Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024

Zulma Cristina Montaña Martínez
Gerente

PARTICIPANTES:

Zulma Cristina Montaña Martínez
Gerente

Andrea Del Pilar Chona Bolívar
Subgerente Administrativo y financiero

Camilo Andrés Rodríguez Farfán
Técnico Operativo

Cesar David Parra Guerrero
Asesor de Planeación

TABLA DE CONTENIDO

INTRODUCCIÓN

El plan de tratamiento de riesgos en conjunto con la política de privacidad y seguridad de la información, se fundamenta en una orientación estratégica que busca fomentar el desarrollo de una cultura preventiva. Se pretende que, al comprender tanto el concepto de riesgo como el contexto, se diseñen acciones preventivas que minimicen el impacto en la E.S.E CRIB en caso de materialización. Además, se procura desarrollar estrategias más objetivas para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos. Esto se hace evidente al comunicar las situaciones que podrían comprometer el cumplimiento de los objetivos establecidos en esta política para el Desarrollo Digital.

Este enfoque responde a las exigencias normativas del estado colombiano, en específico, CONPES 3854 de 2016 y el decreto 1008 de 14 de junio de 2018. Además, se adoptan buenas prácticas y lineamientos de estándares reconocidos, tales como ISO 27005:2013, 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.

La definición del Plan de Tratamiento de Riesgos tiene como objetivo principal mitigar los riesgos identificados durante el análisis de riesgos, enfocándose en la pérdida de la confidencialidad, integridad y disponibilidad de los activos. Esto se traduce en evitar situaciones que puedan obstaculizar el logro de los objetivos institucionales.

Este plan se estructura para evaluar las acciones necesarias para mitigar los riesgos existentes, organizándolas como medidas de seguridad. En la cual la medida se detalla con su nombre, objetivo, justificación, responsable y prioridad correspondiente.

Las medidas previas se han definido cuidadosamente, tomando en consideración la información obtenida del análisis de riesgos. Este análisis de las necesidades especificas del Proceso de Tecnología de la Empresa Social del Estado Centro de Rehabilitación Integral de Boyacá en cuanto a la seguridad de la información, ofreciendo las herramientas necesarias para caracterizar cada medida y establecer los pasos a seguir para su ejecución.

1. NOMBRE DEL PLAN SEGÚN DECREO 612 2018

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

2. DIAGNOSTICO

Se requiere integrar el sistema de gestión de riesgos de la ESE CRIB con los criterios concernientes de seguridad y privacidad de la información, conforme a las directrices establecidas en la guía para la administración del riesgo y el diseño de controles en entidades públicas. Como resultado será la implementación de las políticas:

• Política de privacidad y seguridad de la información

• Política de gestión de riegos

3. MARCO NORMATIVO:

- Ley 100 de 1993 "Por la cual se crea el sistema de seguridad social integral y se dictan otras disposiciones"
- Ley 152 de 1994 "por la cual se establece la Ley Orgánica del Plan de Desarrollo"
- Decreto 1876 de 1994 "por el cual se reglamentan los artículos 96,97 y 98 del Decreto-ley 1298 de 1994 en lo relacionado con las Empresas Sociales del Estado"
- Ley 1438 de 2011 "por medio de la cual se reforma el Sistema General de Seguridad Social en Salud y se dictan otras disposiciones."
- Norma NTC ISO 27001:2013 "Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad del Información (SGSI)"
- Ley 1474 de 2014 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública"
- Ley 1757 de 2015 "*Por la cual se dictan disposiciones en materia de promoción y protección del derecho a la participación democrática*"
- Decreto 1082 de 2015 "Por medio del cual se expide el decreto único reglamentario del sector administrativo de planeación nacional"
- Decreto 1083 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública. - Esta versión incorpora las modificaciones introducidas al Decreto Único Reglamentario del Sector de Función Pública a partir de la fecha de su expedición"
- Decreto 1583 de 2015 "*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública*"
- CONPES 3854 de 2016 "Política Nacional de Seguridad digital"

- Decreto 1499 de 2017 *"Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015"*

- 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."*

- Norma Técnica Colombiana ISO 27005:2018 "Tecnologías de la Información. Técnicas de seguridad. Gestión del Riesgo de la seguridad de la Información"

- Norma Técnica ISO 31000:2018 "Directrices de la gestión del riesgo".

- Ley 1955 de 2019 "Plan de desarrollo 2018-2022 "Pacto por Colombia, Pacto por la equidad"

- Acuerdo N° 100.03.01.03 de 17 de julio de 2020 de junta directiva "Por el cual se aprueba el plan de desarrollo institucional de la Empresa Social del Estado Centro de Rehabilitación Integral de Boyacá para la vigencia fiscal 2020-2023"

4. DEFINICIONES:

- **Riesgo:** es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.

- **Riesgo de seguridad digital:** es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan.

- **Gestión de riesgos de seguridad digital:** es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.

- **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

5. OBJETIVO GENERAL:

Implementar la política de gestión de riesgos vinculándola con la política de privacidad y seguridad de la información de la Empresa Social Del Estado Centro De Rehabilitación Integral de Boyacá, garantizando la confiabilidad e integridad de la información manejada por la ESE CRIB

6. OBJETIVOS ESPECIFICOS:

- Implementar las políticas de privacidad y seguridad de la información y la política de gestión de riesgos en la E.S.E CRIB. Este enfoque estratégico tiene como finalidad alcanzar los objetivos, la misión y la visión institucional, asegurando la protección y preservación de la integridad, confidencialidad, disponibilidad y autenticidad de la información de la entidad.

- Garantizar el cumplimiento de los requisitos legales y reglamentarios establecidos por la legislación colombiana

- Administrar de manera efectiva los riesgos asociados con la política de Privacidad y Seguridad de la información, política de gobierno digital y la continuidad del servicio, siguiendo los modelos y directrices establecidos por el MIN tic y el DAFP para garantizar un enfoque integral y alineado con las mejores prácticas del sector.

- Potenciar y consolidar el conocimiento relacionado con la política de gestión de riesgos en Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, para asegurar una mejora continua y un desempeño óptimo en estas áreas críticas.

7. METODOLOGÍA:

El plan de tratamiento de riesgos de seguridad y privacidad de la información cuenta con la metodología contemplada en las normas NTC ISO 3100:2018, ISO 27005:2018, y en la guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.

Se hace necesario integrar la política de seguridad y privacidad de la información con la política de gestión de riesgos, siguiendo los lineamientos del DAFP

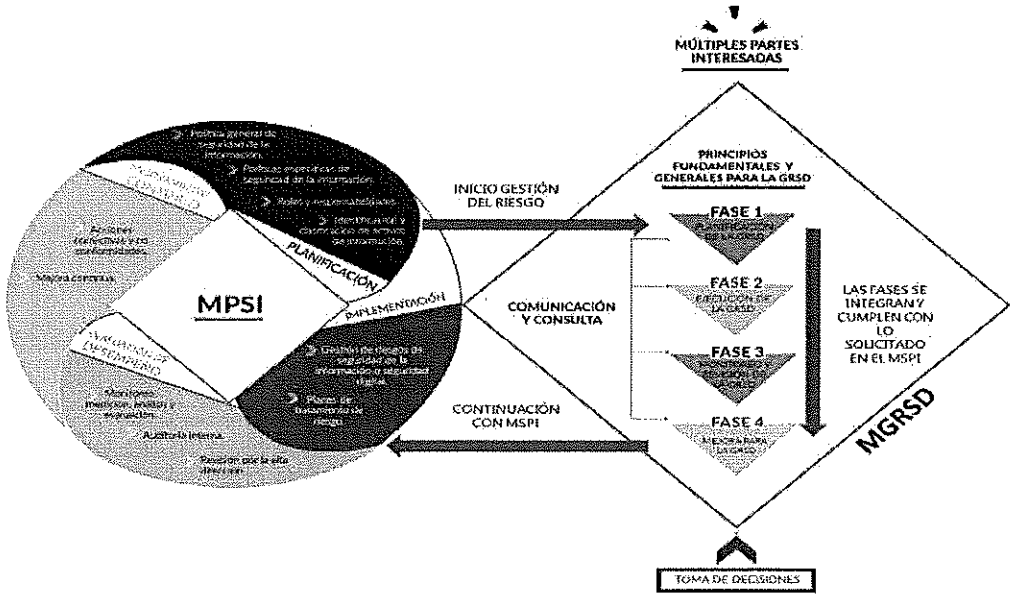

Figura 1. Integración del MPSI con el MGRSD. Tomado de https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b.

La fase 1 de planificación corresponde a implementar la metodología de la gestión del riesgo del DAFP en donde se identifican y se valoran los riesgos de la ESE para establecer controles, así como se muestra a continuación:

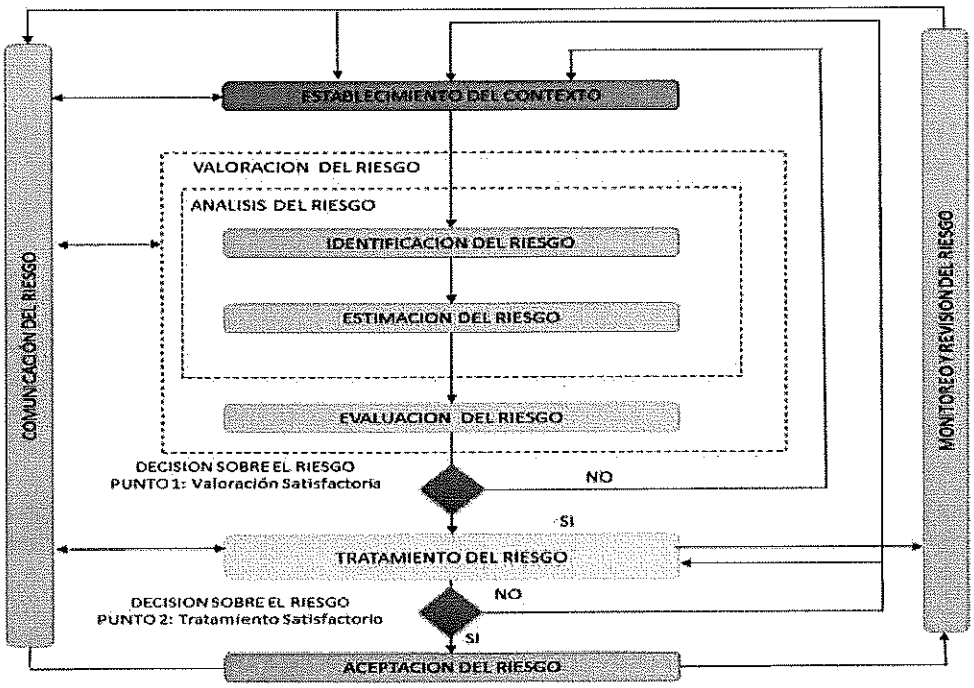

Figura 2. Gestión del riesgo de seguridad de la información según ISO 27005. Fuente: ISO 27005, citado en http://www.uptc.edu.co/export/sites/default/gel/documentos/plan_trata_rie_seg_inf2020.pdf

Para la estimación de los riesgos se tomará la siguiente escala de probabilidad:

ESCALA DE PROBABILIDAD		
	NIVEL	DESCRIPCION
1	Raro	Evento que puede ocurrir sólo en circunstancias excepcionales, entre 0 y 1 vez en 1 semestre.
2	Improbable	Evento que puede ocurrir en pocas de las circunstancias, entre 2 y 5 veces en un semestre.
3	Posible	Evento que puede ocurrir en algunas de las circunstancias entre seis y 10 veces en 1 semestre.
4	Probable	Evento que puede ocurrir en casi siempre entre 11 y 15 veces en 1 semestre.
5		Evento que puede ocurrir en la mayoría de las circunstancias más de 15 veces en 1 semestre.

Figura 3. Escala de probabilidad para medir riesgos. Fuente: Tomado de ISO 31000 citado en http://www.uptc.edu.co/export/sites/default/gel/documentos/plan_trata_rie_seg_inf2020.pdf

Para la valoración de impacto se tomará en cuenta los siguientes criterios:

VALOR DE IMPACTO			
	NIVEL	DESCRIPCION	ESCALA
1	Insignificante	Impacta negativamente de forma leve la imagen y operación de un roi. No tiene impacto Financiero para la Universidad o sus procesos. Impacta negativamente, posibilidad de recibir multas.	>=1 y <=4
2	Menor	Impacta negativamente la imagen y de manera importante la operación de un proceso. Se pueden presentar sobrecostos debido a reprocesos a nivel de un proceso. Impacta negativamente, posibilidad de recibir multas.	>=5 y <=8
3	Moderado	Afecta negativamente la imagen institucional a nivel regional por retrasos en la prestación de los servicios y la operación no sólo del proceso evaluado sino de otros procesos. Se pueden presentar sobrecostos por reprocesos y aumento de carga operativa, no sólo en el proceso evaluado sino a otros procesos. Impacta negativamente, posibilidad de recibir una investigación disciplinaria.	>=9 y <=12
4	Mayor	Imagen institucional a nivel nacional afectada, al igual que la operación por el incumplimiento en la prestación de servicios de la Universidad o el cumplimiento de sus objetivos estratégicos. Se pueden presentar sobrecostos por reprocesos significativos para una sede seccional de la Institución. Impacta negativamente, posibilidad de recibir una investigación fiscal.	>=13 y <=16
5		Imagen institucional afectada a nivel nacional e internacional. Impacta negativamente la operación y el cumplimiento en la prestación de los servicios de la Institución y el incumplimiento de sus objetivos estratégicos. Se pueden presentar sobrecostos debido a reprocesos y aumento de carga operativa importante en toda la Universidad. Impacta negativamente, posibilidad de recibir una intervención o sanción, por parte de entes de control o cualquier ente regulador.	>=17 y <= 20

Figura 4. Valoración de impacto de riesgos. Fuente: Tomado de ISO 31000 citado en http://www.uptc.edu.co/export/sites/default/gel/documentos/plan_trata_rie_seg_inf2020.pdf

Para analizar los riesgos es necesario conciliar los impactos con las probabilidades, lo cual se hace en la matriz IP:

MATRIZ IP

IMPACTO	VALOR	EVALUACION				
	5	5	10	15		
Mayor	4	4	8	12		
Moderado	3	3	6	9	12	15
Menor	2	2	4	6	8	10
Insignificante	1	1	2	3	4	5
	Valor	1	2	3	4	5
	PROBABILIDAD	Raro	Improbable	Posible	Probable	

Figura 5. Matriz Impacto-probabilidad. Fuente: ISO 31000, citado en http://www.uptc.edu.co/export/sites/default/gel/documentos/plan_trata_rie_seg_inf2020.pdf

El adecuado diligenciamiento de la matriz de Impacto-Probabilidad (IP) permitirá a la entidad identificar y priorizar los riesgos, facilitando la formulación de planes de acción y mitigación correspondientes. Aquellos riesgos ubicados en la zona roja se consideran de alto riesgo y requieren acciones de mitigación inmediatas. Los riesgos en la zona amarilla, categorizados como moderados, deben abordarse en el corto y mediano plazo,

mientras que los riesgos en la zona verde, de bajo riesgo, necesitan planes de mitigación para su eliminación o la identificación de posibles riesgos residuales asociados al proceso.

Es imperativo destacar que la gestión integral de riesgos relacionados con la seguridad y privacidad de la información debe estar siempre alineada con lo establecido en la política institucional de gestión de riesgos.

8. PLAN DE ACCIÓN:

No	Actividad	INDICADOR	Tiempo	Responsable
1	Socialización de Política de gestión de riesgos	Socialización de Política de gestión de riesgos a los funcionarios y colaboradores de la E.S.E	Marzo	Sistemas
2	Actualización de la Identificación, valoración y aceptación de los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	Elaboración de matriz de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	Marzo	Planeación y Sistemas
3	Definición de puntos de control de los riesgos identificados	Matriz de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	Marzo	Planeación y Sistemas
4	Realizar seguimiento y evaluación a los controles implementados para tratamiento de Riesgos	Formato de seguimiento de riesgos diligenciado	Marzo-Junio Septiembre-Diciembre	Planeación-Sistemas
5	Socialización de resultados de la política de riesgos en el comité de gestión y desempeño	Acta de comité	Noviembre	Sistemas

8. APROBACION:

La gerencia de la Empresa Social del Estado Centro de Rehabilitación Integral de Boyacá aprueba el Plan de tratamiento de riesgos de seguridad y privacidad de la información a los treinta y uno (31) días del mes de enero de dos mil veinte Tres (2024).

ORIGINAL FIRMADO

ZULMA CRISTINA MONTAÑA MARTINEZ
Gerente E.S.E. Centro de Rehabilitación Integral de Boyacá

Elaboro: Camilo Andrés Rodríguez, Técnico Operativo
Reviso: Andrea del Pilar Chona Bolívar / Subgerente Administrativo y Financiero
Aprobó: Zulma Cristina Montaña Martínez / Gerente

9. REFERENCIAS DOCUMENTALES:

- Política Institucional de Gestión de Riesgos (Basado de Guía de administración de riesgos del DAFP)

CONTROL DEL DOCUMENTO

Solo para diligenciamiento del área de calidad:

MODIFICACIONES						
VERSION ANTERIOR	NUEVA VERSION	FECHA CAMBIO	DESCRIPCION DEL CAMBIO	ELABORO	REVISO	APROBÓ
	1	22/01/2021	Creación del documento	Blanca Nubia Vásquez Moreno.	Diego Fernando Rivera Castro.	Zulma Cristina Montaña Martínez.
	2	05/01/2024	Actualización del documento	Cesar David Parra Asesor de planeación	Dana Mendoza Díaz Asesor de desarrollo de servicios	Andrea del Pilar Chona Subgerente administrativo

LOCALIZACION DEL DOCUMENTO			
CODIGO	NOMBRE	COPIAS	UBICACIÓN
CMC-GC-I03	INSTRUCTIVO ELABORACION DE PLAN INSTITUCIONAL	ORIGINAL	Oficina de Calidad SOGC
CMC-GC-I03	INSTRUCTIVO ELABORACION DE PLAN INSTITUCIONAL	COPIA CONTROLADA	Sistema de Consulta MIPG