Plan de Seguridad y Privacidad de la Información 2022

E.S.E CRIB

Avanzamos por la salud mental de Boyacá.

Centro de Rehabilitación Integral de Boyacá E.S.E.

Zulma Cristina Montaña Martínez
Gerente

PARTICIPANTES:

Zulma Cristina Montaña Martínez
Gerente

Segundo Jacinto Pérez
Subgerente Administrativo y financiero

Camilo Andrés Rodríguez Farfán
Técnico Operativo

Diego Fernando Rivera Castro
Asesor de Planeación

TABLA DE CONTENIDO

INTRODUCCIÓN

Uno de los activos más importantes de la E.S.E CRIB es la información, teniendo en cuenta lo anterior es necesario realizar las mejores prácticas y lineamientos dados por el por el Departamento de Administrativo de la Función Pública con su estrategia MIPG y el Ministerio de las Tecnologías e Información en el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información.

El plan de seguridad y privacidad de la información es uno de los planes que hacen parte del plan de acción de la gerencia de la Empresa Social del Estado Centro de Rehabilitación Integral de Boyacá en cumplimiento con lo dispuesto en el artículo 1 del 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." Mediante el cual se busca la cabal implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) publicado por el ministerio de Tecnologías de la Información y Comunicaciones a través de la dirección de gobierno digital, le cual se encuentra alineado con el marco de referencia de arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y la guía para la administración del riesgo y el diseño de controles en la gestión pública.

El MSPI se actualiza constantemente en concordancia con los cambios técnicos de la Norma NTC ISO 27001 "Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad del Información (SGSI).", lo cual busca que las decisiones relacionadas con los sistemas de información tengan un enfoque estratégico que permita a la Empresa alinearse a lo planteado por el Gobierno Nacional en el plan de desarrollo 2018-2022 "Pacto por Colombia, Pacto por la equidad" Ley 1955 de 2019 en sus artículos 147 "Transformación digital pública" y 148 "Gobierno Digital como política de gestión y desempeño institucional" y el CONPES 3854 de 2016 "Política Nacional de Seguridad digital" , lo cual es garantía de establecer una política de mejoramiento continuo en lo que respecta a la seguridad de la información, lo que propicia una mejor gestión en los procesos institucionales.

1. DESARROLLO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

2. DIAGNOSTICO

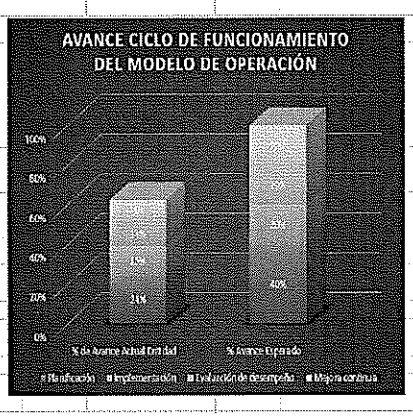
De acuerdo a diagnóstico de madurez de seguridad y privacidad de la información los resultados son los siguientes

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	57	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	20	100	INICIAL
A.8	GESTIÓN DE ACTIVOS	40	100	REPETIBLE
A.9	CONTROL DE ACCESO	63	100	GESTIONADO
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	73	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	50	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	38	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	91	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	50	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	40	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	25	100	REPETIBLE
	PROMEDIO EVALUACIÓN DE CONTROLES	41	100	EFECTIVO

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2020	Planificación	24%	40%
	Implementación	15%	20%
	Evaluación de desempeño	13%	20%
	Mejora continua	10%	20%
TOTAL		62%	100%



NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO
Inicial	INTERMEDIO
Repetible	CRÍTICO
Definido	CRÍTICO
Administrado	CRÍTICO
Optimizado	CRÍTICO

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

TOTAL DE NUMERALES CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

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."*
- 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.

- **Acceso autorizado**: Autorización concedida a un usuario para el uso de determinados recursos. En dispositivos automatizados es el resultado de una autentificación correcta, generalmente mediante el ingreso de usuario y contraseña.

- **Antivirus**: Son programas cuyo objetivo es detectar y/o eliminar virus informáticos.

- **Ataques de denegación de Servicio:** Es un ataque a un sistema de cómputo o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

- **Ataques de fuerza bruta**: Intentar en repetidas ocasiones todas las posibles combinaciones de contraseñas y llaves de encriptación hasta que se encuentre la correcta.

- **Autenticación:** Procedimiento de verificación de la identidad de un usuario.

- **CD/DVD**: Dispositivo de almacenamiento de información.

- **Conexión remota**: El uso de tecnologías de conectividad a través de una red de comunicaciones que permiten acceder e interactuar desde sitios externos a la ESE CRIB con la infraestructura de hardware, software y servicios tecnológicos de la empresa.

- **Confidencialidad**: Protección de información privada o sensible contra divulgación no autorizada.

- **Contraseña**: Seña secreta que permite el acceso a dispositivos, información, bases de datos, recursos o servicios tecnológicos.

- **Control de acceso**: conjunto de reglas, procedimientos, prácticas, o mecanismos que permiten el ingreso a dispositivos, lugar, información o bases de datos mediante la autenticación (físico o lógico).

- **Copia de respaldo:** Copia de información en un soporte que permita su recuperación.

- **Credenciales de acceso**: Datos relacionados con el usuario y contraseña para acceder a un servicio de tecnología.

- **Dirección IP**: es un conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en la red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop, teléfono inteligente) que utilice el

protocolo (Internet Protocol) o, que corresponde al nivel de red

- **Discos de almacenamiento externo**: Los discos de almacenamiento externo son para almacenar información de forma masiva y se puede intercambiar con otros equipos.

- **Disponibilidad**: Garantizar que los sistemas de información y los datos estén listos para su uso cuando se necesite.

- **Dispositivos de almacenamiento local**: Son los discos locales del equipo de cómputo asignado para guardar cualquier tipo de información.

- **DNS**: Sistema de nombre de dominio es un sistema de nomenclatura jerárquica para equipos de cómputo, servicios o cualquier recurso conectado a Internet o a una red privada.

- **Emergencia**: Asunto o situación imprevista desde el área informática que requiere una especial atención y requiere solucionan inmediata para la continuidad de las labores diarias sin que se llegue a presentar un riesgo tecnológico o que pueda llegar afectar a la entidad.
- **Equipo de cómputo**: Entiéndase como las computadoras, equipos de uso personal bien sea de escritorio o portátil y sus periféricos (Pantalla, mouse, teclado, parlantes, entre otros).

- **Gestión documental Electrónico:** sistema de software que controla y organiza los documentos en toda la organización sin importar que se denomine como un documento electrónico de archivo o no. Mediante una plataforma que permite gestionar de manera ágil, segura, flexible y escalable la información institucional, tanto física como digital.

- **Hardware**: Corresponde a todas las partes físicas y tangibles de un sistema de cómputo.

- **Identificación:** Proceso de reconocimiento de la identidad de los usuarios.

- **Identificación única de usuario:** Son los datos de Usuario y contraseña de acceso a los recursos informáticos o sistemas de información.

- **Incidencia:** Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, dispositivos, equipos de cómputo, constituyendo un riesgo para la confidencialidad, disponibilidad o integridad de las bases de datos, información o servicios.

- **Infraestructura Tecnológica**: Conjunto de recursos de telecomunicaciones, hardware y software que permitan el procesamiento, la transmisión y el almacenamiento de cualquier tipo de información.

- **Integridad Informática**: Garantiza que la información no haya sido alterada o modificada por terceros para conservar la validez de la información. la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito.

- **Licencia de software**: Permiso legal otorgado por un tercero con facultades para ello, para utilizar un programa para computador (Software) a cambio de un pago único o periódico.

- **Material de soporte:** Material en cuya superficie se registra información o sobre el cual se pueden guardar o recuperar datos, como el papel, la cinta de video, el CD, el DVD, el disco duro, etc.

- **Perfil de usuario:** Grupo de usuarios a los que se da acceso.

- **Periférico**: Elemento electrónico de entrada y/o salida de información, que pueden ser conectados a un equipo de cómputo. Son periféricos: impresoras, scanner, webcams, proyectores, plotters y artículos similares.

- **Programa malicioso**: Es un tipo de software que tiene como objetivo infiltrarse o dañar un equipo de cómputo, sin el consentimiento de su propietario.

- **Recurso Informático**: Son los equipos de cómputo, servidores, infraestructura tecnológica, equipos de comunicaciones, licencia de software, periférico, software, salas de cómputo, sistema de archivos, software antivirus.

- **Recurso Protegido:** Cualquier componente del sistema de información, como bases de datos, programas, soportes o equipos, empleados para el almacenamiento y tratamiento de datos personales.

- **Red Institucional**: La red institucional es la red de datos de la ESE CRIB que permite la comunicación entre todos los recursos informáticos.

- **Responsable de seguridad:** Una o varias personas designadas por el responsable del tratamiento para el control y la coordinación de las medidas de seguridad.

- **Salvaguardar:** Defender, proteger un activo, información, o sistema de información

- **Seguridad de la información**: Es la protección de los activos de información, frente a una gran variedad de amenazas que existen en el mundo, con el fin de asegurar la disponibilidad de todos los procesos, minimizar el riesgo y apoyar en el cumplimiento de los objetivos de la ESE CRIB.

- **Sesión de Red:** Una sesión es la duración de una conexión empleando una capa de sesión de un protocolo de red, o la duración de una conexión entre un usuario y el equipo de cómputo.

- **Servidor**: Equipo de cómputo con características que le permiten tener mayor capacidad de procesamiento que un equipo de uso personal.

- **Sistema de archivos**: Estructura que se le asigna a un dispositivo de almacenamiento de información para la disposición de los archivos.

- **Software**: Conjunto de componentes o instrucciones lógicas que puede ejecutar una computadora.

- **Software antivirus**: Software especializado en la detección, reconocimiento y limpieza de código malintencionado en archivos digitales.

- **Software malicioso**: Es un tipo de software que tiene como objetivo infiltrarse o dañar un equipo de cómputo sin el consentimiento de su propietario.

- **Tele trabajador:** persona que utiliza la telemática para la realización de su profesión. Esta actividad se realiza fuera del establecimiento empresarial. El aspecto principal del teletrabajador es tener mayor independencia en la realización del trabajo, sin embargo, debido a la evolución de la tecnología la Persona debe desempeñar actividades laborales a través de tecnologías de la información y comunicación por fuera de la ESE CRIB.

- **Unidad de red o carpeta compartida**: Medios informáticos conectados en una red corporativa, para compartir y almacenar información.

USB: Es un dispositivo de almacenamiento de información que utiliza una memoria flash para guardar información.

- **Usuario:** Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos sin identificación de un sujeto.

- **Ventanas emergentes**: El término denomina a las ventanas del navegador de Internet que emergen automáticamente (generalmente sin que el usuario lo solicite). A menudo, las ventanas emergentes se utilizan con el objeto de mostrar un aviso publicitario de manera intrusiva.

- **Virus informático**: Es un programa que tiene por objeto alterar el normal funcionamiento de un equipo de cómputo sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de éste. Los virus pueden destruir, de manera intencionada, los datos almacenados en un sistema de cómputo

5. OBJETIVO GENERAL:

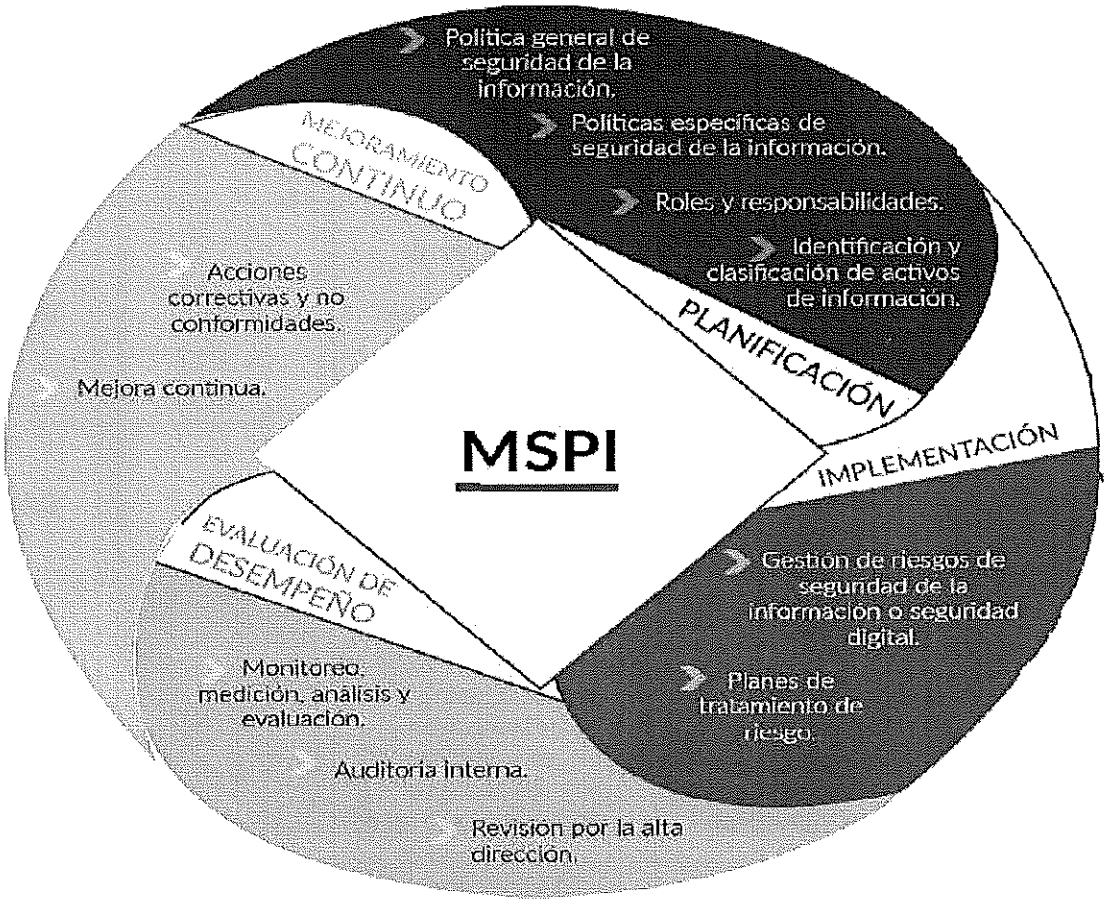
Implementar en la E.S.E CRIB las políticas y lineamentos de seguridad y privacidad de la información en conformidad con los lineamientos de MIN TIC, para garantizar la confidencialidad, integridad y disponibilidad y protección de datos.

6. OBJETIVOS ESPECIFICOS:

- Promover una cultura orientada a la seguridad de la información al interior de la E.S.E CRIB.
- Mantener altos niveles de confidencialidad, integridad y disponibilidad de los activos de información críticos de la E.S.E CRIB.
- Concientizar y sensibilizar a todos los funcionarios, colaboradores, proveedores, contratistas y personas de interés general, acerca del uso racional y seguro de la infraestructura informática, sistemas de información, servicios de red y canales de comunicación.
- Atender de manera eficiente y eficaz los incidentes de seguridad de la información que se presenten en la E.S.E CRIB.
- Controlar, mitigar y/o prevenir impactos ocasionados por posibles materializaciones de riesgos de seguridad de la información, mediante la definición e implementación de medidas de control.
- Dar cumplimiento a la legislación vigente asociada a la seguridad de la información.
- Asegurar el proceso de respuesta a los hallazgos de revisiones y/o auditorias, a través de identificación y ejecución de planes de acción.

7. METODOLOGÍA:

De acuerdo a los lineamientos dispuestos por el MIN TIC, se plantea tener una mejora continua en los procesos de seguridad de la información basándonos en el ciclo PHVA, teniendo en cuenta todos los factores que intervengan en ella tanto externos como internos, y así se genera su plan de mejoramiento para el seguimiento de los indicadores.



8. PLAN DE ACCIÓN:

NO	ACTIVIDAD	INDICADOR	TIEMPO	RESPONSABLE
1	Elaborar la política de privacidad de la información según el lineamiento AD 1 del modelo MSPI	Política de privacidad de la información documentada y aprobada	Febrero	Sistemas
2	Elaborar formato de acuerdo de transferencia de información	Formato de acuerdo de transferencia de información Codificado	Febrero	Sistemas
3	Elaborar Reporte de eventos e incidentes de seguridad de la información de la vigencia 2021.	Reporte de eventos e incidentes de seguridad de la información de la vigencia 2021, certificado por el área de sistemas	Febrero	Sistemas
4	Elaborar diagnóstico de seguridad y privacidad de la información para la vigencia, construido a través de la herramienta	Diagnóstico de seguridad y privacidad de la información para la vigencia, construido a través de la herramienta	Febrero	Sistemas

	de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI).	de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), Socializado en comité de gestión y desempeño		
5	Elaborar organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.	Marzo	Sistemas
6	Socializar política de privacidad de la información según el lineamiento AD 1 del modelo MSPI	Capacitación sobre política de privacidad de la información según el lineamiento AD 1 del modelo MSPI	Marzo	Sistemas
7	Realizar la autoevaluación de infraestructura de red de comunicaciones (IPv4/IPv6)	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección	Abril	Sistemas
8	Elaborar Inventario de partes externas o terceros a los que se transfiere información de la entidad	Inventario de partes externas o terceros a los que se transfiere información de la entidad documentado	Abril	Sistemas
9	Elaborar documento del Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información	Documento del Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información, enviado al área jurídica para su revisión.	Abril	Sistemas - Jurídico

10	Elaborar procedimiento de implementación del modelo de seguridad y privacidad de la información en E.S.E CRIB	Procedimiento de implementación del modelo de seguridad y privacidad de la información en E.S.E CRIB, documentado y aprobado.	Junio	Sistemas
11	Documentar y evaluar la Declaración de aplicabilidad	Declaración de aplicabilidad	Noviembre	Sistemas
12	Elaborar Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, para revisión y aprobación de la alta dirección	Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información revisado y aprobado por la alta dirección	diciembre	Sistemas
13	Elaborar Documento con el resultado de la estratificación de la entidad, para aprobación por parte de la alta dirección	Documento con el resultado de la estratificación de la entidad, aprobado por la alta dirección	diciembre	Sistemas
14	Elaborar Procedimiento de control documental del MSPI, en conformidad con el nivel de madurez de la ESE CRIB	Procedimiento de control documental del MSPI, en conformidad con el nivel de madurez de la ESE CRIB	diciembre	Sistemas

9. APROBACION

La gerencia de la Empresa Social del Estado Centro de Rehabilitación Integral de Boyacá aprueba el Plan se seguridad y privacidad de la información de Adquisiciones a los treinta y uno (31) días del mes de enero de dos mil veinte DOS (2022).

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

ELABORÓ	REVISÓ	APROBÓ
Nombre: Camilo Andrés Rodríguez Farfan. **Cargo:** Técnico Operativo **Fecha:** 29/01/2022	**Nombre:** Diego Fernando Rivera Castro **Cargo:** Asesor Planeación **Fecha:** 29/01/2022	**Nombre:** Zulma Cristina Montaña Martínez **Cargo:** Gerente **Fecha:** 29/01/2022

CONTROL DEL DOCUMENTO

MODIFICACIONES						
VERSION ANTERIOR	NUEVA VERSION	FECHA CAMBIO	DESCRIPCION DEL CAMBIO	ELABORO	REVISO	APROBÓ
	1	29/01/2021	Creación del documento	Diego Fernando Rivera Castro.	Comité de Control Interno.	Zulma Cristina Montaña Martínez.

LOCALIZACION DEL DOCUMENTO			
CODIGO	NOMBRE	COPIAS	UBICACIÓN
PL-GRT-002	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	ORIGINAL	Oficina de Calidad
PL-GRT-002	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	COPIA CONTROLADA	Sistema de Consulta MIPG