Plan de Seguridad y Privacidad de la Información 2024

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

Andrea Del Pilar Chona Bolívar
Subgerente Administrativo y financiero

Camilo Andrés Rodríguez Farfán
Técnico Operativo

Cesar David Parra
Asesor de Planeación

TABLA DE CONTENIDO

INTRODUCCIÓN

Uno de los activos más cruciales para la E.S.E CRIB es la información. En este sentido, resulta imperativo adoptar las mejores prácticas y directrices establecidas tanto por el Departamento Administrativo de la Función Pública, a través de su estrategia MIPG, como por el Ministerio de las Tecnologías de la Información. Este enfoque abarca desde el diagnóstico hasta la mejora continua en la gestión del Modelo de Seguridad y Privacidad de la Información.

El plan de seguridad y privacidad de la información constituye una parte esencial del plan de acción de la gerencia de la Empresa Social del Estado Centro de Rehabilitación Integral de Boyacá, en total conformidad con el artículo 1 del Decreto 612 de 2018. Dicho decreto establece las directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

Este plan tiene como objetivo la plena 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. Este modelo está 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 de manera continua para adaptarse a los cambios técnicos de la Norma NTC ISO 27001 "Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI)". Este enfoque estratégico garantiza que las decisiones relacionadas con los sistemas de información estén alineadas con las directrices del Gobierno Nacional, como se establece en el plan de desarrollo 2018-2022 "Pacto por Colombia, Pacto por la equidad" (Ley 1955 de 2019, artículos 147 y 148) y el CONPES 3854 de 2016 "Política Nacional de Seguridad Digital". Este compromiso asegura el establecimiento de una política de mejoramiento continuo en seguridad de la información, promoviendo una gestión más eficiente de los procesos institucionales.

1. DESARROLLO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

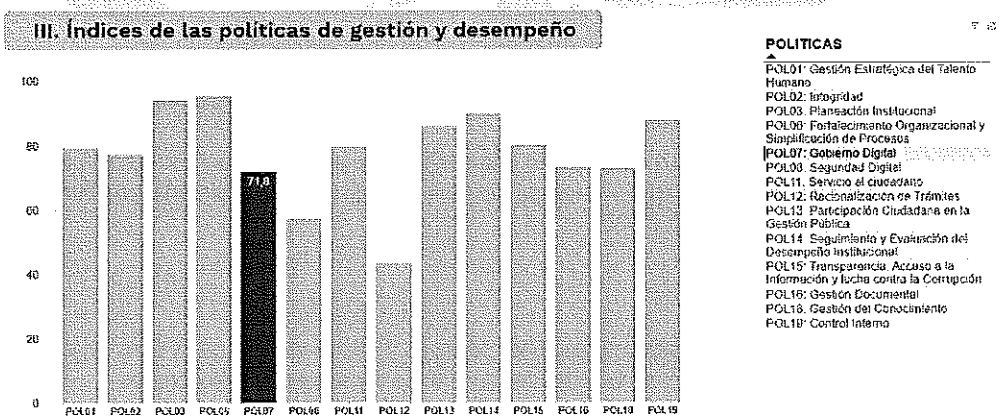
2. DIAGNOSTICO

Considerando los resultados de la encuesta del FURAG realizada durante el año 2023 y el porcentaje obtenido en el Plan de Seguridad y Privacidad de la Información correspondiente a dicho año, se identificaron áreas de oportunidad para el fortalecimiento de estos aspectos. Estas conclusiones han llevado a la formulación de actividades específicas con el objetivo de crear un Plan de Mejoramiento para el año 2024, que no solo aborde las necesidades planteadas en la vigencia anterior, sino que también supere las expectativas y eleve los estándares de seguridad y privacidad de la información en la entidad.

El diseño de este plan se fundamenta en un enfoque proactivo, considerando las lecciones aprendidas y aplicando las mejores prácticas identificadas durante la evaluación de la encuesta FURAG y la revisión del desempeño en seguridad y privacidad de la información en el año anterior. Asimismo, se priorizan aquellas áreas que han demostrado ser críticas para el adecuado funcionamiento del área de sistemas de información.

Las actividades propuestas abarcan aspectos clave, tales como la revisión y actualización de políticas y procedimientos, la implementación de medidas de seguridad adicionales basadas en los hallazgos de la encuesta, la capacitación continua del personal en cuestiones de seguridad informática, y el fortalecimiento de los mecanismos de respuesta a incidentes.

Este Plan de Mejoramiento no solo se orienta a cumplir con los estándares establecidos, sino que también busca instaurar una cultura de mejora continua en el área de sistemas de información. La participación activa y la colaboración de todo el personal serán fundamentales para el éxito de estas iniciativas, garantizando así un desarrollo integral y sostenible en la gestión de la seguridad y privacidad de la información en la entidad durante el año 2024.



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 2020-2024"

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:

Establecer en la E.S.E CRIB las políticas y directrices de seguridad y privacidad de la información, alineadas con las recomendaciones del Ministerio de Tecnologías de la Información y las Comunicaciones (MIN TIC), con el fin de asegurar la confidencialidad, integridad y disponibilidad, así como la protección efectiva de los datos.

6. OBJETIVOS ESPECIFICOS:

- Fomentar una cultura organizacional centrada en la seguridad de la información dentro de la E.S.E CRIB.
- Garantizar los niveles de confidencialidad, integridad y disponibilidad para los activos críticos de información en la E.S.E CRIB.
- Concientizar y sensibilizar a todo el personal, colaboradores, proveedores, contratistas y otras partes interesadas sobre la importancia de un uso responsable y seguro de la infraestructura informática, sistemas de información, servicios de red y canales de comunicación.
- Responder de manera eficiente y eficaz a los incidentes de seguridad de la información que puedan surgir en la E.S.E CRIB.
- Controlar, mitigar y prevenir posibles impactos derivados de riesgos de seguridad de la información mediante la definición e implementación de medidas de control.
- Cumplir con la legislación vigente relacionada con la seguridad de la información.
- Asegurar un proceso efectivo de respuesta a los hallazgos derivados de revisiones y auditorías, mediante la identificación y ejecución de planes de acción

7. METODOLOGÍA:

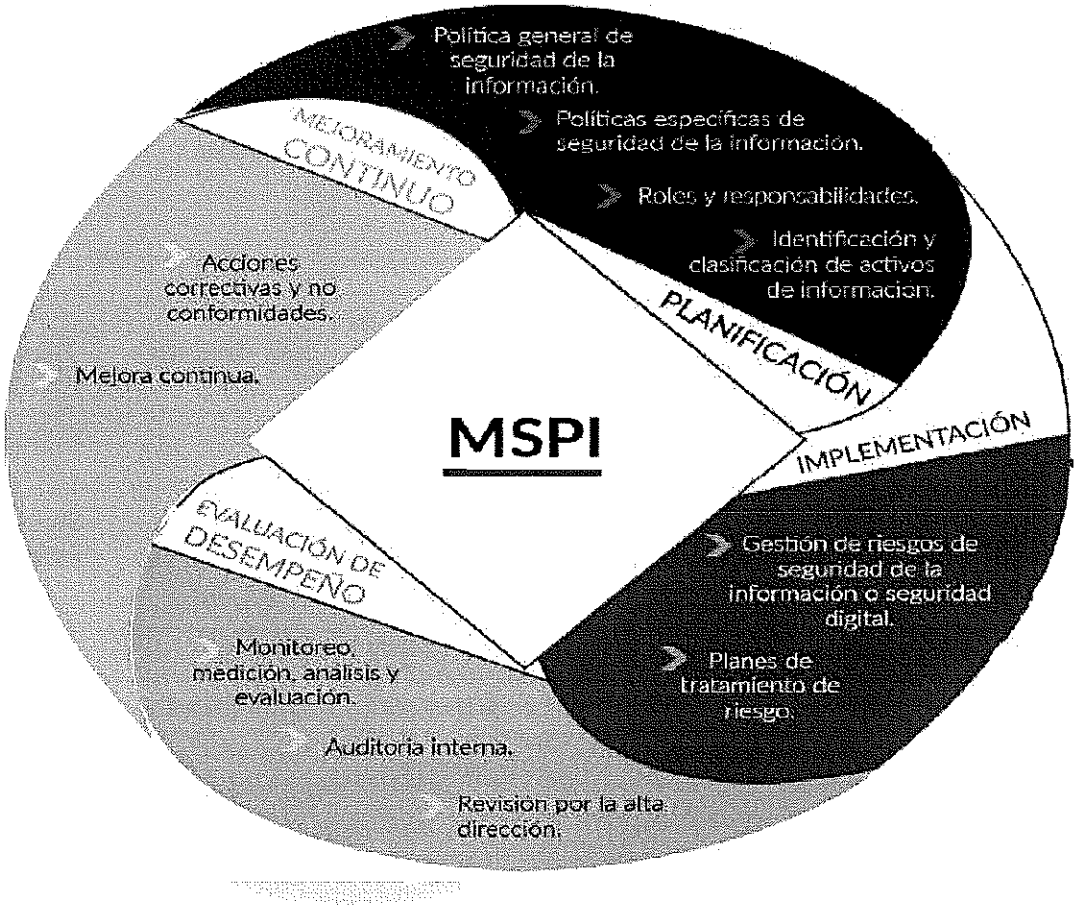
Conforme a las directrices establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MIN TIC), se propone implementar una mejora continua en los procesos de seguridad de la información. Este enfoque se fundamenta en el ciclo PHVA (Planificar, Hacer, Verificar y Actuar), que permite un abordaje sistemático y cíclico para optimizar la seguridad de la información en la E.S.E CRIB.

En este sentido, se busca considerar todos los factores que puedan influir en la seguridad de la información, tanto desde una perspectiva interna como externa. Esto implica evaluar riesgos, identificar vulnerabilidades, y adaptarse a cambios en el entorno tecnológico y normativo.

El plan de mejora resultante estará diseñado de manera integral, abarcando aspectos como políticas y procedimientos, tecnologías de seguridad, capacitación del personal y respuesta a incidentes. Además, se establecerán indicadores clave de rendimiento (KPIs) que permitirán monitorear y evaluar la eficacia de las medidas implementadas.

Este enfoque no solo garantiza el cumplimiento de las directrices del MIN TIC, sino que también posiciona a la E.S.E CRIB para adaptarse proactivamente a los cambios en el panorama de seguridad de la información. Asimismo, al integrar la metodología PHVA, se promueve una gestión ágil y dinámica, permitiendo ajustar estrategias y tácticas en tiempo real a medida que evolucionan los riesgos y las exigencias normativas. La

adopción de esta mentalidad de mejora continua no solo fortalece la seguridad de la información, sino que también contribuye a una gestión más eficiente y resiliente en la entidad.



8. PLAN DE ACCIÓN:

NO	ACTIVIDAD	INDICADOR	TIEMPO	RESPONSABLE
1	Definir un proceso de gestión y gobierno de TI, formalizado a través del Sistema Integrado de Gestión de Calidad de la entidad	Socializar y optimizar el Procedimiento de implementación de Política de Seguridad de información.	Marzo	Sistemas
2	Implementar política de modelo de seguridad y privacidad de la información.	Número de actividades ejecutadas del plan / Numero de actividades planteadas en el plan	Junio - Noviembre	Sistemas
3	Definir aprobar e implementar procedimiento de seguridad y privacidad de la información.	Implementar Procedimiento de implementación de Política de Seguridad de información.	Junio - Noviembre	Sistemas

4	Definir el procedimiento para la atención de incidencias o requerimientos en el servicio tecnológico.	Implementar procedimiento para la atención de incidencias o requerimientos en el servicio tecnológico.	Junio - Noviembre	Sistemas
5	Verificar las necesidades de soluciones de antivirus para los servidores físicos, servidores virtuales y los computadores de la entidad.	Documento con las necesidades tecnológicas de la vigencia 2024.	Febrero	Sistemas
6	Realizar análisis de vulnerabilidades de seguridad a los activos de información (hardware, software, aplicaciones, redes).	Documento de incidentes de seguridad semestralmente.	Junio - Diciembre	Sistemas
7	Socializar el autodiagnóstico en materia de Seguridad Digital en el marco del Comité de Gestión y Desempeño Institucional.	Realizar autodiagnóstico de FURAG	Febrero	Sistemas – Planeación
8	Establecer un procedimiento para la gestión de incidentes de seguridad digital.	Socializar y optimizar procedimiento para la atención de incidencias o requerimientos en el servicio tecnológico.	Junio - Noviembre	Sistemas

9. APROBACION

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

Centro de Rehabilitación Integral de Boyacá E.S.E

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

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