funcionario).

3. Documentación

Descripción:

Establece si el control cuenta con respaldo formal en políticas, manuales, procedimientos o formatos registrados.

Valores posibles:

- **Documentado:** Tiene respaldo escrito, oficial o técnico; se puede auditar (ej. procedimiento, política, instructivo).
- **Sin documentar:** Se ejecuta de manera informal o práctica, sin evidencia escrita sistemática.

4. Frecuencia

Descripción:

Define la regularidad con la que se aplica el control. Puede ser constante o ejecutarse en ciclos específicos.

Valores posibles:

- **Continua:** Se ejecuta constantemente, sin interrupción (ej. monitoreo 24/7, cifrado activo).
- **Aleatoria:** Se ejecuta en momentos específicos, planificados o programados de forma no continua (ej. mensual, trimestral, anual, bimensual).

Nota: Aunque “Aleatoria” es el valor que se ingresa, debe ir acompañada en la descripción de su **periodicidad exacta**: mensual, trimestral, etc.

5. Evidencia
Descripción:
Refleja si el control deja trazabilidad o soporte verificable que permita comprobar su ejecución ante una auditoría.

Valores posibles:

- **Con registro:** El control genera evidencia (ej. acta, correo, captura, log, firma, formato).
- **Sin registro:** El control se realiza, pero no deja huella trazable o verificable.

6. Tratamiento
Descripción:
Indica la estrategia definida para manejar el riesgo en función de su impacto y posibilidad de ocurrencia.

Valores posibles:

- **Reducir – Mitigar:** Disminuir la probabilidad o el impacto mediante controles.
- **Reducir – Compartir:** Transferir parte del riesgo a un tercero (ej. contratos, seguros).
- **Evitar:** Eliminar la causa del riesgo suspendiendo o cambiando la actividad.
- **Aceptar:** Reconocer el riesgo y no tomar medidas adicionales, ya que está dentro del umbral de tolerancia.

3.4. Seguimiento y control

El seguimiento y control se realiza de acuerdo a la GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS VERSIÓN 6.

La oficina de informática y sistemas apoyará a los responsables de los procesos en la definición de los controles y hará seguimiento a su implementación, con el fin, de evidenciar en el siguiente ciclo la efectividad
de los controles implementados y en consecuencia la disminución del riesgo de tipo ***No aceptable***. Así mismo, si se llegan a presentar incidentes de seguridad se validarán los riesgos identificados para determinar si obedece a un riesgo identificado y proceder a valorar, recalificar e implementar nuevos controles.

4. CRONOGRAMA

Para dar cumplimiento al ciclo de riesgo, el cronograma se establece anualmente, los riesgos de seguridad digital identificados se reflejarán en el Mapa de Riesgos Institucional, donde se establecerán las acciones de control y las fechas para implementar dichos controles, la oficina de sistemas e informática apoyará el proceso de definición de los controles con los líderes de cada uno de los procesos de la institución.

5. RECURSOS

La estimación y gestión para la asignación de los recursos para el plan de tratamiento de riesgos de Seguridad de la información identificados en la institución, corresponderá al líder del proceso (dueño del riesgo), quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos y del plan de tratamiento.

Si el establecimiento de los controles implica la adquisición de herramientas tecnológicas bajo la responsabilidad de la División de Sistemas de Información, los recursos de inversión se tomarán del proyecto registro en el POAI.

Fortalecimiento de los recursos tecnológicos, mejoramientos de los servicios de seguridad **informática y electrónica de la Plataforma tecnológica de EMDUPAR S.A. ESP.**

6. INDICADORES

La medición se realiza con un indicador de gestión que está orientado principalmente a disminuir el número de riesgos identificados con nivel alto y externo a través de la implementación y evaluación de controles.

El número de riesgos identificados como no aceptables no debe ser superior al 20% del total de riesgos identificados. La División de Sistemas de Información, asesora a las áreas en el proceso de identificación y valoración de los riesgos de seguridad de información y seguridad digital; los líderes de los procesos solicitarán a la Gestión de Planeación, la inclusión de los mismos en el mapa de riesgos institucional, instrumento en donde se registran los riesgos identificados, su valoración y sus controles, para su seguimiento y control.