Plan de Seguridad y Privacidad de la Información 2021

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

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 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.

DESARROLLO

1. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

2. DIAGNOSTICO

La Empresa Social del Estado Centro de Rehabilitación Integral de Boyacá es una persona jurídica de derecho público dotada legal y estatutariamente de las características especiales inherentes de las entidades del nivel descentralizado departamental, cuenta con personería jurídica, patrimonio propio y autonomía administrativa, sometida al régimen jurídico previsto en el CAPÍTULO III, Artículos 194, 195 y 197 de la Ley 100 de 1993 y sus decretos reglamentarios, por el derecho privado en lo que se refiere a contratación y por el Estatuto de Contratación propio.

La Empresa Social del Estado Centro de Rehabilitación Integral de Boyacá es una empresa especializada en atención en salud mental del departamento de Boyacá, ofrece servicios asistenciales de alta calidad, garantizando eficiencia en la prestación del servicio; dentro de su portafolio de servicios se encuentra servicios Hospitalarios de psiquiatría adulto y ambulatorios de psiquiatría, psiquiatría infantil, neurología, neurología pediátrica, psicología clínica, apoyo terapéutico, apoyo diagnóstico.

La Empresa Social del Estado Centro de Rehabilitación Integral de Boyacá cumple con los lineamientos de seguridad de la información relacionada con historias clínicas, facturación, información financiera, contractual, talento humano y demás que requieran seguridad informática.

La Empresa Social del Estado Centro de Rehabilitación Integral de Boyacá cuenta actualmente con diferentes controles de seguridad, entre ellos los antivirus, accesos limitados a la información según el perfil del profesional, usuarios protegidos con contraseña para cualquier modificación y/o uso, entre otros.

De acuerdo al diagnóstico organizacional llevado a cabo en el mes de junio de 2020 con fines de construcción del plan de desarrollo institucional se identificó un 55% de factores negativos en la cultura organizacional, lo cual se muestra en la siguiente figura:

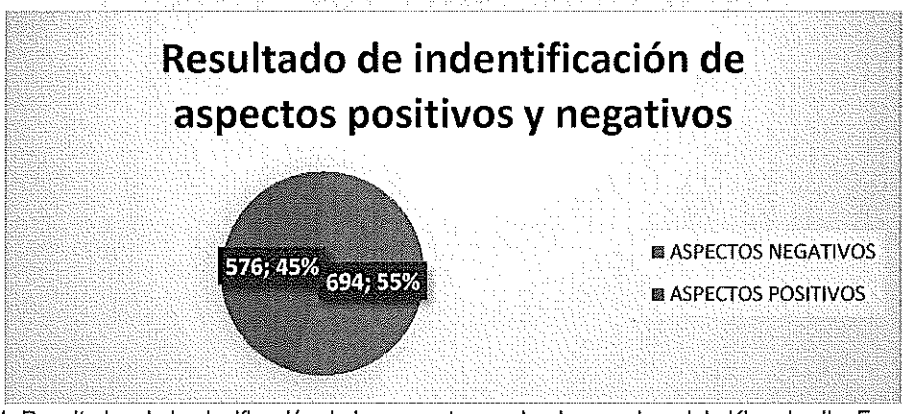


Figura 1. Resultados de la clasificación de los aspectos evaluados en el modelo Khandwalla. Fuente:Plan de desarrollo 2020-2023 "Avanzamos por la salud mental de Boyacá"

De acuerdo a las variables estudiadas en la precitada metodología, se identificó:

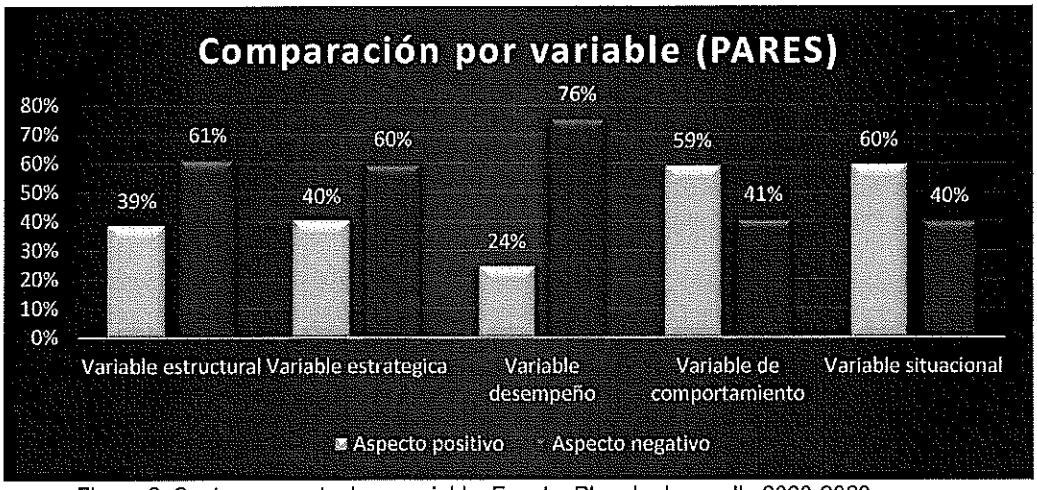


Figura 2. Conteo porcentual por variable. Fuente: Plan de desarrollo 2020-2023

La figura 2, nos indica que en la variable estructural hay un 61% de aspectos negativos, mientras en la variable comportamiento los aspectos positivos llegan a un 59%, esto indica y de acuerdo al diagnóstico organizacional llevado a cabo que la cultura organizacional de la empresa es rígida, pero con las adecuadas motivaciones y directrices se pueden enfocar en una cultura de mejoramiento continuo, en la cual aunque se puede esperar en un principio una resistencia al cambio, la empresa se puede adaptar a la implementación de controles de seguridad de la información.

La estructura organizacional de la Empresa es la siguiente:

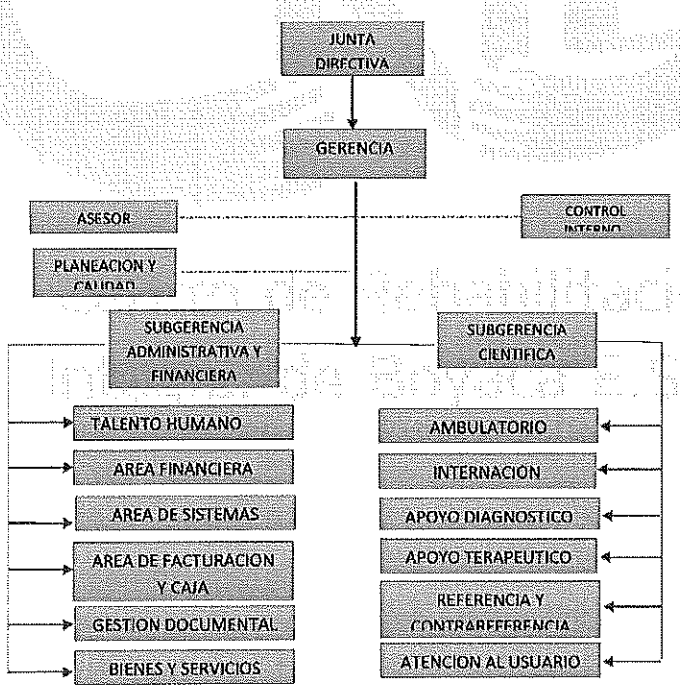


Figura 3. Organigrama de la Empresa.

En esta estructura se puede observar que los procesos institucionales están enfocados en una parte asistencial liderada por la subgerencia científica y una parte administrativa liderada por la subgerencia administrativa y financiera, esta estructura marca el funcionamiento organizacional, el cual se organiza a través de comités

Institucionales mediante los cuales se establecen los debidos canales de comunicación y planes de acción para el funcionamiento organizacional de la entidad.

Además, la alta dirección desde la gerencia y sus subgerencias tienen establecidos de manera oportuna canales de comunicación con las demás dependencias de la empresa, aunado a esto es menester mencionar que para la construcción del plan de desarrollo se tuvo en cuenta todos los colaboradores de la organización a través de mesas de trabajo organizadas por áreas.

La Empresa Social del Estado Centro de Rehabilitación Integral de Boyacá tiene actualmente 36 funcionarios de planta, para poder garantizar la adecuada prestación del servicio se contratan colaboradores mediante contratos de prestación de servicios, lo cual implica cambios en los líderes de ciertos procesos , lo cual hace que se no se establezca una memoria institucional de forma adecuada, aunado a esto no existe documentación sobre los procesos y procedimientos para garantizar esta memoria institucional.

Actualmente contamos con información física la cual reposa en un archivo según la dependencia, la información que se encuentra registrada en el software CNT se realiza un backup diario en el servidor 1 de la entidad, en el software Armorum se genera un backup cada mes en el servidor 2 de la entidad y la información de cada puesto de trabajo se encuentra respalda en un disco duro del área de sistemas el cual realiza backup cada 3 meses.

Se realiza constante actualización a los diferentes puestos de trabajo de la entidad y de igual manera a los softwares que se cuenta en la institución (CNT, ARMORUM).

Actualmente la Empresa no cuenta con procesos uniformes y algunos no guardan coherencia con las practicas operativas institucionales.

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.*"

- 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:

Establecer las directrices, lineamientos y medidas organizacionales, técnicas, físicas, legales y culturales para la adecuada gestión de la seguridad y privacidad de la información; enmarcadas en la implementación del MSPI (Modelo de Seguridad y Privacidad de la Información) definido por el MINTIC, identificando, valorando y gestionando los riesgos asociados a la misma y propendiendo por garantizar la confidencialidad, integridad y disponibilidad de la información para la empresa social del estado centro de rehabilitación integral de Boyacá.

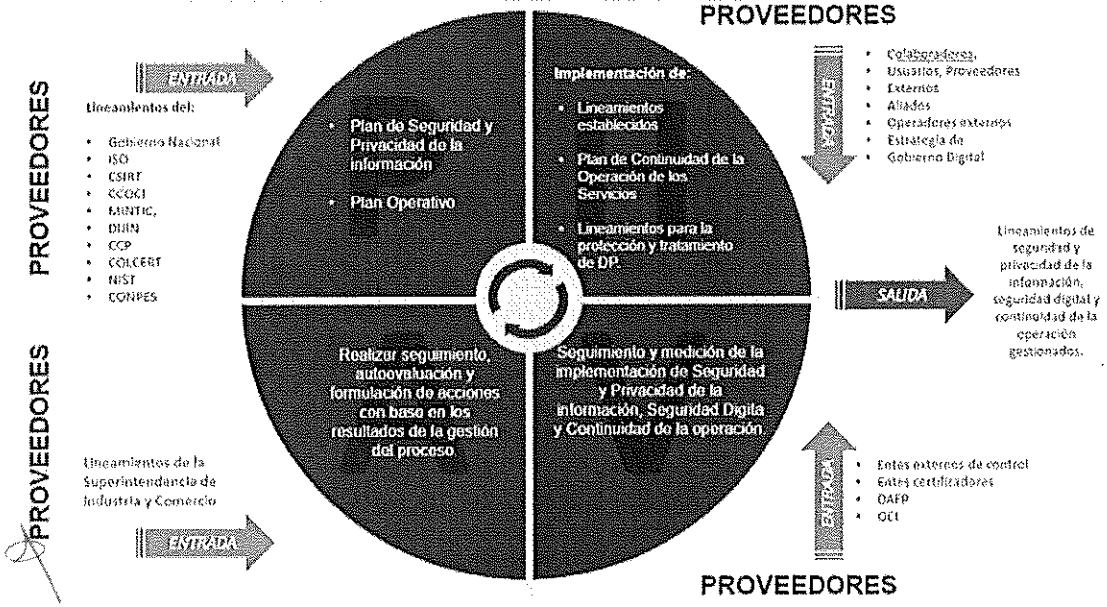
6. OBJETIVOS ESPECIFICOS:

- Garantizar la confidencialidad, integridad y disponibilidad de la información institucional como activo de la organización, con la incorporación de buenas prácticas, preservación de la infraestructura tecnológica y normas de calidad aplicables a la gestión segura de las Tecnologías de la Información y la Comunicación.

- Garantizar la protección de los datos personales de los cuales es responsabilidad la ESE CRIB en sistemas de información, bases de datos, soportes y equipos empleados en el tratamiento de los datos, teniendo en cuenta la normativa interna vigente

7. METODOLOGÍA:

De acuerdo a los lineamientos dispuestos por el ministerio de las telecomunicaciones, 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:

A continuación, se describe los diferentes lineamientos para la ejecución del MSPI (Modelo de Seguridad y Privacidad de la Información) y se realizara seguimiento trimestral y auditoria a la ejecución de las acciones planteadas.

8.1. LINEAMIENTOS DE SEGURIDAD PARA TELETRABAJO

Los lineamientos de seguridad para el teletrabajo comprenden: descripción del servicio y conexión remota a la red de datos, acceso al sistema de telefonía, acceso a servidores de archivos, acceso a sistemas de información, almacenamiento de la información, uso de hardware y software. Podrán aplicarse teniendo en cuenta el rol desempeñado en la ESE CRIB.

8.1.1. Descripción

La ESE CRIB ha adoptado modalidades de contratación de colaboradores en teletrabajo (Teletrabajadores), por lo tanto, se hace necesario establecer las condiciones técnicas y de seguridad sobre las cuales el teletrabajador accederá a los recursos, bases de datos personales y servicios de tecnología de la ESE CRIB.

8.1.2. Acceso a la red de datos

Para el desarrollo de las actividades en modalidad de Teletrabajo se puede requerir de una conexión remota a la red de datos de la ESE CRIB, a través de un aplicativo que cumpla con requisitos mínimos para garantizar la integridad y confidencialidad en la transferencia de información. En caso que el colaborador no requiera hacer uso de los servicios descritos a continuación, no se hace necesario la asignación de una VPN, pero deberá apoyarse en las herramientas colaborativas dispuestas por la empresa.

Para el establecimiento de la conexión remota se tienen en cuenta los siguientes aspectos:

Evitar establecer conexiones a redes inalámbricas desconocidas o que estén habilitadas sin seguridad, es decir, que no solicite claves de ingreso. El riesgo aparece cuando el punto de acceso está abierto intencionalmente con un propósito.

8.1.3. Almacenamiento de información

- Usar el repositorio institucional asignado por la ESE CRIB para guardar la información, en caso de almacenarla en los discos locales del equipo asignado, se debe utilizar la partición protegida y descargar la información en los repositorios institucionales posteriormente, para prevenir qué ante una situación de hurto del equipo de cómputo, se pierda y exponga la información de la institución.
- La conexión de medios extraíbles al equipo del Teletrabajador como (USB, Unidades CD/DVD, Discos externos, entre otros, son monitoreadas y eventualmente podrá ser restringida de acuerdo con los lineamientos que la ESE CRIB disponga para evitar la fuga de información y garantizar la confidencialidad y protección de los datos. En los equipos de cómputo de los Teletrabajadores no se permite el almacenamiento de archivos de música, videos y cualquier otro formato o información de carácter personal, salvo aquellos cuyo uso o almacenamiento sea para ejecutar labores propias de la empresa.
- La oficina de sistemas está facultada para eliminar archivos que no cumplan con los propósitos de la ESE CRIB.
- En caso de requerir documentos físicos o información en dispositivos de almacenamiento extraíbles (como USB, CD, discos duros externos, entro otros) para el desarrollo de su actividad, el Teletrabajador es responsable por la custodia y preservación de los mismos; se recomienda no dejarlos expuestos a terceros no autorizados, guardarlos bajo llave y en un lugar seguro. Tener en cuenta el tratamiento de datos personales de acuerdo a este manual.

8.1.4. Acceso a servidores de archivos

El acceso a servidores de archivos en modalidad de Teletrabajo se asigna de acuerdo a los perfiles autorizados para realizar las labores propias del cargo, por lo tanto, se debe tener en cuenta los siguientes aspectos:

- Velar por la seguridad y confidencialidad de la información contenida en los servidores de archivo.
- Evitar compartir el equipo de cómputo con personas no autorizadas, para que no exista un acceso no permitido a la información y a los sistemas de información de la ESE CRIB.

8.1.5. Acceso a los sistemas de información

El acceso a los sistemas de información en modalidad de Teletrabajo se asigna de acuerdo a los perfiles autorizados para realizar las labores propias del cargo, considerando los siguientes aspectos:

- Acceder con las credenciales asignadas al Teletrabajador para acceder a los sistemas de información.
- Las credenciales asignadas para el acceso a los sistemas de información, son de uso personal e intransferible, por tanto, no se comparten o divulgan.
- Salvaguardar la información contenida en los diferentes sistemas de información a los que se tenga acceso autorizado, evitando compartir el equipo de cómputo con personas ajenas.

8.1.6. Uso de hardware y software

El hardware y software otorgado por la ESE CRIB, para el desarrollo de la modalidad de Teletrabajo se utiliza únicamente para llevar a cabo las actividades laborales asignadas por la empresa. Por lo anterior se tienen en cuenta los siguientes aspectos:

- Evitar abrir correos electrónicos, descargar o ejecutar archivos de los cuales no se conozca su procedencia. Este tipo de práctica es una de las principales fuentes de virus o programas maliciosos, que pueden generar un daño irreversible al computador y afectar la confidencialidad de la información de la empresa.
- Evitar abrir y ejecutar ventanas emergentes, barras de herramientas, programas, enlaces desconocidos; estos pueden conducir a sitios de suplantación web para capturar datos que pueden afectar la disponibilidad, integridad y confidencialidad de la información de la empresa.
- Evitar instalar programas ajenos a los autorizados por la ESE CRIB o que no correspondan al desarrollo normal de las actividades asignadas. El único proceso autorizado para instalar software en los equipos de cómputo institucionales es el proceso de gestión de la información.
- La oficina de sistemas, instala una herramienta de antivirus para proteger el equipo de amenazas de virus, es recomendable que el Teletrabajador compruebe el correcto funcionamiento del mismo, y si presenta alguna falla se reportan para el servicio de soporte necesario.

El Teletrabajador es responsable por los daños ocasionados a los equipos de cómputo generados por mal uso de los mismos, por lo tanto, se tienen en cuenta las siguientes recomendaciones:

- Evitar exponer el equipo de cómputo en sitios públicos como centros comerciales o campos abiertos.
- Hacer uso del equipo de cómputo asignado únicamente en el lugar de teletrabajo aprobado por la ESE CRIB.
- Evitar exponer el equipo de cómputo en zonas donde exista humedad.
- Evitar golpes y consumir líquidos mientras se desarrollan actividades de Teletrabajo ya que existe el riesgo de avería parcial o total del equipo de cómputo.
- Evitar utilizar o dejar el equipo de cómputo donde pueda sufrir calentamiento, esto generaría daño en la fuente y a nivel general.
- En caso de pérdida o hurto del equipo de cómputo, el Teletrabajador debe informar inmediatamente a la gerencia.
- No está autorizado ningún tipo de modificación en el hardware.

- El Teletrabajador debe verificar el estado en el cual es entregado el equipo en el momento de su recepción. Para ello se genera un formato de entrega que debe ser firmado indicando conformidad en la entrega y recepción por parte del Teletrabajador.

8.2. LINEAMIENTOS DE SEGURIDAD PARA EL CORREO ELECTRÓNICO

8.2.1. Descripción

La ESE CRIB ha adoptado servicios de correo institucional, por lo tanto, se hace necesario establecer las condiciones técnicas y de seguridad sobre las cuales los funcionarios, contratistas y cualquier otro que tenga un vínculo directo y así lo amerite acceda a estos recursos.

8.2.2. Aspectos generales

- Cada cuenta de correo electrónico tiene asociado un conjunto de recursos de almacenamiento que es ilimitado.
- El servicio de correo administrativo permite la transferencia de archivos como adjuntos del mensaje o compartidos a través de sus herramientas.
- Las imágenes enviadas en el cuerpo del mensaje electrónico no son mayores a 10 Megabytes, un mayor peso de la imagen genera lentitud en la distribución y saturación del correo.
- Mientras no se acredite un vínculo directo con la ESE CRIB, ninguna persona o empresa podrá solicitar cuenta de correo asociada a los dominios institucionales.
- Las cuentas de usuario de correo son generadas bajo el estándar estipulado en la creación de cuentas de la ESE CRIB, en caso de que un usuario deba realizar un cambio de cargo se conserva la misma cuenta de correo, se parte del principio que el correo es un medio de comunicación mas no de almacenamiento de información.

8.2.3. Administración del correo electrónico

Creación, borrado o inactivación de las cuentas de correo electrónico

- Dominio "@cribsaludmental.gov.co"

La creación de las cuentas es realizada por orden de la gerencia.

La inactivación de la cuenta la realizará la oficina de sistemas, de acuerdo a la solicitud de la Gerencia una vez finalizado el contrato o por una ausencia temporal.

Todo correo, en su contenido y firma debe cumplir con lo definido por la gerencia.

8.2.4. Acceso al servicio de correo electrónico

Todo usuario de la empresa que posea una cuenta de correo institucional, puede acceder a esta dentro o fuera de las instalaciones de la ESE CRIB.

8.2.5. Uso del correo electrónico

- El correo electrónico pertenece a la ESE CRIB, bajo el contexto de uso institucional, propio de las actividades administrativas; estando terminantemente prohibido realizar cualquier otra actividad o transacción comercial.
- El uso inapropiado del correo electrónico de la institución acarrea la aplicación de las medidas disciplinarias a que haya lugar y demás acciones legales del caso.

- Se debe evitar el envío de archivos con extensiones .EXE, .BAT, .COM, .DLL, .VBS, por razones de seguridad y para evitar propagación de virus.
- Evitar abrir correos de los cuales no se conozca el remitente y absténgase de abrir los archivos adjuntos.
- Se prohíbe usar el correo institucional para: enviar contraseñas; enviar mensajes que inciten a la comisión de delitos; reenviar archivos de los que no se conozca su origen y que no sean confiables; distribuir información confidencial de la ESE CRIB; la difusión de insultos o información que atente contra la moral y buenas costumbres; distribuir mensajes que argumenten solicitudes de redistribución a otros correos o información publicitaria que sea diferente a los objetivos y propósitos de la ESE CRIB, enviar información que vulnere la confidencialidad de un tercero o que haga cuestionamientos públicos de la honra, la intimidad de las personas o violación de los datos personales.
- Se debe evitar usar cualquier forma engañosa de enviar correos electrónicos, como edición de fechas, remitentes, encabezados entre otros.
- Se debe evitar utilizar el correo para enviar cadenas, advertencias o cualquier tipo de mensaje similar.
- Se debe evitar usar claves de acceso débiles o fáciles de adivinar tales como: nombre propio, nombre de algún familiar cercano, fechas de nacimiento, aniversario, nombre de mascota, número de identificación, entre otras.
- Se recomienda cambiar la clave del correo, cuando ingrese por primera vez y de forma periódica.
- Toda la información contenida en los buzones de correo institucionales es propiedad de la ESE CRIB por lo tanto puede ser inspeccionada en cualquier momento a solicitud de los organismos de control interno o por requerimientos judiciales sin previo consentimiento del usuario de la cuenta de correo.
- Ninguna persona está autorizada para acceder a información de otro usuario. Solamente por motivos jurídicos o disciplinarios se abrirán los archivos a las instancias correspondientes, previo permiso de una autoridad competente.
- La oficina de sistemas es responsable de tomar las medidas necesarias para que el servidor no admita adjuntos en el correo que tengan virus informáticos, no obstante, se mantiene actualizado el sistema de antivirus de los equipos de cómputo propiedad ESE CRIB.
- Los equipos propiedad de la ESE CRIB cuentan con actualización del antivirus periódica, no se autoriza la desinstalación del mismo, la instalación de otra versión o marca del software de antivirus.
- El usuario dueño del buzón es responsable de todos los mensajes de correo que sean enviados a su nombre.
- Se debe informar a la oficina de sistemas sobre cualquier anomalía que sea detectada en el correo, así como la apertura de un correo sospechoso o cualquier alerta generada por el antivirus o en caso de detectar algún tipo de incidente de seguridad.

Son considerados actos inapropiados contra el servicio de correo electrónico en la ESE CRIB aquellos que afecten la disponibilidad del servicio tales como:

- Ataques de denegación de servicios a los servidores de la ESE CRIB o que a través de la empresa se realicen hacia terceros.
- Ataques de fuerza bruta para obtener credenciales de acceso a cualquier servidor o servicio de la ESE CRIB o utilizar la infraestructura de la empresa para realizar cualquier ataque hacia terceros.
- Envío de correo masivo sin las autorizaciones correspondientes desde el correo de la ESE CRIB.
- Envío de información pornográfica u otra información que estimule la comisión de delitos.
- Accesos no autorizados a sistemas de correo de la ESE CRIB.
- Intercambio de mensajes que vaya en contra de la ley de derechos de autor o desfavorezca la protección de la propiedad intelectual o datos personales.
- Cualquier acto contrario a las presentes condiciones de uso será considerado un acto inapropiado y será sancionado conforme a las normas internas vigentes y a la legislación colombiana si el acto lo amerita.

8.3. LINEAMIENTOS DE SEGURIDAD PARA EL USO DE MEDIOS DE ALMACENAMIENTO EXTRAÍBLES O REMOVIBLES

8.3.1. Descripción

La utilización de dispositivos removibles o extraíbles de almacenamiento (Memorias USB/Flash, SD, microSD, CD/DVDs re escribibles, discos duros portátiles, dispositivos electrónicos como celulares, tablets, entre otros) por parte de los usuarios, se encuentra restringido, y podrá ser autorizado a algunos funcionarios directos de la ESE CRIB que lo requieran, cumpliendo con los lineamientos estrictamente establecidos por la empresa. El colaborador que los utilice con la autorización respectiva deberá buscar en todo momento preservar la Confidencialidad de la información de la ESE CRIB almacenada en éste, así como evitar contagiar la red de la empresa de código malicioso o dañino (virus, troyanos, Spyware, etc.).

8.3.2. Uso de medios de almacenamiento extraíbles

- Evitar hacer copias de respaldo de información en estos medios, se debe guardar en los repositorios institucionales para el almacenamiento de información, según corresponda.
- No se divulga, ni transfiere la información almacenada en los medios extraíbles a personas ajenas a la empresa. Esto puede comprometer la confidencialidad de la información de la ESE CRIB.
- Los usuarios o personas que pertenezcan a servicios tercerizados contratados por la ESE CRIB, no podrán utilizar dispositivos removibles o extraíbles de almacenamiento (Memorias USB/Flash, SD,microSD, CD/DVDs re escribibles, discos duros portátiles, dispositivos electrónicos como, tablets, entre otros) diferentes a los asignados y autorizados para cumplir o ejecutar sus labores en las instalaciones teniendo en cuenta situaciones en las cuales posea o manipule información de la ESE CRIB..
- El servicio de navegación prestado por la ESE CRIB es suministrado y autorizado únicamente para propósitos de la prestación de servicios de salud, y podrá ser restringida o limitada a áreas consideradas confidenciales, debido a que gestionan o manipulan información clasificada como confidencial o sensible para la ESE CRIB.

Si se utiliza los medios de almacenamiento extraíbles autorizados en un equipo de cómputo diferente al de la ESE CRIB se tiene en cuenta las siguientes recomendaciones:

- Copiar información almacenada en los medios de almacenamiento extraíbles a los discos locales del equipo de cómputo asignado solamente después del escaneo previo.
- Al momento de conectar los medios de almacenamiento extraíbles al equipo de cómputo de la ESE CRIB., realiza un escaneo previo con el antivirus autorizado por la empresa con el fin de evitar que se transfieran virus informáticos y software malicioso.
- No exponer los medios de almacenamiento extraíbles en lugares públicos.
- Proteger los medios de almacenamiento extraíbles de humedad y golpes.
- Evitar consumir bebidas durante la utilización de los medios extraíbles.

8.4. LINEAMIENTOS DE SEGURIDAD PARA COPIAS DE RESPALDO

8.4.1. Descripción

Los sistemas de información que almacenan, procesan o transmiten información clasificada como confidencial, en infraestructura tecnológica propia de la ESE CRIB (Físicos o virtuales) o contratados a terceras partes (Físicos o en Internet), deberán asegurar la generación de copias de respaldo, su periodo de retención, rotación y métodos apropiados para su restauración. Estas copias de seguridad deben estar en lugares apropiados cumpliendo los requisitos de condiciones ambientales y de seguridad, en custodia para garantizar su integridad y disponibilidad y realizar una verificación periódica que los datos retenidos en los medios son fiables y garantizan una recuperación de los sistemas.

Las copias de respaldo de todos los sistemas de información y/o aplicativos contenidos en los servidores de la ESE CRIB se realizan bajo los lineamientos establecidos en el documento procedimiento de copias controladas que se encuentre vigente, bajo la responsabilidad de la oficina de calidad.

Desde la oficina de sistemas se realizan copias de respaldo de los equipos de cómputo de los funcionarios, que las solicitan.

En casos especiales que se necesite realizar copia de respaldo de un equipo específico, la solicitud se debe realizar a la Gerencia quien comunicará a la oficina de sistemas.

8.4.2. Restauración de copias de respaldo

Mediante el proceso de restauración de copias de respaldo se logra obtener información que por causas diversas sufrió pérdida o modificación, se requiera verificar datos que por alguna razón no son consistentes o para realizar pruebas de integridad.

8.4.3. Respaldo de servicios alojados en internet o en sitios alternos de proveedores de servicios

- *Para servicios en modalidad de Alojamiento Web:*

- Cuando se contrate o configure un servicio en la modalidad de hosting, a través del contrato el proveedor debe garantizar la realización de copias de respaldo periódicos a los datos, las aplicaciones y demás información según las necesidades de cada servicio.
- Se tiene en cuenta las tablas de retención de información para las copias de respaldo de acuerdo a lo definido en la empresa.
- Al finalizar el contrato, el proveedor debe entregar copia de toda la información de la empresa en un formato estándar y legible.
- El proveedor garantiza contractualmente la confidencialidad de la información que se encuentre alojada en sus equipos, teniendo en cuenta los lineamientos definidos en este manual para la administración de datos personales y un contrato de transmisión de datos vigente.
- Se tiene en cuenta las tablas de retención de información para las copias de respaldo de acuerdo a lo definido en la empresa.

8.5. LINEAMIENTOS DE SEGURIDAD PARA LOS REPOSITORIOS INSTITUCIONALES

8.5.1. Descripción

La ESE CRIB ofrece tres tipos de repositorios institucionales, con el propósito de garantizar el respaldo y asegurar, proteger y centralizar la información de cada proceso. El acceso a los repositorios institucionales se da a través del usuario y contraseña asignados a los funcionarios para la sesión de red o cuenta de correo electrónico; por lo cual el acceso a los repositorios es responsabilidad exclusiva de los funcionarios.

La oficina de sistemas, garantiza la disponibilidad de los repositorios institucionales.

8.5.2. Uso de los repositorios institucionales

- Evitar divulgar y/o transferir la información sensible almacenada en los repositorios institucionales a personas no autorizadas.
- El usuario al cual se asigna un equipo de cómputo, es el único responsable del equipo asignado y de la información de la ESE CRIB a la que se acceda a través de este.
- Las credenciales asignadas para el acceso a los repositorios institucionales son de uso personal e intransferible.
- El usuario es responsable de bloquear la sesión de red o su cerrar su cuenta de correo electrónico al momento de levantarse del puesto de trabajo.

La información que se guarda en estos repositorios institucionales es la siguiente:

- Información registros del sistema de gestión de calidad.
- Información que este en versión final (Informes, presentaciones, hojas trabajo, contratos entre otros)

- Información que cada proceso considere importante para el desarrollo de sus actividades y/o que deba mantenerse bajo controles de seguridad y con su respectivo respaldo y protección, para mitigar el riesgo de pérdida de información o acceso indebido o no autorizado a la misma.

La información que NO se guarda en las unidades de red o carpetas compartidas es la siguiente:

- Información personal, música en cualquier formato, videos, fotos e imágenes cuya propiedad intelectual no sea de la ESE CRIB o que vaya en contra de las normas vigentes relacionadas con derechos de autor y privacidad.
- Información cuya procedencia sea desconocida.
- Información que no se considere relevante para la normal ejecución de las actividades de cada proceso debe guardarse en los discos locales (Unidades nombradas con C y/o D) del equipo de cómputo asignado a cada usuario.

Para el almacenamiento y asignación de nombres a los archivos que se guarden en los repositorios institucionales (carpetas compartidas) se tiene en cuenta:

- La estructura de carpetas de los repositorios asignados a cada proceso ha sido definida de acuerdo a lo siguiente:
  -> Carpeta con Nombre de proceso
  -> Subcarpeta del año
  -> Subcarpetas por áreas o subprocesos
  -> Subcarpeta compartida para el proceso

  Para solicitar la recuperación de información de la copia respaldo de los repositorios institucionales se realiza la solicitud a la Gerencia.

8.6 LINEAMIENTOS DE SEGURIDAD PARA LA ADMINISTRACIÓN DE CUENTAS Y CONTRASEÑAS DE USUARIO

8.6.1. Descripción

El acceso a la mayoría de los servicios de tecnología se da por medio de la validación de un nombre de usuario y una contraseña, por lo tanto, es necesario definir los lineamientos para que estas credenciales de acceso tengan los elementos de seguridad básicos para minimizar el riesgo de acceso por parte de personas no autorizadas.

8.6.2. Administración de cuentas

La administración de cuentas contempla los distintos tipos de cuenta y las medidas pertinentes para la vinculación o la desvinculación del personal directo o de terceros en la ESE CRIB. Entre ellos se crea, cancela o deshabilita los permisos de acceso a los sistemas de información de la empresa que el usuario utilice y se elimina cualquier vínculo a nivel de publicaciones y de cualquier tipo contractual que se encuentre habilitado.

8.6.3. Cuentas normales

- La subgerencia administrativa o científica, informará a la oficina de sistemas cuando ingrese un nuevo funcionario, para asignar las cuentas, con los perfiles correspondientes a cada sistema de información para desempeñar el cargo.
- Las cuentas de usuario serán la identificación única para acceder a los diferentes sistemas de información y/o aplicativos y recursos informáticos de la ESE CRIB.

- Cada cuenta de usuario normal tiene los privilegios de accesos debidamente autorizados para desempeñar las labores propias al cargo para el cual fue contratado.

8.6.4. Cuentas privilegiadas

Se entiende como cuentas privilegiadas aquellas credenciales de acceso con privilegios de administración sobre los sistemas de información, motores de bases de datos o software base (sistemas operativos). Estas cuentas son asignadas al técnico operativo los rigen los siguientes lineamientos.

8.6.5. Uso de cuentas y contraseñas de usuario

- Todas las credenciales asignadas son de uso personal e intransferible, por tanto, no se comparten ni divulgan bajo ninguna circunstancia.
- Evitar usar contraseñas de acceso débiles o fáciles de adivinar como: nombre propio, nombre de algún familiar cercano, fechas de nacimiento, aniversario, nombre de mascota, número de identificación, entre otras.
- Evitar almacenar las contraseñaeaas en sistemas de computador, en archivos de software o dispositivos, manuales o formatos no protegidos.
- Evitar dejar las contraseñas en un lugar visible a personas no autorizadas.
- Evitar formar contraseñas con números y/o letras que estén adyacentes en el teclado. Ejemplos: 123456, 1q2w3e o 123QWEasd.
- Evitar el uso de contraseñas grupales, compartidas o genéricas.
- Las contraseñas contienen una longitud mínima de 8 caracteres.
- Son alfanuméricas, es decir contiene números, letras y caracteres especiales.
- Evitar la reutilización de contraseñas antiguas por lo menos de doce meses atrás.
- Cambiar la contraseña periódicamente cada tres meses.

8.7. LINEAMIENTOS DE SEGURIDAD PARA LA INFRAESTRUCTURA TECNOLÓGICA

8.7.1. Mantenimiento preventivo y correctivo

- Es obligación de la oficina de sistemas garantizar el correcto funcionamiento de los equipos de cómputo, razón por la cual desde allí se concretan tiempos de mantenimiento de los equipos con los funcionarios.
- El mantenimiento se realiza de acuerdo con los procedimientos definidos en el sistema de gestión de la calidad institucional.

8.7.2. Renovación tecnológica y reposición de equipos

- La reposición de equipos consiste en la asignación de un equipo diferente al asignado inicialmente al funcionario cuando por fallas mayores éste quede inservible o cuando le sea hurtado. En este último caso el funcionario presenta la denuncia ante las autoridades competentes.
- La renovación tecnológica consiste en la asignación de un equipo nuevo por obsolescencia.

La renovación tecnológica se realizará con base en la disponibilidad presupuestal de la ESE CRIB, en el período específico.

8.7.3. Asignación de equipos de cómputo a colaboradores

- La oficina de sistemas es la encargada de administrar y asignar los equipos de cómputo, periféricos a los funcionarios que requieran estos recursos. Dicha asignación se realiza una vez la Gerencia notifica la formalización de la relación contractual, el cargo a desempeñar, el nombre del funcionario y el tipo de contrato.

- El uso del equipo de cómputo asignado es personal e intransferible, es utilizado para realizar actividades institucionales. Por lo tanto, el funcionario asume responsabilidad en forma expresa de su uso o por parte de terceros.
- El equipo asignado es entregado al funcionario con las aplicaciones y software requerido de acuerdo al cargo y el tipo de contrato.

8.7.4. Equipos de cómputo de contratistas y proveedores

Los equipos de cómputo propiedad de contratistas o proveedores que estén ubicados en las instalaciones de la ESE CRIB, deben contar con las respectivas licencias de software para las aplicaciones. En caso de incumplimiento de lo anterior, el contratista o proveedor asume las implicaciones legales del caso.

- Las labores de mantenimiento y soporte de los equipos de cómputo propiedad de contratistas o proveedores que estén ubicados en las instalaciones de la ESE CRIB, no serán atendidas por la oficina de sistemas en aquellos equipos en los cuales la relación contractual definida con el tercero lo especifique.
- El acceso a la red de datos de la ESE CRIB de los equipos de cómputo propiedad de contratistas o proveedores que estén ubicados en las instalaciones de la empresa, sólo se permite si éstos cuentan con software antivirus, antispyware licenciados, actualizados y con las actualizaciones de seguridad del sistema operativo.
- El acceso a Internet de los equipos de cómputo propiedad de contratistas o proveedores que estén ubicados en las instalaciones de la ESE CRIB, será restringido, excepto en aquellos casos que la relación contractual definida con el tercero lo especifique.

8.7.5. Equipos que ingresan a la ESE CRIB

- La ESE CRIB no asume responsabilidad alguna, sobre los equipos de cómputo que ingresen a sus instalaciones y que no hayan sido asignados por la Gerencia.

8.7.6. Instalación de Software

- No se permite la instalación de software diferente al que se le entrega con el equipo de cómputo. Es facultad exclusiva de la oficina de sistemas realizar la instalación de software en los equipos de cómputo de la ESE CRIB.
- La instalación de software adicional, es una actividad exclusiva de la oficina de sistemas, con el fin de gestionar las licencias de software propiedad de la empresa.
- Para la instalación de software especializado o adicional al que se entrega con el equipo de cómputo se hace la solicitud a través de las subgerencias administrativo y científica a la oficina de sistemas, aun cuando se trate de software con licenciamiento libre.
- No se instalan licencias propiedad del funcionario o de alguna otra entidad sin la autorización de la Gerencia.
- La copia de archivos de música y video en los equipos de la ESE CRIB está restringida.

8.8. LINEAMIENTOS DE SEGURIDAD PARA CERTIFICADO DIGITAL

8.8.1. Descripción

A partir del uso de firmas digitales la ESE CRIB busca otorgar la validez jurídica a los documentos y certificaciones que expida digitalmente.

8.8.2. Lineamientos generales

Para el trámite, solicitud, adquisición, revocación de firmas digitales a nombre de la empresa deben ser considerados los siguientes aspectos:

- Toda solicitud de adquisición, revocación o reposición de firmas digitales está a cargo de la Gerencia.
- Los colaboradores que cuentan con firma digital o certificados como representantes jurídicos deben tramitar la solicitud a través de la Gerencia, quien es el único enlace para el trámite con la entidad de certificación.

8.9. LINEAMIENTOS ADMINISTRACIÓN DE DATOS PERSONALES (HABEAS DATA)

8.9.1. Medidas de seguridad comunes

Estas medidas de seguridad aplican para todo tipo de datos: públicos, semiprivados, privados, sensibles de acuerdo con la definición establecida en la Ley Estatutaria 1581 de 2012, que se encuentren en bases de datos automatizadas o no automatizadas en la ESE CRIB.

Los responsables nombrados de las bases de datos no automatizadas serán los encargados de asegurar el cumplimiento de los controles aplicables a las mismas y descritas dentro de este manual en el numeral. Para las bases de datos automatizadas la Gerencia apoyará la implementación de los controles.

8.9.2. Gestión de documentos y soportes

Los documentos y soportes en los que se encuentran las bases de datos se determinan en el inventario de documentos y soportes.

Los responsables del tratamiento de las bases de datos son los encargados de vigilar y controlar que personas no autorizadas, no puedan acceder a los documentos y soportes con datos personales.

Los documentos y soportes deben ser clasificados según el tipo de información que contienen, ser inventariados y ser accesibles solo por el personal autorizado, salvo que las características de los mismos hagan imposible la identificación referida, en cuyo caso se dejará constancia motivada en el registro de entrada y de salida de documentos y en documentos anexos al manual.

La identificación de los documentos y soportes que contengan datos personales sensibles debe realizarse utilizando sistemas de etiquetado comprensibles y con significado que permita a los usuarios autorizados identificar su contenido y que dificulten la identificación para el resto de personas.

La salida de documentos y soportes que contengan datos personales fuera de los locales que están bajo el control del responsable del tratamiento debe ser autorizada por este último. Este precepto también es aplicable a los documentos o soportes anexados y enviados por correo electrónico.

8.9.3. Control de acceso

El personal de la ESE CRIB solamente debe acceder a aquellos datos y recursos necesarios para el desarrollo de sus labores y sobre los cuales se encuentren autorizados por el responsable del tratamiento.

La ESE CRIB se ocupa del almacenamiento de una lista actualizada de usuarios, perfiles de usuarios, y de los accesos autorizados para cada uno de ellos. En el caso de soportes informáticos, puede consistir en la asignación de contraseñas, y en el caso de documentos, en la entrega de llaves o mecanismos de apertura de dispositivos de almacenamiento donde se archive la documentación.

La modificación sobre algún dato o información, así como la concesión, alteración, inclusión o anulación de los accesos autorizados y de los usuarios recogidos en la lista actualizada mencionada en el párrafo anterior, corresponde de manera exclusiva al personal autorizado.

Cualquier personal ajeno a la ESE CRIB, que, de forma autorizada y legal, tenga acceso a los recursos protegidos, estará sometido a las mismas condiciones y tendrá las mismas obligaciones de seguridad que el personal propio.

8.9.4. Ejecución del tratamiento fuera de los locales

El almacenamiento de datos personales del responsable del tratamiento o encargado del tratamiento en dispositivos portátiles y su tratamiento fuera de los locales requiere una autorización previa por parte de la ESE CRIB, y el cumplimiento de las garantías de seguridad correspondientes al tratamiento de este tipo de datos.

8.9.5. Bases de datos temporales, copias y reproducciones

Las bases de datos temporales o copias de documentos creadas para trabajos temporales o auxiliares deben cumplir con el mismo nivel de seguridad que corresponde a las bases de datos o documentos originales. Una vez que dejan de ser necesarias, estas bases de datos temporales o copias son borradas o destruidas, impidiéndose así el acceso o recuperación de la información que contienen.

Solamente el personal autorizado para realizar copias o reproducciones de bases de datos automatizadas corresponde a la oficina de sistemas.

8.9.6. Medidas de seguridad para bases de datos no automatizadas

Los colaboradores de la ESE CRIB que tengan bajo su custodia bases de datos no automatizadas tendrán las obligaciones que a continuación se enuncian:

8.9.6.1. Almacenamiento

Garantizar el apropiado almacenamiento de la documentación física y digital en la cual reposan los datos objeto de tratamiento siguiendo los procedimientos adecuados para garantizar una correcta conservación, localización y consulta de la información, y que a su vez permitan el correcto ejercicio de los derechos de los Titulares consagrados en la ley.

8.9.6.2. Control de acceso a documentos digitales y físicos.

Usar en debida forma los dispositivos de almacenamiento digital con mecanismos apropiados y provistos por la ESE CRIB para evitar el acceso a la información en ellos contenida por personas no autorizadas.

Para los archivos físicos se deberán utilizar los muebles dispuestos por la empresa como: archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otros controles que eviten el acceso a la información por personas no autorizadas.

En ambos casos, el acceso debe estar limitado únicamente a personal autorizado.

8.9.6.3. Custodia de documentos

Deber de diligencia y custodia durante la revisión o tramitación de los mismos. En caso de tener que compartir la información que está bajo su responsabilidad con otro proceso o colaborador de la ESE CRIB el proceso solicitante deberá realizar dicha petición por medio escrito, explicando detalladamente cual será la actividad institucional a ser realizada con estos datos, verificando que se tenga autorización para ello de parte de los titulares y haciendo la debida consulta previa a gerencia para su concepto favorable, de otro modo estarían incurriendo en un mal manejo de las bases de datos.

8.9.6.4. Copia o reproducción

La copia o reproducción de la información solo podrá realizarse por los usuarios debidamente autorizados y con fines específicos y legítimos dentro de las actividades de la ESE CRIB, posterior a esto y si no es necesaria su conservación se deberá proceder a la destrucción de dicha información de manera que impida su recuperación.

8.9.6.5. Archivo de documentos

La ESE CRIB, fija los criterios y procedimientos de actuación que se deben utilizar para el archivo de documentos que contengan datos personales conforme a la Ley. Los criterios de archivo garantizan la conservación, localización y consulta de los documentos y hacen posible los derechos de consulta y reclamo de los Titulares.

Para los documentos que sean archivados se debe considerar, entre otros, criterios como el grado de utilización de los usuarios con acceso autorizado a los mismos, la actualidad de su gestión y/o tratamiento y la diferenciación entre bases de datos históricas y de administración o gestión de la empresa.

Los dispositivos de almacenamiento de documentos deben disponer de llaves u otros mecanismos que dificulte su apertura, excepto cuando las características físicas de éstos lo impidan, en cuyo caso la ESE CRIB, adoptará las medidas necesarias para impedir el acceso de personas no autorizadas.

Cuando los documentos que contienen datos personales se encuentren en proceso de revisión o tramitación y, por tanto, fuera de su medio de almacenamiento, ya sea antes o después de su archivo, la persona que se encuentre a cargo de los mismos debe custodiarlos e impedir en todo caso que personas no autorizadas puedan acceder a ellos.

Los medios de almacenamiento que contengan documentos con datos personales clasificados con nivel de seguridad sensible, deben encontrarse en áreas o locales en las que el acceso esté protegido con puertas de acceso con sistemas de apertura de llave u otros mecanismos similares. Estas áreas deben permanecer cerradas cuando no se precise el acceso a dichos documentos.

8.9.6.6. Acceso a los documentos

El acceso a los documentos ha de realizarse exclusivamente por el personal autorizado por los responsables del tratamiento, siguiendo los mecanismos y procedimientos definidos.
El procedimiento de acceso a los documentos que contienen datos clasificados como sensibles implica el registro de accesos a la documentación, la identidad de quien accede, el momento en que se produce el acceso y los documentos a los que se han accedido. El acceso a documentos con este tipo de datos se realiza por personal autorizado; si se realiza por personas no autorizadas deberá ser reportado como un incidente de seguridad.

9. ROLES Y RESPONSABILIDADES DE LOS FUNCIONARIOS

Apropiar el manual de Seguridad de la Información mediante la incorporación de buenas prácticas en el uso de la información, sistemas de información y recursos informáticos de la ESE CRIB, como una herramienta para garantizar la confidencialidad, integridad y disponibilidad de la información institucional.

De acuerdo a los siguientes indicadores

NIVEL	META	PROCESO	ACTIVIDADES PARA EL CUMPLIMIENTO DE LAS METAS ANUALES	INDICADOR / FÓRMULA
APOYO	Cumplimiento de la politica deTransparencia y acceso a la información aumentando en 30% la evaluacion del autodiagnostico	GESTION DE LA INFORMACION Y COMUNICACIONES	Ejecutar el plan de accion elaborado para el año 2021, en relación con política deTransparencia y acceso a la información, en el marco de MIPG	Porcentaje de cumplimiento en la evaluacion del autodiagnostico
APOYO	Cumplimiento de las política de Gobierno digital logrando un incremento del 20% de la linea base	GESTION DE LA INFORMACION Y COMUNICACIONES	Ejecutar el plan de accion elaborado para el año 2021, con respecto a la política de Gobierno Digital , en el marco de MIPG	Porcentaje de cumplimiento en la evaluacion del autodiagnostico
APOYO	Racionalizacion de los tramites en el SUIT	SISTEMAS	realizar la inscripcion y racionalizacionnde las tramites en el sistema SUIT	N° de tramites isncritos en el SUIT
APOYO	Cumplimiento del programa de gestion de tecnologia y mejoramiento del ambiente fisico (cambio 15 equipos tecnologicos)	GESTION DE LA INFORMACION Y COMUNICACIONES	Implementar el Programa De Renovación Tecnologica, Dotación Y Mantenimiento preventivo	No de actividades Desarrollada / No de actividades programadas x 100
APOYO	Cumplimiento de reporte y gestión de indicadores ante el comité de gestion y desempeño con seguimiento de control interno	GESTION DE LA INFORMACION Y COMUNICACIONES	Realizar seguimiento a la gestión por indicadores	Número de indicadores reportados / Total de indicadores aplicables x 100
APOYO	Cumplimiento de las acciones definidas en los mapas de riesgo por proceso y dar cumplimiento a el plan de tratamiento y riesgos de seguridad informatica	GESTION DE LA INFORMACION Y COMUNICACIONES	Implementar las acciones definidas para la administración de los riesgos priorizados	No de actividades Desarrollada / No de actividades programadas x 100
APOYO	Actualizar procedimientos planes y programas aprobados e implementados (PETI, Manual seguridad de la informacion y plan de tratamiento y riesgos de seguridad informatica)	GESTION DE LA INFORMACION Y COMUNICACIONES	Documentacion, aprobacion e implementacion de procedimientos del area	Procedimientos entregados /Total de procedimientos del area *100

9.2. PROCESOS

3.2.1. GESTIÓN DEL TALENTO HUMANO

Velar por el cumplimiento del Reglamento Interno de Trabajo, en los casos que aplique con respecto a los lineamientos de seguridad de la información, enunciados en el presente manual.

3.2.2. GESTIÓN DE LA INFORMACIÓN

- Implementar las herramientas y controles respectivos para facilitar el cumplimiento de los lineamientos de seguridad de la información, enunciados en el presente manual
- Garantizar la operación permanente de los recursos informáticos y sistemas de información. Fortalecer la cultura digital en la ESE CRIB.

8. 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 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. 891 800 082-7

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

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	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-003	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	ORIGINAL	Oficina de Calidad
PL-GRT-003	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	COPIA CONTROLADA	Sistema de Consulta MIPG