PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

HOSPITAL ESPECIAL DE CUBARÁ ESE

ENERO 2025

HOSPITAL ESPECIAL
DE CUBARÁ
Empresa Social del Estado
NIT. 826.002.304-1

CONTENIDO

INTRODUCCION

La ESE HOSPITAL ESPECIAL DE CUBARA, identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la entidad, razón por la cual es necesario que la ESE establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Por tal razón se adopta el Modelo de seguridad y privacidad de la información MSPI bajo los lineamientos del Ministerio de las TIC's a través de la estrategia de gobierno en línea, para generar este Plan, es necesario realizar un diagnóstico del estado actual en materia de seguridad de la información, así mismo, identificar las necesidades de la ESE en este ámbito.

Una vez realizado este diagnóstico, se identifican las debilidades, fortalezas y oportunidades de mejora, generando una política de seguridad. El presente documento, expone los lineamientos planteados para implementar las mejoras prácticas de seguridad informática en la ESE, con el fin de optimizar la disponibilidad, la integridad, la confidencialidad, privacidad, entre otros principios relevantes, teniendo en cuenta la infraestructura y limitaciones actuales.

1. QUIENES SOMOS

Somos una Empresa Social del Estado, que presta servicios de salud de baja y mediana complejidad a la población colona e indígena del municipio de Cubará y zona de influencia, que busca brindar servicios integrales en salud, basados en la educación preventiva, mejorando la calidad de vida, orientada en la atención humanizada con enfoque diferencial. Su gestión se basa en el desarrollo comunitario e intercultural y la promoción de su talento humano, mediante la innovación en el uso de tecnologías de la información y la comunicación e implementación de herramientas administrativas.

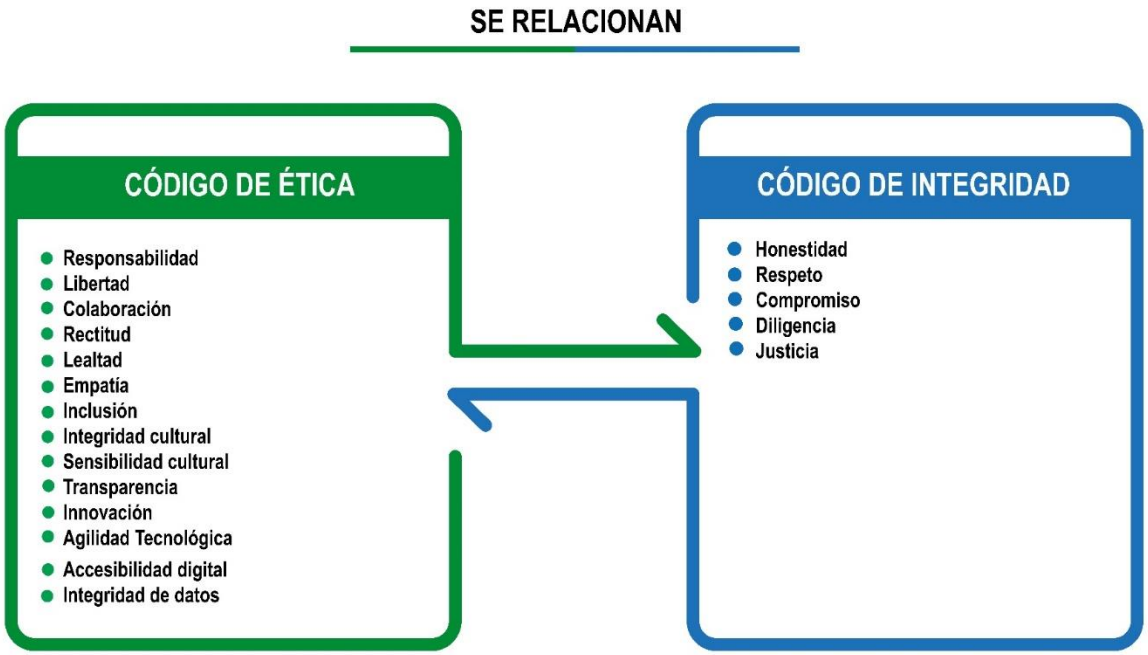
2. MISIÓN

El Hospital Especial de Cubará se compromete a proporcionar servicios de salud integrados y de alta calidad, destacando por la implementación de soluciones de telemedicina que aseguren el acceso y eficiencia en la atención médica para nuestras diversas comunidades, incluidas las colonas, indígenas y NARP. Nos enfocamos en combinar la tecnología avanzada con un profundo respeto y entendimiento de la diversidad cultural, ofreciendo un enfoque de atención médica personalizado y éticamente enriquecido. A través de nuestra gestión, buscamos ser líderes en innovación y en la prestación de cuidados de salud con un modelo que valora y respeta las variadas prácticas y tradiciones de todas las comunidades que servimos.

3. VISIÓN

Para 2027, el Hospital Especial de Cubará será un referente en la aplicación de la telemedicina y en la integración de un enfoque intercultural en la prestación de servicios de salud. Nos destacaremos por nuestro modelo innovador que combina tecnología de punta con un profundo compromiso hacia la inclusión y el respeto de la diversidad étnica y cultural. Nuestro hospital será sinónimo de excelencia, accesibilidad y adaptabilidad, donde el personal capacitado y dedicado utiliza las mejores herramientas tecnológicas para ofrecer cuidados de salud excepcionales, humanizados y adaptados a las necesidades específicas de cada comunidad. Así, garantizamos una atención médica eficiente y respetuosa, estableciendo nuevos estándares para el cuidado de la salud en un entorno multicultural

4. **VALORES INSTITUCIONALES**



CÓDIGO DE ÉTICA

- **Responsabilidad:** Nos comprometemos con la integridad y la transparencia en cada acción que emprendemos. La responsabilidad es fundamental para cultivar la confianza dentro y fuera de nuestra institución y asegura que cada decisión y acción refleje nuestro compromiso con la excelencia en la atención médica y el bienestar comunitario.
- **Libertad:** Promovemos un ambiente donde todos tienen la libertad de expresar sus opiniones, tomar decisiones informadas y participar activamente en su cuidado y en la mejora continua de nuestros servicios. La libertad en nuestro hospital también implica responsabilidad personal y colectiva para garantizar que nuestras acciones beneficien a todos.
- **Colaboración:** Fomentamos una cultura de colaboración interna y externa, trabajando juntos hacia metas comunes. La colaboración en nuestro hospital se traduce en compartir conocimientos, prácticas y recursos de manera efectiva, no solo entre los empleados, sino también con pacientes y comunidades, para mejorar los resultados en salud.
- **Rectitud:** Nos adherimos firmemente a principios de equidad y justicia en todas nuestras operaciones. La rectitud en nuestro hospital significa actuar siempre con integridad, asegurando que

todas las decisiones y procedimientos sean justos y correctos, especialmente cuando enfrentamos dilemas éticos o desafíos operativos.

- **Lealtad:** Mantenemos un compromiso inquebrantable con nuestros principios y nuestra comunidad. La lealtad en nuestro contexto se refiere a mantenerse fiel a nuestros compromisos y valores, apoyando a nuestros pacientes, equipo y comunidad incluso en momentos de adversidad, garantizando una relación basada en la confianza y el respeto mutuo.
- **Empatía:** Promovemos activamente la empatía como un pilar de nuestra práctica médica y administrativa. Este valor nos impulsa a ponernos en el lugar de nuestros pacientes y sus familias, entendiendo sus contextos únicos y respondiendo a sus necesidades emocionales y culturales de manera comprensiva y respetuosa.
- **Inclusión:** Nos comprometemos a garantizar que todos los servicios y espacios del hospital sean accesibles e inclusivos para todos los individuos, independientemente de su origen étnico, lingüístico, cultural, religioso o de cualquier otra índole. La inclusión en nuestra institución significa adaptar nuestros servicios para reflejar y respetar la diversidad de la comunidad que servimos.
- **Integridad Cultural:** Valoramos y respetamos las diversas prácticas culturales y las perspectivas de salud de nuestras comunidades. La integridad cultural implica un compromiso para integrar prácticas médicas culturalmente apropiadas que sean respetuosas y efectivas para los diferentes grupos étnicos y culturales atendidos.
- **Sensibilidad Cultural**: Nos esforzamos por educar y capacitar a nuestro personal en sensibilidad cultural para mejorar la interacción y la comunicación con pacientes de diversas culturas. Este valor garantiza que nuestros servicios sean entregados de manera que sean culturalmente comprensibles y relevantes, fomentando una mayor efectividad en el tratamiento y cuidado.
- **Transparencia**: Aseguramos una comunicación abierta y honesta tanto dentro de nuestra organización como con nuestros pacientes y la comunidad. La transparencia no solo se refiere a la claridad en nuestras operaciones y decisiones, sino también a ser abiertos sobre nuestras capacidades y siempre buscar la mejora continua.
- **Innovación:** Fomentamos una cultura de innovación continua para mejorar la calidad y la eficiencia de nuestros servicios de salud. Este valor impulsa la adopción de nuevas tecnologías y enfoques, permitiéndonos ofrecer soluciones avanzadas y personalizadas de atención médica que responden a las necesidades cambiantes de nuestra comunidad
- **Agilidad Tecnológica:** Nos comprometemos a mantener una infraestructura tecnológica ágil que nos permita adaptarnos rápidamente a los avances en el campo de la medicina y la información. La agilidad tecnológica asegura que podemos responder eficazmente a las emergencias, mejorar la comunicación con los pacientes y optimizar la gestión hospitalaria.

- **Accesibilidad Digital:** Promovemos la accesibilidad digital para garantizar que todos nuestros pacientes y su comunidad puedan beneficiarse de nuestras tecnologías. Esto incluye proporcionar plataformas y herramientas que sean fácilmente utilizables por personas de todas las edades y habilidades, reduciendo las barreras digitales y facilitando el acceso a la información de salud.
- **Integridad de Datos:** Nos comprometemos a proteger la integridad y la confidencialidad de los datos de los pacientes. Este valor es fundamental en un entorno en el que el uso de TICs es intensivo, asegurando que toda la información médica y personal sea manejada con los más altos estándares de seguridad y ética.

5. **CODIGO DE INTEGRIDAD**

- **Honestidad:** Actúa siempre con fundamento en la verdad, cumpliendo los deberes con transparencia y rectitud, y siempre favoreciendo el interés general.
- **Respeto:** Reconocer, valorar y tratar de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición
- **Compromiso**: Ser consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar.
- **Diligencia:** Cumplir con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud, destreza y eficiencia, para así optimizar el uso de los recursos del Estado.
- **Justicia**: Actuar con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.

6. OBJETIVOS

6.1 Objetivo General

Desarrollar el Plan de Seguridad y Privacidad de la Información para el Hospital Especial de Cubara ESE.

6.2 Objetivos Especificos

- Establecer los lineamientos generales del manejo de la información para el Hospital Especial de Cubara ESE.
- Generar el Modelo de Seguridad y Privacidad de la Información.
- Implementar el Plan de Acción.

7. MARCO LEGAL

El presente documento se realizó basado en la norma ISO – IEC 27001:2013 Sistema de Gestión de la Seguridad de la Información, apoyados en el Plan de Seguridad y Privacidad de la información del Hospital Especial de Cubara ESE.

8. SEGURIDAD DE LA INFORMACION

La seguridad de la información es definida por la norma ISO/IEC 27001 como: "La Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad", este es un concepto que no debe confundirse con la seguridad informática, la cual únicamente se encarga de la seguridad en medios informáticos, teniendo en cuenta que la información puede estar contenida de otras maneras.

Más específicamente, la ISO define integridad, disponibilidad y confidencialidad de la siguiente manera:

- Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos de información. [NTC 5411-1:2006].
- Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [NTC 5411-1:2006].
- Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados. [NTC5411- 1:2006].

9. LINEAMIENTOS GENERALES DEL MANEJO DE LA INFORMACION

A continuación, se presenta un diagnóstico del estado actual del manejo de la información en el Hospital Especial de Cubara ESE.

9.1 Gestion de archivos

Con el fin de garantizar la administración y el control sobre los activos de la ESE, cada dependencia debe mantener el inventario actualizado, identificando al propietario de cada elemento, quien debe asegurar la información y los activos asociados con su proceso. Este inventario debe actualizarse siempre que se realice algún desplazamiento de cualquier activo, el funcionario responsable deberá mediante un oficio, informar a almacén y al area de sistemas y estadística del movimiento que se va a realizar, incluyendo detalladamente los equipos y sus respectivos seriales.

Cuando se presente alguna falla o daño en cualquiera de los activos de información, se debe reportar inmediatamente al area de sistemas, quien es el único responsable de hacer el diagnóstico, la reparación o reemplazo del elemento afectado.

Todos los activos de información son propiedad exclusiva del Hospital Especial de Cubara ESE, de igual manera, es el dueño de la propiedad intelectual desarrollada por los funcionarios y contratistas derivadas del objeto y cumplimiento de funciones y/o de las tareas asignadas. Los administradores de estos activos de información son funcionarios, contratistas o colaboradores directos y autorizados de la ESE.

Todo cambio, creación, eliminación o modificación de programas, aplicativos, formatos y reportes que afecte los recursos informáticos, deben ser solicitados formalmente por los usuarios a las respectivas Subdirecciones con el fin de que los administradores de los sistemas ejecuten dichas solicitudes.

9.2 Acceso a la informacion

Cada dependencia de la ESE, debe establecer políticas de acceso a los sistemas de información con el fin de evitar los riesgos asociados al acceso no debido de los mismos.

En caso de que personas o Entidades externas requieran acceder a información específica y confidencial, se debe cumplir con los protocolos legales establecidos para la transmisión de la información que tiene establecida la ESE.

9.3 Uso de usuarios y contraseñas

La oficina de informática y estadística es la encargada de administrar y generar las contraseñas para el acceso al sistema de información Rocky, a las redes de WIFI distribuidas en las instalaciones de la ESE, así como la gestión de las contraseñas de los usuarios de los equipos de comunicaciones y las claves iniciales de las cuentas de los correos institucionales.

Cada funcionario o contratista deberá tener una clave personal e intransferible de acceso que le permitirá ingresar de forma exclusiva al equipo de cómputo asignado para su labor, así como a las bases de datos y a los aplicativos a los que está autorizado.

Cabe resaltar que cada funcionario o contratista es responsable del uso de su clave de acceso debiéndola mantener en secreto, ya que cualquier modificación no autorizada de la información, daño o acceso irregular que ocurra y se detecte, es responsabilidad directa del funcionario, pudiendo hacerse acreedor a las sanciones de tipo legal y disciplinario que esto conlleve.

En caso de que el personal requiera algún permiso especial o algún cambio en la configuración de su usuario en Rocky, estos cambios deben ser autorizados por las Subdirecciones y solicitados por escrito o vía correo electrónico, una vez autorizado, serán ejecutados directamente por el area de sistemas

9.4 Uso de Internet/Intranet de la ESE

El acceso al servicio de Internet/Intranet es utilizado por funcionarios, contratistas o practicantes, cabe resaltar que no hay ningún tipo de bloqueo de páginas por parte del area de sistemas, comprometiendo a los funcionarios a utilizar este activo con responsabilidad y ética laboral. Todos los funcionarios, contratistas y practicantes con autorización al uso y acceso a estos servicios deben:

- Utilizar este servicio exclusivamente para fines laborales.
- Conservar normas de respeto, confidencialidad y criterio ético
- Descargar documentos o archivo tomando las medidas de precaución es responsabilidad de cada usuario con el fin de evitar el acceso de virus en las redes y equipos informáticos, en caso de necesitar asesoría en este proceso, se debe hacer el requerimiento a la oficina de Informática y estadística quien debe prestar apoyo.
- Está Prohibido él envió, descarga y/o visualización de páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor y/o que atenten contra la buena imagen de la ESE o su Personal.

9.5 Uso de dispositivos de almacenamiento externo

La ESE no restringe el uso de dispositivos de almacenamiento externo a sus funcionarios, teniendo en cuenta su utilidad para transportar y resguardar información, incluso ha facilitado la adquisición de estos dispositivos para su utilización institucional. Sin embargo, es responsabilidad de cada funcionario la correcta utilización de estos medios.

9.6 Seguridad de la informacion

Los trabajadores de planta y contratistas son responsables de la información que manejan y deben garantizar su custodia, integridad, confidencialidad, disponibilidad y confiabilidad, evitando pérdidas, accesos no autorizados, exposición, modificación y/o utilización indebida de la misma, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica. El software adquirido y desarrollado por funcionarios o colaboradores de la ESE, es exclusivo para las operaciones de la Institución, estado prohibida su utilización, copia o venta para fines ajenos a la ESE.

9.7 Uso de impresoras y escaneres

La utilización de las impresoras debe estar basada en la política de cero papel adoptada por la institución, primando la impresión a doble cara, la utilización de papel reciclable y los correos electrónicos con el fin de reducir la cantidad de papel gastado.

Cabe resaltar que la utilización de las mismas es exclusiva para asuntos laborales, estando prohibido la impresión de documentos personales con los equipos de la ESE. Cualquier fallo que se presente, debe ser informado al area de sistemas, la cual realizará las reparaciones correspondientes y, en caso de presentarse malas utilizaciones por parte del personal responsable, se haran los reportes correspondientes.

9.8 Seguridad fisica y el entorno

Las áreas designadas para el almacenamiento de los activos de información (Servidores, Routers, Switches, UPS y cableado estructurado), son áreas restringidas cuyo acceso está controlado por el personal del area de sistemas de la ESE.

9.9 Control de virus informaticos

El Hospital Especial de Cubara ESE, cuenta con un Router Mikrotik, quien tiene configurado un cortafuegos el cual previene ataques informáticos desde agentes externos a la intranet. En cuanto a los virus de computadoras, los funcionarios deben evitar al máximo la utilización de medios extraíbles de dudosa reputación que puedan infectar los equipos o la infraestructura de red, esto también aplica a los correos electrónicos y mensajes que se reciben de la internet y que pueden contener software malicioso, la ESE cuenta con licencia de antivirus Bitdefender para todos los equipos de computo y esta licencia se renueva anualmente para una proteccion constante.

9.10 Almacenamiento y respaldo de informacion

El Hospital Especial de Cubara ESE, cuenta con dos copias de seguridad en servidores diferentes del sistema de información Rocky una almacenada localmente y otra en la nube en el servicio de google drive,

esta contiene las historias clínicas, información de facturación y financiera de la ESE. Las copias de seguridad de la información local de cada funcionario, es responsabilidad de cada cual, solicitando el apoyo, si es necesario, del area de sistemas.

10. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones- MINTIC, publica la cartilla del Modelo de Seguridad y Privacidad de la Información, este documento suministra requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información – MSPI, con el fin de servir como guía para la implementación del Plan de Seguridad y Privacidad de la Información en las Entidades Públicas.

Esta implementación está directamente relacionada con las necesidades actuales, los requisitos de seguridad, procesos y tamaño de la infraestructura de la ESE, con el fin de promover y preservar la confidencialidad, integridad y disponibilidad de los activos de información.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, contribuir a mejorar los procesos de intercambio de información pública, dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en las entidades y Optimizar la gestión de la seguridad de la información al interior de las entidades, entre otras prácticas.

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que la ESE pueda gestionar adecuadamente la seguridad y privacidad de sus activos de información.

Estas fases, contienen objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible. En la siguiente figura, se presenta el macro modelo de la descripción del ciclo de operación planteado por el MinTic.

11. PLAN DE ACCION

COMPONENTE	ACTIVIDADES	RESPONSABLE	META	FECHA
DIAGNOSTICO	Determinar el estado actual de la gestión de seguridad y privacidad de la información	Area de sistemas	Diagnostico del estado actual	2025
PLANIFICACION	Actualizar el inventario de activos de información de la ESE	Area de sistemas	Cuadro de inventario actualizado	Semestral
	Monitorear las contraseñas de acceso a los sistemas con el personal activo de la ESE	Area de sistemas	Contraseñas actualizadas	Febrero 24
	Inhabilitar el acceso a los usuarios que ya no pertenecen a la ESE	Area de sistemas	Nueva tabla de usuarios con acceso al sistema	Cada 2 meses
	Monitorear el consumo del ancho de banda de la red institucional por	Area de sistemas	Control sistemático a través del Router Mikrotik	Mensual

	parte de los funcionarios			
	Realizar mantenimiento periódico a las impresoras de la ESE	Area de sistemas	Correcto funcionamiento de las Impresoras	Anualmente y de acuerdo al cronograma de mantenimiento
	Realizar monitoreo permanente del estado de la sala de cómputo	Area de sistemas y Area de mantenimiento	Correcto funcionamiento de los equipos de red	Permanente
	Implementar una herramienta informática para automatizar las copias de seguridad en un servidor nuevo	Area de sistemas	Copias de Seguridad realizadas	Febrero 28
IMPLEMENTACION	Implementación del Plan de Tratamiento de Riesgos	Area de sistemas	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Anual
EVALUACION Y DESEMPEÑO	Realizar la revisión y el seguimiento de la ejecución del plan de Tratamiento de Riesgos	Area de sistemas	Informe de avances	Anual

MEJORA CONTINUA	Evaluación semestral de oportunidades de mejoramiento	Area de sistemas	Informe de oportunidades de mejora	Semestral

12. EVALUACIÓN Y SEGUIMIENTO

Corresponderá a la administración y al comité de gestión y desempeño realizar el respectivo monitoreo de las acciones realizadas de manera mensual, con el fin de garantizar el cumplimiento durante su vigencia 2025.

- **Indicador de Cumplimiento:** Este indicador tiene como propósito evaluar de manera mensual la implementación efectiva de las actividades diseñadas en el marco del plan de bienestar, estímulos e incentivos para los trabajadores, asegurando que cumplan con los objetivos establecidos y que aporten al bienestar integral del personal.

$$Porcentaje\ de\ Ejecución = \left(\frac{Actividades\ ejecutadas}{Actividades\ programadas}\right) * 100$$

13. METODOLOGIA PARA LA APROBACIÓN

La metodología de aprobación de los planes institucionales, según el **Decreto 612 de 2018**, debe articularse al funcionamiento del **Comité Institucional de Gestión y Desempeño (CIGD)**, como instancia clave de dirección estratégica. Este comité tiene la responsabilidad de revisar, validar y aprobar los planes institucionales antes de su implementación, asegurando su alineación con los objetivos estratégicos y la normatividad vigente. A continuación, se detalla una metodología para la aprobación:

Identificación y preparación de los planes institucionales

- Las áreas responsables elaboran los planes institucionales con base en los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG) y las políticas definidas.

Revisión preliminar

- Antes de presentar los planes al CIGD, estos son revisados por los equipos técnicos o las instancias internas de cada área para asegurar que cumplen con los requisitos normativos

Socialización con el Comité Institucional de Gestión y Desempeño

- Las áreas responsables presentan los planes al CIGD mediante sesiones programadas.

Ajustes y retroalimentación

- Si el CIGD encuentra inconsistencias o áreas de mejora, devuelve los planes a las áreas responsables con recomendaciones claras.
- Las áreas responsables realizan los ajustes necesarios y vuelven a presentar los planes.

Aprobación

- Una vez que el CIGD considera que el plan cumple con todos los requisitos, se emite un acta de aprobación formal, que incluye los compromisos adquiridos por las áreas responsables.

Comunicación y oficialización

- Los planes aprobados son comunicados a toda la institución mediante los canales definidos.

Seguimiento y evaluación

- El CIGD programa seguimiento mensual al cumplimiento del plan establecido.
- Se monitorean los avances con base en los indicadores definidos y se toman decisiones oportunas para garantizar su implementación efectiva.

EDWIN GIOVANNI QUINTERO TELLEZ
Gerente Hospital Especial de Cubará
C.C 79.824.210

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Arnold Steven de la Rosa Machado Ingeniero de sistemas	Edwin Giovanni Quintero Téllez Gerente	Comité de gestión y desempeño