Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2021

Zulma Cristina Montaña Martínez
Gerente

PARTICIPANTES:

Zulma Cristina Montaña Martínez
Gerente

Jesús Antonio Salamanca Torres
Subgerente Administrativo y financiero

Camilo Andrés Rodríguez Farfán
Técnico Operativo

Diego Fernando Rivera Castro
Asesor de Planeación

TABLA DE CONTENIDO

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 (Perdida de la Confidencialidad de los activos, Perdida de Integridad de los activos y Perdida 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 medias 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.

DESARROLLO

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

2. DIAGNOSTICO

La junta directiva mediante Acuerdo N° 100.03.01.03 del 17 de julio de 2020 aprobó el plan de desarrollo institucional de la Empresa Social del Estado Centro de Rehabilitación Integral de Boyacá para la vigencia fiscal 2020-2023 presentado por la gerente.

En el direccionamiento estratégico del precitado plan de desarrollo se contemplan 4 líneas estratégicas que responden al diagnóstico organizacional de la entidad, estas son:

1. Talento humano.
2. Desarrollo Administrativo.
3. Infraestructura.
4. Desarrollo de servicios.

En la línea estratégica de Infraestructura en la política de gestión tecnológica se contempla el plan de gestión de tecnologías de información el cual busca que las acciones de la entidad se enfoquen en la adecuada administración de los recursos tecnológicos de la entidad, garantizando la seguridad de la información en todos los procesos institucionales.

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"

- 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:

Desarrollar un plan de gestión de seguridad y privacidad de la información que permita minimizar los riesgos de pérdida de archivos de la información en la Empresa Social Del Estado Centro De Rehabilitación Integral de Boyacá

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 contextos establecidos en la Entidad.

- 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 e ISO 27005, lo cual permite tener al presente plan tener un enfoque por procesos, lo cual es lo más adecuado dado que el desarrollo organizacional de la Empresa Social del Estado Centro de Rehabilitación Integral de Boyacá está basado en procesos de tipo estratégico, misionales, de apoyo y de evaluación, por lo tanto el proceso general para el proceso del sistema general de sistemas de información de la empresa seguirá el siguiente proceso:

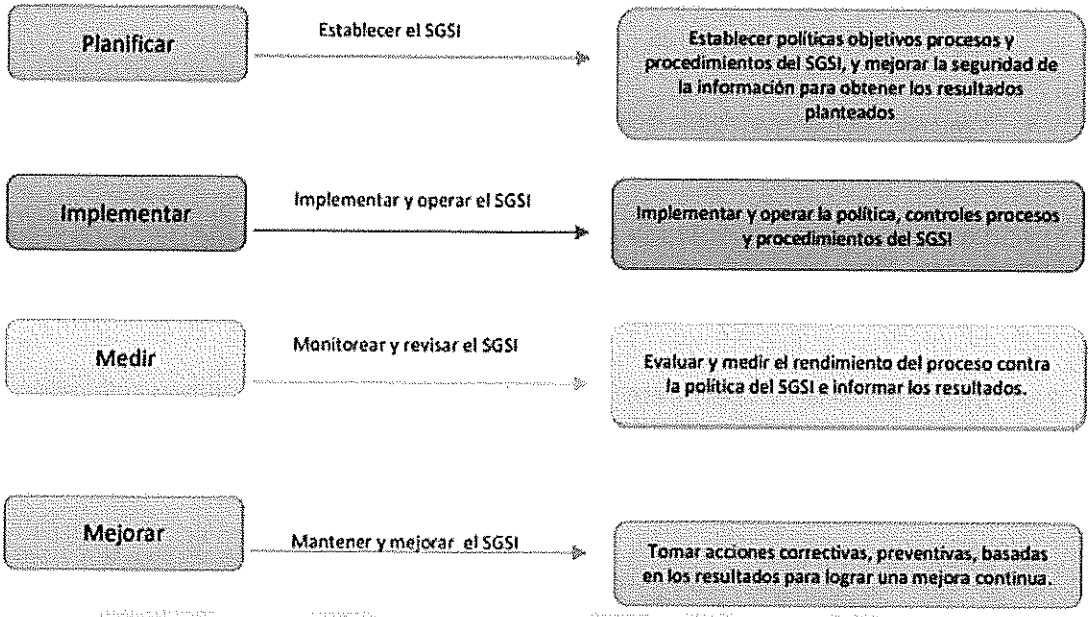

Figura 1. Proceso de gestión de un sistema de información. Tomado de http://www.uptc.edu.co/export/sites/default/gel/documentos/plan_trata_rie_seg_inf2020.pdf

Durante todo el proceso de implementación del presente plan que responde al proceso PHVA de mejoramiento continuo de procesos, se debe tener en cuenta la identificación, valoración y mitigación de los riesgos, con lo que en el establecimiento de la política de sistema de gestión de sistema de información se debe tener en cuenta la gestión integral de riesgo.

A continuación, se listan las fases metodológicas de implementación del plan que estarán a cargo en primera línea del técnico operativo de la Empresa como líder del proceso de tecnologías de información de la Empresa, y en segunda línea la oficina de planeación hará el respectivo acompañamiento y seguimiento:

- **Fase 1: Análisis de la información**

En esta etapa se evaluarán los resultados de entrevista con los colaboradores del proceso de TI, se desarrollarán las siguientes actividades:

- Aplicar las políticas de tratamiento de riesgos.
- Determinar los controles (se desprenden de las medidas) aplicados en la ESE CRIB
- Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos.

- **Fase 2: Desarrollo de los proyectos**

En esta fase se realizarán las actividades que permitan la estructuración de las medidas.

- Determinar el nombre de la medida.
- Definir los responsables de cada medida.
- Establecer el objetivo de cada medida.
- Elaborar la justificación de la medida.
- Definir las actividades a realizar para el desarrollo de la medida.

- **Fase 3: Análisis de los proyectos**

- Definición de los controles relacionados con cada medida.
- Validar los riesgos mitigados por cada medida.

- Análisis de la aplicabilidad de las medidas.
- Priorización de las medidas.

- **Fase 4: Definición del organigrama de responsabilidad**

  En esta fase se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo, teniendo en cuenta su estructura organizacional para la gestión de riesgos su administración en las tres líneas de defensa.

- Definición del grupo de trabajo de gestión de riesgo.
- Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de las medidas.

- **Fase 5: Ciclo de vida del tratamiento de riesgos**

  Definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Tratamiento de Riesgos

  La implementación de estas fases debe responder al siguiente proceso de gestión de riesgo de la seguridad de la información extraído de la Norma ISO 27005 que adapta la metodología de gestión de riesgos de la ISO 31000.

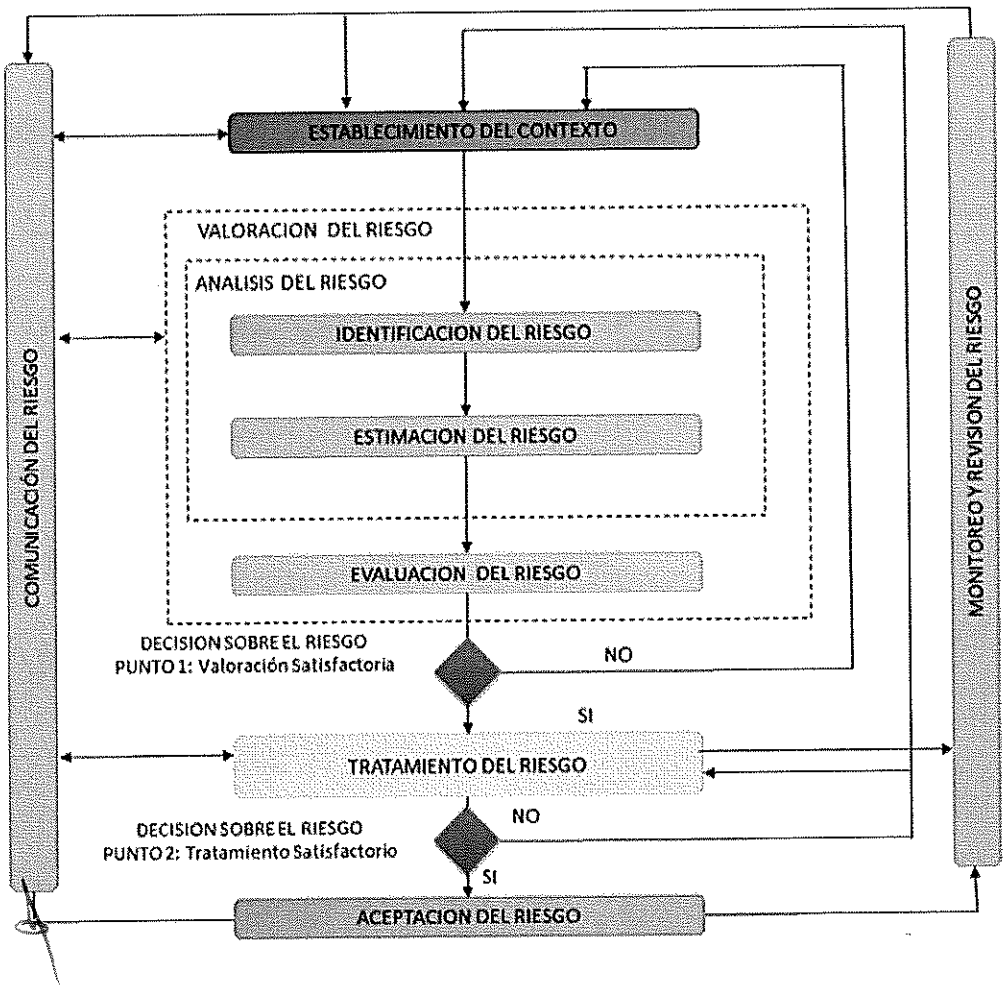

Figura 1. Gestión del riesgo de seguridad de la información según ISO 27005. Fuente: ISO 27005, citado en http://www.uptc.edu.co/export/sites/default/gel/documentos/plan_trata_rie_seg_inf2020.pdf

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 2. 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 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 3. 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 en la matriz IP:

MATRIZ IP

IMPACTO	VALOR	EVALUACION				
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

Figura 4. 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.

8. PLAN DE ACCIÓN:

GESTION	ACTIVIDAD	TAREA	RESPONSABLE	FECHA DE EJECUCION
Gestión De Riesgos	Establecimiento de la política de gestión de riesgos	Establecer la política de gestión de riesgos	Planeacion y sistemas	Febrero de 2021
	Actualización de lineamientos de riesgos	Documentar la implementación de la metodología de gestión de riesgos	Planeación y Sistemas	Febrero de 2021

Sensibilización	Socialización guía y Herramienta - Gestión de riesgos y seguridad privada de la información seguridad digital y continuidad de la operación	Planeación y Sistemas	Marzo 2021
Identificación de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación	Identificación análisis y evaluación de riesgos - seguridad y privacidad de la información, seguridad digital y continuidad de la operación	Planeación y Sistemas	Abril de 2021
	Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Planeación y Sistemas	Abril de 2021
Aceptación de riesgos identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Planeación y Sistemas	Abril de 2021
Publicación	Publicación matriz de riesgos - SIMIG	Planeación y Sistemas	Mayo de 2021
Seguimiento fase de tratamiento	Seguimiento estado planes de tratamiento de riesgos identificados y verificación de evidencias	Planeación y Sistemas	Marzo-Diciembre 2021
Evaluación de riegos residuales	evaluación de riegos residuales	Planeación y Sistemas	Marzo, junio, septiembre. Diciembre de 2021
Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la	Planeación y Sistemas	Marzo, junio, septiembre. Diciembre de 2021

		evaluación de riesgos residuales		
		Actualización guía gestión de residuos seguridad de la información, de acuerdo a los cambios solicitados	Planeación y Sistemas	Junio 2021
	Monitoreo y revisión	Generación, presentación y reporte de indicadores	Planeación y Sistemas	Marzo, junio, septiembre. Diciembre de 2021
Sistema de gestión	Establecimiento de un sistema general de sistemas de información (SGSI) para la E.S.E.	Hacer un diagnóstico en sistemas de información de manera metodológica	Sistemas	Febrero 2021
		Diseñar un sistema general de sistemas de información para la E.S.E. que tome en cuenta lo dispuesto en el plan de seguridad y privacidad de la información y basado en riesgos	Sistemas	Marzo 2021
		Establecer plan operativo para la cabal implementación del SGSI en la E.S.E	Sistemas	Marzo 2021
		Llevar a cabo el seguimiento al plan operativo del SGSI, documentado planes de mejoramiento	Planeación-Control Interno	Junio, Septiembre, Diciembre de 2021

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 de Adquisiciones a los veintinueve (29) días del mes de enero de dos mil veinte uno (2021).

EMPRESA SOCIAL DEL ESTADO CENTRO DE REHABILITACIÓN INTEGRAL DE BOYACÁ GERENCIA NIT. 7.800.982

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

9. REFERENCIAS DOCUMENTALES:

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

	PLAN	VERSION: 1
		CODIGO: PL-GRT-003
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		FECHA: 29/01/2021

ELABORÓ	REVISÓ	APROBÓ
Nombre: Diego Fernando Rivera Castro **Cargo:** Asesor Planeación **Fecha:** 22/01/2021	**Nombre:** Comité de Control Interno **Fecha:** 29/01/2021	**Nombre:** Zulma Cristina Montaña Martínez **Cargo:** Gerente **Fecha:** 29/01/2021

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.

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