



PLAN

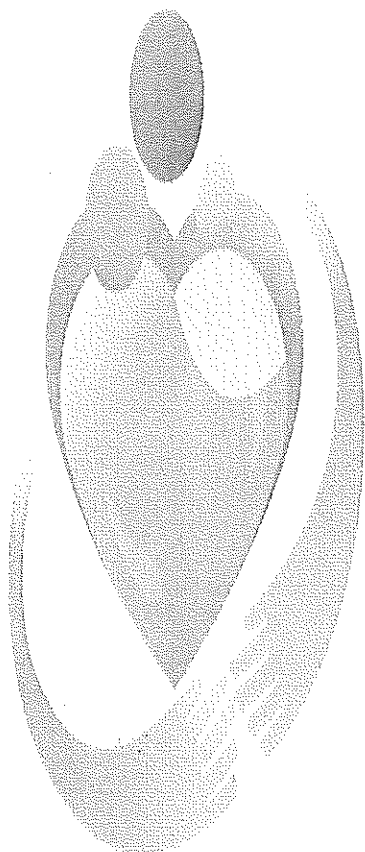
VERSION: 1

CODIGO: PL-GRT-003

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

FECHA: 31/01/2022

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2023




CSE **CRIB**

Avanzamos por la salud mental de Boyacá.

Zulma Cristina Montaña Martínez
Gerente

Este es un formato de registro, se advierte al colaborador que su contenido no puede ser objeto de modificaciones posteriores a la fecha de edición sin que informe directamente de tales cambios a la oficina de calidad

	PLAN	VERSION: 1
		CODIGO: PL-GRT-003
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		FECHA: 31/01/2022

PARTICIPANTES:

Zulma Cristina Montaña Martínez
Gerente

Segundo Jacinto Pérez
Subgerente Administrativo y financiero

Camilo Andrés Rodríguez Farfán
Técnico Operativo


Cesar David Parra
Asesor de Planeación



	<p style="text-align: center;">PLAN</p>	VERSION: 1
		CODIGO: PL-GRT-003
<p style="text-align: center;">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</p>		FECHA: 31/01/2022

TABLA DE CONTENIDO

1.	NOMBRE DEL PLAN SEGÚN DECRETO 612 2018	5
2.	DIAGNOSTICO.....	5
3.	MARCO NORMATIVO:	5
4.	DEFINICIONES:	6
5.	OBJETIVO GENERAL:	7
6.	OBJETIVOS ESPECIFICOS:	7
7.	METODOLOGÍA:	7
8.	PLAN DE ACCIÓN:	11
8.	APROBACION	12
9.	REFERENCIAS DOCUMENTALES:	12

Handwritten signature

	PLAN	VERSION: 1
		CODIGO: PL-GRT-003
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		FECHA: 31/01/2022

INTRODUCCIÓN


El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la institución en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital, ciudadanos-usuarios y hogares empoderados del Entorno Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares 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.

Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos (Pérdida de la Confidencialidad de los activos, Pérdida de Integridad de los activos y Pérdida de Disponibilidad de los activos) evitando aquellas situaciones que impidan el logro de los objetivos institucionales.

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medidas de seguridad, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad.

Las anteriores medidas se definieron teniendo en cuenta la información del análisis de riesgos, el cual brindó información acerca de las necesidades del Proceso de Tecnología de la Empresa Social del Estado Centro de Rehabilitación Integral de Boyacá, en cuanto a la seguridad de la información y proporcionó las herramientas necesarias para definir cada una de las características de las medidas y la definición de los pasos a seguir para su ejecución.

	PLAN	VERSION: 1
		CODIGO: PL-GRT-003
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		FECHA: 31/01/2022

1. NOMBRE DEL PLAN SEGÚN DECRETO 612 2018

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

2. DIAGNOSTICO

Es necesario incorporar en el sistema de administración de riesgos de la ESE CRIB los criterios relacionados con los riesgos de seguridad y privacidad de la información en conformidad con la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 del DAFP, con lo cual se hace necesario actualizar los siguientes documentos:

- Política de Administración de riesgos
- Matriz de riesgos del proceso gestión de recursos tecnológicos

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"

Este es un formato de registro, se advierte al colaborador que su contenido no puede ser objeto de modificaciones posteriores a la fecha de edición sin que informe directamente de tales cambios a la oficina de calidad



PLAN

VERSION: 1

CODIGO: PL-GRT-003

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


FECHA: 31/01/2022

- 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.

Este es un formato de registro, se advierte al colaborador que su contenido no puede ser objeto de modificaciones posteriores a la fecha de edición sin que informe directamente de tales cambios a la oficina de calidad

	PLAN	VERSION: 1
		CODIGO: PL-GRT-003
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		FECHA: 31/01/2022

- **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:

Gestionar los riesgos asociados a la seguridad y privacidad de la información en la Empresa Social Del Estado Centro De Rehabilitación Integral de Boyacá, en conformidad con el modelo de gestión de riesgos de seguridad Digital, estableciendo controles efectivos que propendan por garantizar la confiabilidad e integridad de la información que maneja la ESE CRIB.

6. OBJETIVOS ESPECIFICOS:

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación que la E.S.E CRIB pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.
- Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, de acuerdo con los modelos y lineamientos establecidos por el MIN tic y el DAFP.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación.

7. METODOLOGÍA:

El presente plan de tratamiento de riesgos de seguridad y privacidad de la información basa su proceso metodológico en la NTC ISO 3100:2018, ISO 27005:2018 y la guía para la administración del riesgo y del diseño de controles en entidades públicas del DAFP.



El presente plan debe integrarse con el plan de seguridad privacidad de la información para aplicar el modelo nacional

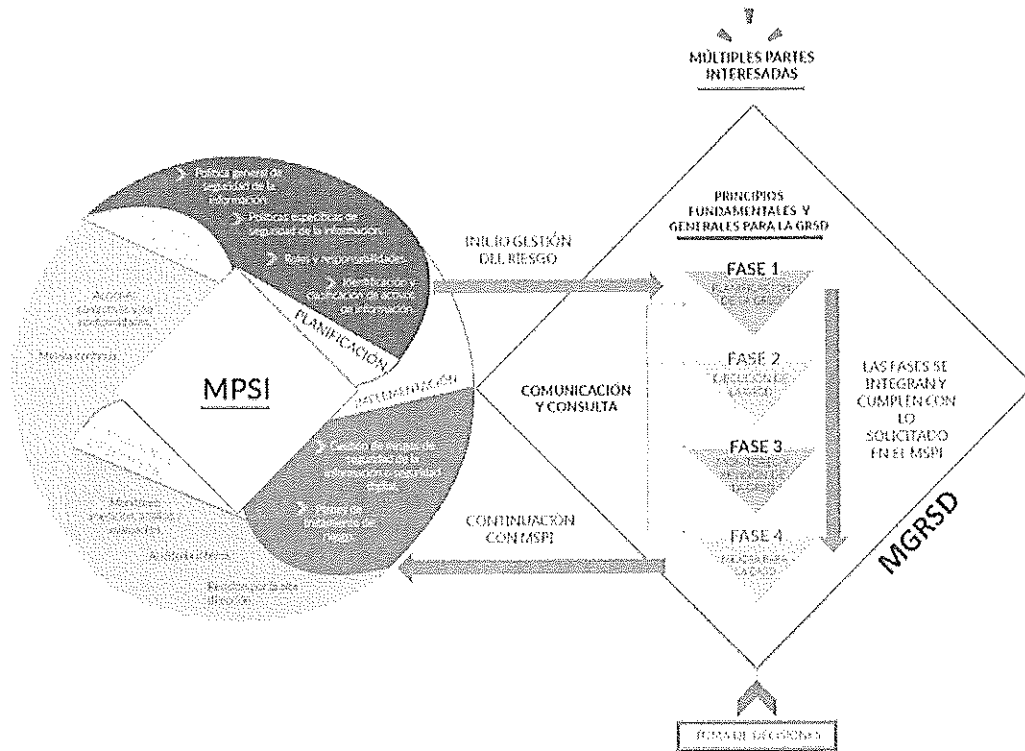


Figura 1. Integración del MPSI con el MGRSD. Tomado de <https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b>.

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:

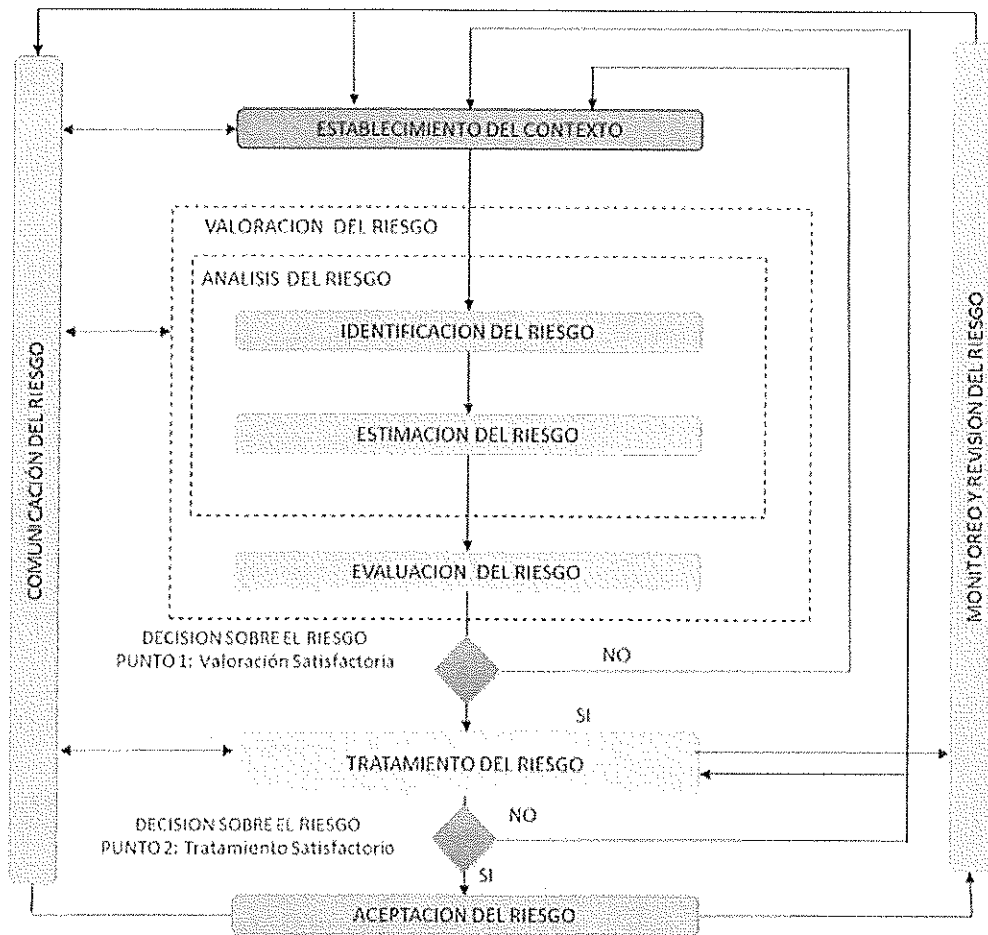



Figura 2. Gestión del riesgo de seguridad de la información según ISO 27005. Fuente: ISO 27005, citado en http://www.uptc.edu.co/export/sites/default/gel/documentos/plan_trata_rie_seg_inf2020.pdf

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	Casi Seguro	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

Este es un formato de registro, se advierte al colaborador que su contenido no puede ser objeto de modificaciones posteriores a la fecha de edición sin que informe directamente de tales cambios a la oficina de calidad

	PLAN	VERSION: 1
		CODIGO: PL-GRT-003
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		FECHA: 31/01/2022

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 rol. 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 Catastrófico	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.upic.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 en la matriz IP:

MATRIZ IP

IMPACTO	VALOR	EVALUACION				
		1	2	3	4	5
Catastrófico	5	5	10	15	20	25
Mayor	4	4	8	12	16	20
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	Casi Seguro

Este es un formato de registro, se advierte al colaborador que su contenido no puede ser objeto de modificaciones posteriores a la fecha de edición sin que informe directamente de tales cambios a la oficina de calidad


	PLAN	VERSION: 1
		CODIGO: PL-GRT-003
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		FECHA: 31/01/2022

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 diligenciamiento de la matriz IP permitirá a la entidad identificar los riesgos que deben ser priorizados para Poder establecer los respectivos planes de acción y mitigación, los riesgos que se identifiquen en la zona roja, se consideran zona de alto riesgo y debe mitigarse de manera inmediata, los riesgos en la zona amarilla son de riesgo moderado y deben mitigarse en el corto y mediano plazo y los riesgos en la zona verde son de bajo riesgo y debe establecer planes de mitigación para intentar eliminarlo o identificar si se trata de un riesgo residual asociado al proceso.


Es necesario mencionar que la gestión integral de riesgos asociados a la seguridad y privacidad de la información debe estar siempre en concordancia con lo establecido en la política de gestión de riesgos institucional.

Para la ejecución de las fases 2-3-4 se plantea el siguiente plan de acción.

8. PLAN DE ACCIÓN:

No	Actividad	INDICADOR	Tiempo	Responsable
1	Establecimiento de la política de gestión de riesgos en conformidad con el MGRSD	Política de gestión de riesgos conformidad con el MGRSD, Aprobada	Marzo	Planeación y Sistemas
2	Socialización de Política de gestión de riesgos conformidad con el MGRSD	Socialización de Política de gestión de riesgos conformidad con el MGRSD en el comité de gestión y desempeño	Abril	Sistemas
3	Identificación y valoración de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	Matriz de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	Abril	Planeación y Sistemas
4	Aceptar los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	Riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación, Aceptados	Abril- Mayo	Comité de Control Interno
5	Presentación de evidencias de seguimiento y valoración a los puntos de control de la matriz de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	Formato de seguimiento de riesgos diligenciado	Septiembre - Diciembre	Planeación-Sistemas
6	Elaborar manual de identificación, evaluación, seguimiento y control de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación, alineándolo a la política de seguridad digital de MIPG	Manual de identificación, evaluación, seguimiento y control de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación, alineándolo a la política de seguridad digital de MIPG, Aprobado	Agosto- Septiembre	Sistemas

Este es un formato de registro, se advierte al colaborador que su contenido no puede ser objeto de modificaciones posteriores a la fecha de edición sin que informe directamente de tales cambios a la oficina de calidad

	PLAN	VERSION: 1
		CODIGO: PL-GRT-003
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		FECHA: 31/01/2022

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 (2023).



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

 PROYECTO Segundo Leopoldo Pérez Archila Subgerente Administrativo y Financiero.	 REVISÓ César David Parra Guerrero Asesor de Planeación.	 APROBO Zulma Cristina Montaña Martínez/Gerente Gerente
---	---	--

9. REFERENCIAS DOCUMENTALES:

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

ELABORÓ	REVISÓ	APROBÓ
Nombre: Camilo Andrés Rodríguez Farfan Cargo: Técnico Operativo Fecha: 30/01/2023	Nombre: Cesar David Parra Cargo: Asesor Planeación Fecha: 30/01/2023	Nombre: Zulma Cristina Montaña Martínez Cargo: Gerente Fecha: 30/01/2023

CONTROL DEL DOCUMENTO

MODIFICACIONES						
VERSION ANTERIOR	NUEVA VERSION	FECHA CAMBIO	DESCRIPCION DEL CAMBIO	ELABORO	REVISO	APROBÓ
	1	22/01/2021	Creación del documento	Diego Fernando Rivera Castro.	Comité de Control Interno	Zulma Cristina Montaña Martínez.
	2	31/01/2022	CAMBIO DE VERSION	Diego Fernando Rivera Castro.	Comité de Control Interno	Zulma Cristina Montaña Martínez.
	3	31/01/2023	Cambio de versión-	Cesar David Parra	Comité de Control Interno	Zulma Cristina Montaña Martínez.

Este es un formato de registro, se advierte al colaborador que su contenido no puede ser objeto de modificaciones posteriores a la fecha de edición sin que informe directamente de tales cambios a la oficina de calidad



PLAN

VERSION: 1

CODIGO: PL-GRT-003

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

FECHA: 31/01/2022

			actualización de actividades			
--	--	--	------------------------------	--	--	--

LOCALIZACION DEL DOCUMENTO

CODIGO	NOMBRE	COPIAS	UBICACIÓN
PL-GRT-003	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	ORIGINAL	Oficina de Calidad
PL-GRT-003	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	COPIA CONTROLADA	Sistema de Consulta MIPG

[Handwritten mark]

