PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD EN EL INFORMACION

Bello – Antioquia
Enero de 2024

1. INTRODUCCIÓN

El constante crecimiento de la información que las organizaciones manejan hace que aumente el factor del riesgo, lo que hace necesario mantenerla identificada y protegida contra posibles riesgos que se puedan presentar. La ESE Bellosalud administra, recolecta, actualiza, procesa, utiliza, almacena y transfiere información física, digital y electrónica con el propósito de dar cumplimiento a los objetivos estratégicos de la Entidad utilizando mecanismos adecuados para cuidar el derecho a la intimidad personal, familiar y al buen nombre de todos los beneficiarios de la Entidad, permitiendo el acceso a los documentos públicos y evitando el acceso a los que se consideren reservados o confidenciales.

Para lograr la toma de decisiones con base en información de altos estándares de calidad, resolver problemas y prestar los servicios a los ciudadanos y funcionarios de la ESE, es necesario que esta sea real, oportunidad y de acceso a las personas que lo requieren. Internacionalmente la norma ISO 31000 ayuda a establecer un Sistema de Gestión de Riesgos de cualquier tipo, incluyendo riesgos asociados a la información, esto permite reducir las falencias propias de la información a través de un tratamiento continuo y apropiado de los controles que mitiguen las afectaciones negativas a la organización.

El plan de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a la institución minimizar pérdidas y maximizar oportunidades.

El presente documento define las medidas de seguridad identificadas para desarrollar e implementar el plan de tratamiento para los riesgos de Seguridad y Privacidad de la Información.

Lo anterior adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

2. OBJETIVOS.

2.1. GENERAL.

Establecer los conceptos básicos y metodológicos para una adecuada Administración de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital a partir de su identificación, manejo y seguimiento.

2.2. ESPECIFICOS.

• Involucrar y comprometer a todos los funcionarios en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

• Establecer, mediante una adecuada Administración del Riesgo, una base confiable para la toma de decisiones y la planificación institucional.

1. NORMATIVIDAD

- 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 1078 de 2015. “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.”
- 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”
- 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”

2. ALCANCE.

Este plan, proporcionará una metodología establecida por la institución para realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación; que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Orienta sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis y valoración de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

3. DIRECCIONAMIENTO ESTRATEGICO.

LINEA ESTRATEGICA: A la hora de garantizar la seguridad en cualquier entorno, además de tener las medidas técnicas y legales adecuadas es de vital importancia el factor humano, ya que con frecuencia los mayores problemas de seguridad se presentan por errores o descuidos en el hacer diario del personal, por tal motivo se debe capacitar al personal que tiene acceso a la información digital y física de la institución, para minimizar y eliminar el riesgo de pérdida o daño, parcial o total de la información.

4. GESTION DE RIESGO EN LA SEGURIDAD INFORMATICA.

La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo. En su forma general contiene cuatro fases.

4.1. ANALISIS

Determina los componentes de un sistema que requiere protección, las vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.

4.2. CLASIFICACIÓN

Determina si los riesgos encontrados y los riesgos restantes son aceptables.

4.3. REDUCCIÓN

Define e implementa las medidas de protección; además, sensibiliza y capacita los usuarios conforme a las medidas.

4.4. CONTROL

Analizar el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento. Todo el proceso está basado en las llamadas políticas de seguridad, normas y reglas institucionales, que forman el marco operativo del proceso, con el propósito de potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas con el resultado de reducir el riesgo.

Orientar el funcionamiento organizativo y funcional.

Garantizar corrección de conductas o prácticas que nos hacen vulnerables

5. METODOLOGIA DE EVALUACIÓN DEL RIESGO.

Es el primer paso hacia la gestión de riesgos, se necesita definir las reglas para llevar a cabo la gestión de riesgo, ya que querrá que toda la ESE lo haga de la misma forma, el principal problema del plan de tratamiento de riesgos de seguridad de la información es que la institución lo ejecute de diferente forma en las distintas áreas.

6. IDENTIFICACIÓN DEL RIESGO.

La finalidad de esta fase es descubrir, reconocer y registrar los riesgos. Este proceso incluye la identificación de las causas y el origen de los riesgos, los sucesos o situaciones que pueden tener un impacto en los objetivos de la organización

7. METODOS DE IDENTIFICACIÓN DEL RIESGO PUEDEN INCLUIR.

Métodos basados en evidencias como pueden ser, las listas de verificación y las revisiones de datos históricos. Enfoques sistemáticos de equipos, como los grupos de expertos que siguen un método con una sistemática estructurada de preguntas para identificar los riesgos.

8. ANALISIS DEL RIESGO.

Esta fase implica una comprensión del riesgo, es decir, determinar sus consecuencias y probabilidades, teniendo en cuenta la presencia y la eficacia de los

controles existentes. Los métodos que se utilizan para este análisis de riesgos pueden ser cualitativos, semicuantitativos o cuantitativos. La apreciación cualitativa se suele expresar con niveles del tipo “alto”, “medio” y “bajo” para definir las consecuencias, las probabilidades o el nivel de riesgo. Los métodos semicuantitativos utilizan escalas de valoración numérica lineales o logarítmicas principalmente.

El análisis cuantitativo trabaja con valores numéricos realistas y obtiene el mismo tipo de resultados. El problema suele ser que, en ocasiones, junto a estos valores deben tenerse en cuenta otros factores difícilmente cuantificables o simplemente que faltan datos.

9. EVALUACIÓN DEL RIESGO

En la fase de evaluación se toman las decisiones sobre las acciones futuras basadas en el conocimiento del riesgo que se ha obtenido durante la fase de análisis. En la mayoría de las ocasiones, el criterio para tomar la decisión de, si se debe tratar el riesgo y cómo hacerlo, depende de los costos/beneficios de aceptar el riesgo y/o de implantar los controles pertinentes. El criterio de “tan bajo como razonablemente sea posible” es un clásico de este enfoque de criterio.

10. ELECCIÓN DE LAS TECNICAS DE APRECIACIÓN DEL RIESGO

Llega el momento clave de ver que técnica/herramienta vamos a elegir. Los principales factores a tener en cuenta son:

- La disposición de recursos adecuados en tiempo y experiencia, así como el presupuesto con el que contamos.
- La naturaleza y el grado de la incertidumbre, que depende de la calidad, cantidad e integridad de los datos e información disponible sobre los riesgos considerados.
- La complejidad de los riesgos

11. COMPONENTES DE LA IDENTIFICACIÓN DEL RIESGO

11.1. CAUSAS DEL RIESGO.

Son las causas, uno de los aspectos a eliminar o mitigar para que el riesgo no se materialice; esto se logra mediante la definición de controles efectivos. Para realizar el análisis de las causas existen varias técnicas, Usualmente se utiliza la técnica de lluvia de ideas para identificar todo aquello que puede ser considerado dentro del análisis de riesgos y para que esta sea eficaz, se debe considerar que:

- Debe haber un moderador que tome nota y que organice las exposiciones de todos los participantes, indicando el tiempo que cada cual tiene para presentar sus ideas.
- Es más importante la cantidad de ideas que la calidad de las mismas. Todas las ideas son valiosas para el proceso de recopilación de información.
- No se deben calificar las ideas como buenas o malas, son simplemente puntos de vista que capitalizados pueden brindar alternativas no consideradas.
- Es importante soportarse en las ideas de los otros. Es decir, agregar valor a las apreciaciones de otros o considerar situaciones a partir de las mismas.
- El análisis de las ideas se debe realizar al final, por el moderador, quien las organizará y las expondrá a manera de resultado.
- Todos deben participar de manera equitativa, es importante no fijar la atención en pocos participantes, ni mantenerse en la palabra sin dar la oportunidad a otro de expresar sus ideas.

11.2. CONSECUENCIAS

Son los efectos que se generan o pueden generarse con la materialización del riesgo sobre los objetivos de los procesos y de la ESE; dichos efectos generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

Se debe determinar las consecuencias del riesgo en escala ascendente; definiendo cual podría ser el efecto menor que puede causar la materialización del riesgo hasta llegar al efecto mayor generado.

12. CLASIFICACION DE LOS RIESGOS

Durante la etapa de identificación, se realiza una clasificación del riesgo, según sus características, con el fin de orientar la formulación de un tratamiento adecuado que posibilite la mitigación del riesgo mediante la definición de controles y planes de manejo:

CLASE DE RIESGO	DEFINICIÓN
ESTRATÉGICO	Son los riesgos relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia
OPERATIVO	Relacionados con el funcionamiento y operatividad de los sistemas de información de la entidad: definición de procesos, estructura de la entidad, articulación entre dependencias.
FINANCIEROS	Relacionados con el manejo de los recursos de la entidad: ejecución presupuestal, elaboración estados financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes
CUMPLIMIENTO	Capacidad de cumplir requisitos legales, contractuales, ética pública y compromiso con la comunidad.
TECNOLOGÍA	Capacidad para que la tecnología disponible satisfaga las necesidades actuales y futuras y el cumplimiento de la misión
IMAGEN	Tienen que ver con la credibilidad, confianza y percepción de los usuarios de la entidad.

ESCALA PARA CALIFICAR LA PROBABILIDAD DEL RIESGO		
NIVEL	**CONCEPTO**	**FRECUENCIA**
RARO	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años
IMPROBABLE	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
MODERADO	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
PROBABLE	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos 1 vez en el último año
CASI CERTEZA	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

ESCALA PARA CALIFICAR EL IMPACTO DEL RIESGO							
Tipo de efecto o impacto		Estratégicos	Operativos	Financieros	Cumplimiento	Tecnología	Imagen
INSIGNIFICANTE	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos o bajos sobre la institución	Afecta el cumplimiento de algunas actividades	Genera ajustes a una actividad concreta	La pérdida financiera no afecta la operación normal de la institución	Genera un requerimiento	Afecta a una persona o una actividad del proceso	Afecta a un grupo de servidores del proceso
MENOR	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la institución	Afecta el cumplimiento de las metas del proceso	Genera ajustes en los procedimientos	La pérdida financiera afecta algunos servicios administrativos de la institución	Genera investigaciones disciplinarias, y/o fiscales y/o penales	Afecta el proceso	Afecta a los servidores del proceso
MODERADO	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la Institución	Afecta el cumplimiento de las metas de un grupo de procesos	Genera ajustes o cambios en los procesos	La pérdida financiera afecta considerablemente la prestación del servicio	Genera interrupciones en la prestación del bien o servicio	Afecta varios procesos de la institución	Afecta a todos los servidores de la institución
MAYOR	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la institución	Afecta el cumplimiento de las metas de la institución	Genera intermitencia en el servicio	La pérdida financiera afecta considerablemente el presupuesto de la institución	Genera sanciones	Afecta a toda la institución	Afecta el sector
CATASTROFICO	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la institución	Afecta el cumplimiento de las metas del sector y del gobierno	Genera paro total de la institución	Afecta al presupuesto de otras entidades	Genera cierre definitivo de la institución	Afecta al municipio	Afecta al municipio, Todos los usuarios de la institución

13. VALORACIÓN DE LOS RIESGOS

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo. Lo anterior de acuerdo con los formatos Identificación y evaluación de controles y Valoración del riesgo.

14. IDENTIFICACIÓN DE CONTROLES

Los controles son las acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo; estos, deben estar directamente relacionados con las

causas o las consecuencias identificadas para el riesgo y eliminarlas o mitigarlas. La administración del riesgo contribuirá a la gestión de la entidad, en la medida en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

A continuación, se presentan las características mínimas que se deben tener en cuenta para la definición de los controles

CARACTERISTICAS	DESCRIPCIÓN
Objetivos	No dependen del criterio de quien lo define y/o ejecute, sino de los resultados que se esperan obtener
Pertinentes	Están directamente orientados a atacar las causas o consecuencias del riesgo
Realizable	Se deben definir controles que la entidad o el proceso esté en capacidad de llevar a cabo
Medibles	Permiten el establecimiento de indicadores para verificar el cumplimiento de su aplicación y/o efectividad
Periódicos	Tienen frecuencia de aplicación en el tiempo
Efectivos	Eliminan o mitigan las causas o consecuencias y evitan la materialización del riesgo
Asignables	Tienen responsables definidos para su ejecución

15. ETAPAS PARA LA ADMINISTRACION DEL RIESGO

A continuación, se presenta cada una de las etapas a desarrollar durante la administración del riesgo; en la descripción de cada etapa se desplegarán los aspectos conceptuales y operativos que se deben tener en cuenta.

- **Contexto estratégico:** Determinar los factores externos e internos del riesgo.
- **Identificación:** Identificación de causas, riesgos, consecuencias y clasificación del riesgo.
- **Análisis:** Calificación y evaluación del riesgo inherente.
- **Valoración:** identificación y evaluación de controles, incluye la determinación del riesgo residual.
- **Manejo**: determinar, si es necesario, acciones para el fortalecimiento de los controles.
- **Seguimiento:** evaluación integral de los riesgos.

16. SEGUIMIENTO DE RIESGOS

Cada 6 meses se realizará seguimiento a todo el componente de administración de riesgos y verificará aspectos como:

Cumplimiento de las políticas y directrices para la administración del riesgo: Metodología de Administración del Riesgo (diseño y funcionamiento).

Administración de los riesgos por proceso e institucionales: calificación y evaluación, efectividad de los controles y cumplimiento de las acciones.

Los resultados de la evaluación y las observaciones de la persona que haga las veces de auditor deben ser presentados, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo en la organización.

17. DEFINICIONES

- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **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).
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.
- **Control o Medida**: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

ALEXIS ALBERTO AGUDELO GOMEZ
Subgerente Administrativo y Financiero

SEGUIMIENTO, CONTROL Y MEJORA

Las acciones y actividades articuladas al plan de acción de acuerdo a lo estipulado en el decreto 612 de 2018 se encuentran diligenciadas en el formato establecido para tal fin.

MODIFICACIONES

Versión	Fecha	Razón
01	31/01/2021	Plan de tratamiento de riesgos de seguridad y privacidad de la información
02	31/01/ 2022	Actualización para vigencia 2022
03	31/01/2023	Actualización para vigencia 2023
03	30/01/2024	Actualización para vigencia 2024

APROBACIÓN.

Elaboró	Revisó	Aprobó
Ingeniero de Sistemas	Subgerente Administrativo y Financiero	Gerente