PLAN DE TRATAMIENTO DE RIESGOS 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

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.

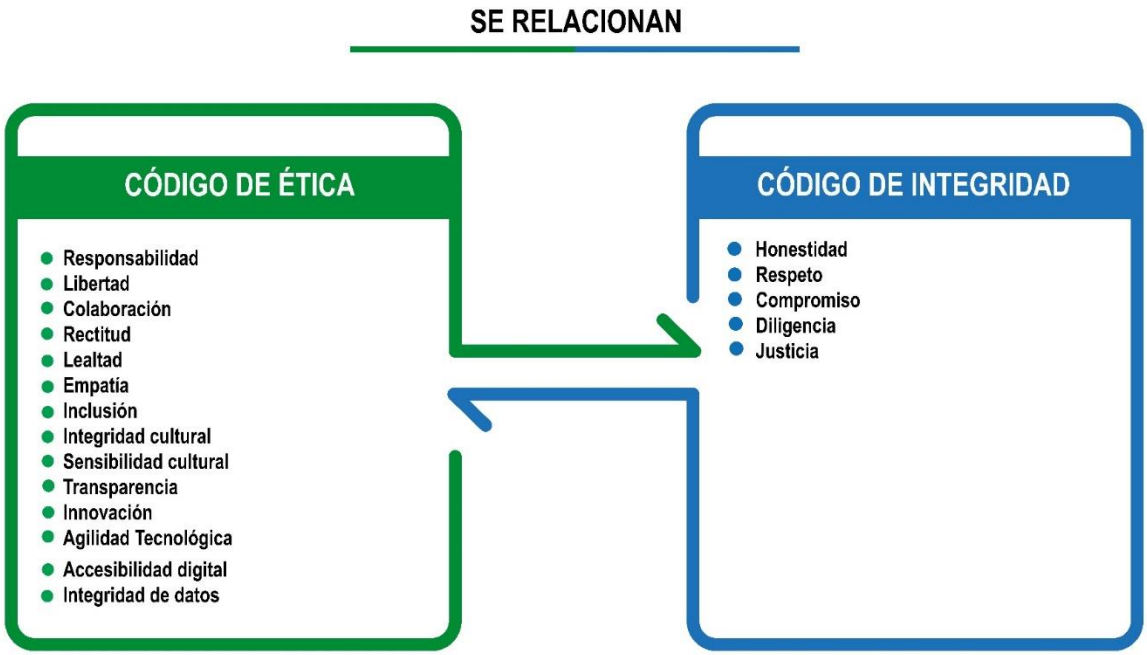
2. **MISIÓN**

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



4.1. 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.

4.2. 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.

5. INTRODUCCION

Teniendo en cuenta que la actual revolución digital genera nuevos riesgos y amenazas para garantizar la confidencialidad, integridad y disponibilidad de la información generada por los procesos de la E.S.E Hospital Especial de Cubará, se hace necesaria la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, que garantice la protección de la información ante la ocurrencia de eventos que pongan en peligro su integridad.

Para la realización de este Plan, La E.S.E acogió la Matriz del Mapa de Riesgos de Seguridad Digital proporcionada por el Ministerio de las Tics, realizando la identificación de los activos de información junto con sus posibles amenazas, vulnerabilidades, proporcionando controles para el manejo de los mismos, basados en el impacto de la probabilidad de ocurrencia

6. OBJETIVOS

6.1 Objetivo General

Desarrollar el Plan de gestión de Seguridad y Privacidad de la Información que permita minimizar los riesgos de perdida de activos de la información en la E.S.E Hospital Especial de Cubará

6.2 Objetivos Específicos

- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana en materia de seguridad de la información.
- Priorizar los riesgos según los criterios establecidos en el Mapa de Riesgos de Seguridad Digital.
- Realizar la identificación de los principales Activos de Información presentes en la E.S.E.
- Identificar las principales amenazas que afectan a los activos.
- Definir el impacto de la ocurrencia de las amenazas.
- Establecer controles, responsables y periodos de ejecución de las acciones de mitigación de las amenazas de los activos de la información.
- Medir a través de indicadores, el manejo de los riesgos establecidos.

7. ALCANCE Y LIMITACIONES

7.1 Alcance

La E.S.E Hospital Especial de Cubará, con el propósito de realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la Información, debe lograr el compromiso para emprender la implementación de este plan en todos los procesos institucionales que se generen, mediante el uso de buenas prácticas y lineamientos nacionales, y locales, con el propósito que ello contribuya a la toma de decisiones y prevenir incidentes que puedan comprometer los activos de información, designando roles de liderazgo que apoyen y asesoren la implementación del Plan, capacitando al personal de la Entidad para su correcta ejecución.

7.2 Limitaciones

Crear el rubro de presupuesto necesario para apoyar la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la E.S.E Hospital Especial de Cubará

8. EJECUCION DEL PLAN

8.1 Importancia de la gestión de riesgos

La evolución en el manejo de la información, impulsada por el creciente uso de procesos digitales, ha transformado muchos procedimientos que anteriormente no requerían el uso de recursos tecnológicos. Por ello, se hace prioritario salvar, proteger y custodiar los activos de la información de la E.S.E Hospital Especial de Cubará.

Siguiendo los lineamientos trazados por el Gobierno Nacional en cumplimiento de la ley de transparencia 1712 del 2014 y Gobierno en Línea, que vienen impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información, con iniciativas como el concurso Máxima Velocidad, creado por el Ministerio de las TICS, la E.S.E da cumplimiento al Decreto 1078 de 2015, por medio del cual "Se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

Para la realización del plan de tratamiento de riesgos de seguridad y privacidad de la información se utilizó la Guía 7 Gestión de riesgos y la Guía 8 Controles de seguridad de la información.

8.2 Definición Gestión De Riesgos

Según la Organización Internacional de Normalización (ISO), la gestión del riesgo se define como: "Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. (NTC ISO 31000:2011)". Según la Cartilla de Administración de Riesgos del DAFP, la administración del riesgo se divide en los siguientes procesos:

PROCESO PARA LA ADMINISTRACIÓN DEL RIESGO·

8.3 Identificación del riesgo

Para la identificación de los riesgos, el Ministerio de las TIC, en su guía número 7 de Seguridad y Privacidad de la Información, establece la siguiente lista de clasificación de riesgos:

- **Riesgo Estratégico:** Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta Gerencia.

- **Riesgos de Imagen:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
- **Riesgos Operativos:** Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.
- **Riesgos financieros:** Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
- **Riesgos de Cumplimiento:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad de acuerdo a su misión.
- **Riesgos de Tecnología:** Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

8.4 Identificación de los activos de información

El Mapa de Riesgos de Seguridad Digital, proporcionado por el Ministerio de Las TIC, define los siguientes tipos de Activo de Información:

- **Información y Datos de la Entidad:** Datos e información almacenada o procesada física o electrónicamente, tales como: Bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
- **Sistemas de información y aplicaciones de software**: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
- **Dispositivos de tecnologías de información-hardware:** Equipos de Cómputo que por su criticidad son considerados activos de información, no solo activos fijos.
- **Soporte para el saneamiento de información:** Equipo para almacenamiento de información como: USB, Discos Duros, CDs, SAND, NAS.
- **Servicios:** Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e intranet.

Teniendo en cuenta los criterios mencionados, se identifican los siguientes activos de información:

Tipo de activo de información	Activo de información
Servicios	Canal de datos, Conexión a internet, Servidor de almacenamiento
Información y datos de la entidad	Documentación de las diferentes áreas del hospital y bases de datos de los sistemas: Rocky, Genesis, Suite de Google
Sistemas de información y aplicaciones de software	Rocky, Genesis, Office, Softros LAN Messenger, PDF24, Anydesk, Adobe Reader, Software de equipos de laboratorio.
Dispositivos de tecnologías de información-hardware	Servidor de archivos, servidor Rocky, servidor financiero
Soporte para el saneamiento de información	Discos duros externos, USB, CDs

8.5 Identificación de amenazas

Una amenaza tiene el potencial de causar daños a la información, los procesos y los sistemas y, por lo tanto, a la E.S.E Hospital Especial de Cubará. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas). A continuación, se describen las amenazas identificadas:

Activo de información	Propiedad afectada	Amenazas
Canal de datos, Conexión a internet, Servidor de almacenamiento	Interrupción en la comunicación entre sistemas	Perdida de datos, acceso no autorizado, Ataques cibernéticos
Documentación de las diferentes áreas del hospital y bases de	Archivos y bases de datos de la institución	Perdida de datos, ataques de ransomware, filtración y acceso no autorizado

datos de los sistemas: Rocky, Genesis, Suite de Google		
Rocky, Genesis, Office, Softros LAN Messenger, PDF24, Anydesk, Adobe Reader, Software de equipos de laboratorio.	Software necesario en todos los procesos de la institución	Ataques cibernéticos, Virus informáticos, acceso no autorizado
Servidor de archivos, servidor Rocky, servidor financiero	No acceso a las bases de datos	Ataques cibernéticos, virus
Discos duros externos, USB, CDs	Perdida de datos	Virus, acceso no autorizado

8.6 Identificación de las vulnerabilidades

A continuación, se presentan las vulnerabilidades que podrían causar la materialización de las amenazas para cada activo de información:

Activo de información	Amenazas	Vulnerabilidades
Canal de datos, Conexión a internet, Servidor de almacenamiento	Perdida de datos, acceso no autorizado, Ataques cibernéticos	Falta de copias de seguridad, errores humanos, fallas de hardware, falta de medidas de seguridad,
Documentación de las diferentes áreas del hospital y bases de datos de los sistemas: Rocky, Genesis, Suite de Google	Perdida de datos, ataques de ransomware, filtración y acceso no autorizado	Falta de copias de seguridad, errores humanos, fallas de hardware, falta de medidas de seguridad
Rocky, Genesis, Office, Softros LAN Messenger, PDF24, Anydesk, Adobe Reader, Software de equipos de laboratorio.	Ataques cibernéticos, Virus informáticos, acceso no autorizado	Falta de firewalls y antivirus, software desactualizado, errores humanos
Servidor de archivos, servidor Rocky, servidor financiero	Ataques cibernéticos, virus	Falta de firewalls y antivirus, software desactualizado, falta de

		mantenimiento, falta de controles de acceso.
Discos duros externos, USB, CDs	Virus, acceso no autorizado	Falta de firewalls y antivirus y restricciones de acceso

8.7 Análisis de riesgo inherente

Para cuantificar y clasificar el riesgo inherente, se toma como base: La tabla de probabilidad, la tabla de impacto y la matriz de calificación:

Tabla de Probabilidad: La probabilidad es la medida para estimar la ocurrencia del riesgo y se mide con criterios de frecuencia.

TABLA DE PROBABILIDAD			
NIVEL	DESCRIPTOR	DESCRIPCIÓN (FACTIBILIDAD)	FRECUENCIA
1	RARO	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años.
2	IMPROBABLE	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
3	POSIBLE	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
4	PROBABLE	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de 1 vez en el último año.
5	CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Tabla de impacto: Son las consecuencias potenciales que genera el hecho que se materialice en el riesgo

TABLA DE IMPACTO			
TIPO	**NIVEL**	**DESCRIPTOR**	**DESCRIPCIÓN** En caso que el riesgo se materialice el impacto u afectación sería.....
CONFIDENCIALIDAD EN LA INFORMACIÓN	1	INSIGNIFICANTE	Se afecta a una persona en particular.
	2	MENOR	Se afecta a un grupo de trabajo interno del proceso.
	3	MODERADO	Se afecta a todo el proceso.
	4	MAYOR	La afectación se da a nivel estratégico.
	5	CATASTRÓFICO	La afectación se da a nivel institucional.
CREDIBILIDAD O IMAGEN	1	INSIGNIFICANTE	Se afecta al grupo de funcionarios y contratistas del proceso.
	2	MENOR	Se afecta a todos los funcionarios y contratistas de la entidad.
	3	MODERADO	Se afecta a los usuarios de la Sede Central de la entidad.
	4	MAYOR	Se afecta a los usuarios de las Direcciones Territoriales.
	5	CATASTRÓFICO	Se afecta a los usuarios de la Sede Central y de las Direcciones Territoriales.
LEGAL	1	INSIGNIFICANTE	Se producen multas para la entidad.
	2	MENOR	Se producen demandas para la entidad.
	3	MODERADO	Se producen investigaciones disciplinarias.
	4	MAYOR	Se producen investigaciones fiscales.
	5	CATASTRÓFICO	Se producen intervenciones y o sanciones para la entidad por parte de un Ente de contro u otro Ente regulador.
OPERATIVO	1	INSIGNIFICANTE	Se tendrían que realizar ajustes a una actividad concreta del proceso.
	2	MENOR	Se tendrían que realizar ajustes en los procedimientos del proceso.
	3	MODERADO	Se tendrían que realizar ajustes en la interacción de procesos.
	4	MAYOR	Se presentarían intermitencias o dificultades en la operación del proceso
	5	CATASTRÓFICO	Se presentaría paro o no operación del proceso.

Matriz de Calificación, Evaluación y respuesta a los riesgos: Representa la Zona en la que se encuentra el riesgo a la que se enfrenta inicialmente un proceso o la Entidad en ausencia de controles.

CONCEPTO		IMPACTO				
		1	2	3	4	5
PROBABILIDAD		INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
	VALOR	1	2	3	4	5
RARA VEZ (1)	1	11	12	13	14	15
IMPROBABLE (2)	2	21	22	23	24	25
POSIBLE (3)	3	31	32	33	34	35
PROBABLE (4)	4	41	42	43	44	45
CASI SEGURO (5)	5	51	52	53	54	55

ZONA DE RIESGO BAJA
ZONA DE RIESGO MODERADA
ZONA DE RIESGO ALTA
ZONA DE RIESGO EXTREMA

Basados en las figuras presentadas anteriormente, se presenta el análisis del riesgo inherente para E.S.E Hospital Especial de Cubará:

Activo de información	Probabilidad	Impacto	Zona de riesgo
Canal de datos, Conexión a internet, Servidor de almacenamiento	Posible	Mayor	Alta

Documentación de las diferentes áreas del hospital y bases de datos de los sistemas: Rocky, Genesis, Suite de Google	Posible	Mayor	Extrema
Rocky, Genesis, Office, Softros LAN Messenger, PDF24, Anydesk, Adobe Reader, Software de equipos de laboratorio.	Casi seguro	Mayor	Alta
Servidor de archivos, servidor Rocky, servidor financiero	Posible	Mayor	Extrema
Discos duros externos, USB, CDs	Casi seguro	Moderado	Moderada

9. IDENTIFICACION DE CONTROLES

En esta etapa, se establecieron los controles que se realizan para mitigar el riesgo inherente, teniendo como referencia las opciones del manejo del riesgo, la descripción del mismo y el responsable de ejecutar su control:

Activo de información	Opciones de manejo del riesgo	Descripción del control	Responsable
Canal de datos, Conexión a internet, Servidor de almacenamiento	Reducir el riesgo	Monitorear el canal de datos de la entidad	Área de sistemas
Documentación de las diferentes áreas del hospital y bases de datos de los sistemas: Rocky, Genesis, Suite de Google	Reducir el riesgo	Se cuenta con un plan de seguridad de la información	Área de sistemas
Rocky, Genesis, Office, Softros LAN Messenger, PDF24, Anydesk, Adobe Reader, Software de equipos de laboratorio.	Reducir el riesgo	Monitorear los distintos softwares utilizados garantizando actualizaciones y soporte	Área de sistemas
Servidor de archivos, servidor Rocky, servidor financiero	Reducir el riesgo	Monitoreo de los servidores garantizando su correcto funcionamiento y continuidad, aplicar controles de acceso a las consolas de administración	Área de sistemas
Discos duros externos, USB, CDs	Reducir el riesgo	Restricciones de conexiones de dispositivos externos	Área de sistemas

10. PLAN DE TRATAMIENTO DE RIESGOS

Luego de elegir los controles más adecuados para tener un nivel de riesgo aceptable para los procesos, se diseñó el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información, en el cual se tienen en cuenta la reducción del riesgo, los controles, las actividades y los responsables de la ejecución, y así medir periódicamente la ejecución de los mismos mediante un indicador definido para cada activo de la información.

Activo de información	Opciones de manejo del riesgo	Controles	Actividad	Objetivo	Responsable	Periodo/ Fecha	Indicador
Canal de datos, Conexión a internet, Servidor de almacenamiento	Reducir el riesgo	Mantenimiento preventivo de los equipos de red	Contratar los servicios para el mantenimiento de los equipos de red	Realizar un adecuado soporte a los equipos de red de la entidad	Área de sistemas	Anualmente	Numero de mantenimientos realizados /número de mantenimientos programados
Documentación de las diferentes áreas del hospital y bases de datos de los sistemas: Rocky, Genesis, Suite de Google	Reducir el riesgo	Socializar plan de seguridad de la información con toda el área de sistemas	Almacenar las copias de seguridad de una forma periódica	Reducir la perdida de información	Área de sistemas	Semestral	Copias programadas/ Copias realizadas
Rocky, Genesis, Office,	Reducir el riesgo	Soporte a los distintos	Verificar funcionamiento,	Mantener la continuida	Área de sistemas	Trimestral	Cantidad de equipos

Softros LAN Messenger, PDF24, Anydesk, Adobe Reader, Software de equipos de laboratorio.		softwares utilizados en la entidad	licencias y permisos de los distintos softwares	d de los servicios y actividades del hospital			verificados /Cantidad de equipos totales
Servidor de archivos, servidor Rocky, servidor financiero	Reducir el riesgo	Mantenimiento preventivo servidores físicos	Realizar mantenimiento a los equipos que funcionan como servidor en la institución	Mantener la continuidad de los servicios y actividades del hospital	Área de sistemas	Anualmente	Cantidad de mantenimientos realizados /Cantidad e equipos

11. 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.

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

12. 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