TABLA DE CONTENIDO

1. INTRODUCCIÓN

Diariamente el Hospital Raúl Orejuela Bueno E.S.E. utiliza las plataformas tecnológicas para la captura, procesamiento y reporte de información, para procesarse internamente y externamente, también para comunicarse con los diferentes actores del sistema de salud, lo cual implica que la institución sea vulnerable a ataques mal intencionados o mala manipulación de la información lo que acarrea problemas económicos, legales, y administrativos por lo cual este documento busca establecer un línea de trabajo que permita a la entidad sortear los riesgos que lo rodean y lograr que su información este segura.

La institución en pro de mejorar continuamente, implementa un método lógico y sistemático que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados el

manejo de la información institucional, para lograr que estos no afecten de una manera relevante a la misma.

El presente Plan fue elaborado por parte del Equipo de Tecnologías y Técnicas de la Información, con base en el proceso dinámico de planeación - el cual es enunciativo y no taxativo -. Por ello, podrá ser objeto de modificación o actualización, en el proceso de su implementación, en el evento de variar las condiciones internas o externas que lo originaron. Su ejecución se hará de acuerdo con la disponibilidad presupuestal y los recursos en caja.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Desarrollar una guía para el control y minimización de los riesgos y así proteger la privacidad de la información y los datos tanto de los procesos como de las personas vinculadas con la información de la institución.

2.2. OBJETIVOS ESPECÍFICOS

- Lograr un diagnóstico real de la situación actual de la institución en materia de riesgos de seguridad y privacidad de la Información.
- Aplicar las metodologías, mejores prácticas y recomendaciones dadas por la Función Pública y MinTIC para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Optimización de los recursos de la institución en la aplicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

3. ALCANCE

El plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional.

4. RESPONSABLE

Subgerencia Administrativa, Líder de Programa (Tecnologías y Técnicas de Información).

5. MARCO NORMATIVO

- Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública

- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública

- Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública
- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales
- Ley 594 de 2000 - Ley General de Archivos
- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática
- Ley Estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad
- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo
- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos
- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública
- Decreto 2364 de 2012 - Firma electrónica
- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos
- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales
- Ley 527 de 1999 - Ley de Comercio Electrónico
- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
- Ley Estatutaria 1581 de 2012 - Protección de datos personales
- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información.

6. DEFINICIONES

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC27000).
- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art

- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **Responsabilidad Demostrada:** Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Partes interesadas:** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

7. POLITICAS RELACIONADAS

- PO1-TIC “Política Protección de Datos”
- PO2-TIC “Política de Seguridad de la Información Digital”

8. PROGRAMAS / PROYECTOS RELACIONADOS

Plan de Desarrollo Institucional 2024-2027 “EL HROB te cuida”
Conforme al Artículo 339 de la Constitución Política de Colombia, modificado por el Acto Legislativo 003 de 2011, las entidades deben elaborar y adoptar, planes de desarrollo que aseguren el uso eficiente de los recursos y el adecuado desempeño de las funciones asignadas. Estos planes están compuestos por una parte estratégica y un plan de inversiones de mediano y corto plazo, en este sentido; el Plan de Desarrollo Institucional de la E.S.E. Hospital Raúl Orejuela Bueno 2024-2027 denominado "**El HROB Te Cuida**", está diseñado conforme a los principios, políticas y directrices del Sistema General de Seguridad Social en Salud.

El Hospital Raúl Orejuela Bueno E.S.E. en su plan estratégico “EL HOSPITAL TE CUIDA” definió cuatro líneas estratégicas HOSPITAL MAS SANO (Fortalecer la prestación de los servicios de salud con la implementación de la Estrategia de Atención Primaria en Salud en la población asignada al Hospital Raúl Orejuela Bueno.), HOSPITAL MAS HUMANO (Mejorar el nivel de satisfacción del cliente interno y externo), HOSPITAL MAS BACANO (Mejorar el ambiente físico y tecnológico del Hospital) y HOSPITAL MAS SOSTENIBLE (Mejorar la gestión de los recursos financieros, asegurando una adecuada planificación, ejecución y seguimiento de los ingresos y gastos).

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se encuentra alineado al Plan de Desarrollo Institucional y da cumplimiento a éste, de la siguiente manera:

- **LINEA ESTRATÉGICA: HOSPITAL MAS BACANO**
- **OBJETIVO ESTRATÉGICO No.3:** Mejorar el ambiente físico y tecnológico del Hospital.
- **Objetivo Específico:** Mejorar tecnológicamente la E.S.E. en aporte al cumplimiento de la misión, la calidad y seguridad de los servicios, la satisfacción de los usuarios, el bienestar del cliente interno y al posicionamiento de la institución de manera que contribuya a la venta de servicios y la productividad.
- **Meta de Producto:** Modernización de los elementos que hacen parte tecnológica (Hardware, Software) de la E.S.E. que permiten la articulación de los procesos misionales y de apoyo a la gestión, contribuyendo con esto a la construcción de un hospital más bacano.
- **Indicador:** Elementos TIC modernizados del Hospital Raúl Orejuela Bueno
- **Meta 2024-2027:** 100%.

9. EVALUACIÓN Y MONITOREO

El monitoreo y revisión debe asegurar que las acciones establecidas en los mapas de riesgo se están llevando a cabo y evaluar la eficacia en su implementación, adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden influir en la aplicación de acciones preventivas

Permite determinar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo. Se evalúan verificando su documentación, aplicación y efectividad

Monitorear periódicamente la evaluación de los riesgos desarrollada en la entidad, donde a su vez se validen los niveles aceptables del riesgo residual después de la aplicación de controles y medidas administrativas.

El Hospital debe conservar información documentada apropiada como evidencia de los resultados del monitoreo y la medición. Resultados de las auditorías internas.

La entidad ha definido lineamientos en cuanto a la protección de las instalaciones físicas, equipos de cómputo y su entorno para evitar accesos no autorizados y minimizar riesgos de la información de la entidad: Monitorio con cámara y seguridad de los data center y cuartos de comunicación para ingreso solo del personal de sistemas.

La entidad ha implementado mecanismos para detectar periódicamente vulnerabilidades de seguridad en el funcionamiento de: a) su infraestructura, b) redes, c) sistemas de información, d) aplicaciones y/o e) uso de los servicios: Monitoreo diario por parte del ing. de infraestructura.

La entidad ha implementado lineamientos contra modificación o pérdida accidental de información: monitoreo de cuantos casos al año se han presentado y si la recuperación de la información ha sido satisfactoria.

Cuántos ataques recibió la entidad en el último año que impidieron la prestación de algunos de los servicios que la entidad ofrece a los ciudadanos y empresas.

10. DESCRIPCION DEL PLAN

10.1. IDENTIFICAR EL RIESGO

El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas recolectan datos de entrada para esta actividad.

10.2. CATEGORÍAS DE RIESGOS

- **Estratégicos:** Relacionados a lineamientos, políticas, estrategias o directrices no adecuadas o no convenientes para la Entidad.
- **Operativo:** Relacionado a procesos, conductas o actividades inapropiadas, contrarias al deber ser o que presente una posible brecha frente a la calidad esperada.
- **Gerenciales:** posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
- **Financiero:** Relacionado con la asignación, suficiencia o recaudo de recursos económicos que puedan afectar a corto, mediano o largo plazo financieramente a los procesos o la entidad.
- **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.
- **Corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **De Imagen:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
- **Tecnológico:** Relacionado al uso, manejo o disposición de equipos biomédicos, industriales o de cómputo y periféricos.
- **Seguridad Digital:** Posibilidad Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

10.3. DESCRIPCIÓN DE CAUSAS

Se describen las causas asociadas al riesgo identificado, pueden ser intrínsecas: atribuidas a personas, métodos, materiales, equipos, instalaciones, directamente involucradas en el proceso o externas: cuando provienen del entorno en el que se desarrolla el proceso.

10.4. CONSECUENCIAS

Se describen los efectos asociados a la materialización del riesgo, que incidan sobre el objetivo del proceso o la Entidad. Pueden agruparse en: Daños a pacientes o trabajadores, Perdidas.

10.5. BARRERAS DE SEGURIDAD EXISTENTES

Se describen los controles implementados o barreras que existen actualmente para evitar la

materialización del riesgo, se pueden encontrar en los protocolos o procedimientos documentados, en las guías de reacción inmediata o en los correctos de buenas prácticas de seguridad del paciente.

10.6. VALORACIÓN DEL RIESGO

Se mide en cuanto a probabilidad e impacto para obtener un dato cuantitativo que permita su comparación y priorización, como se muestra en las siguientes escalas de valoración:

ESCALA DE VALORACIÓN DE PROBABILIDAD		
Valor	**Grado Daño**	**Percepción del Proceso**
1	**Muy baja**	Nunca ha ocurrido el evento
2	**Baja**	Una vez cada dos años
3	**Moderado**	De 6 meses un año
4	**Alta**	De un mes a seis meses
5	**Muy Alta**	Mas de una vez por mes

ESCALA DE VALORACIÓN IMPACTO		
Valor	**Grado Daño**	**Percepción del Proceso**
1	**Muy baja**	No genera impactos visibles en el proceso. No afecta la imagen ni bienes de la organización. Los clientes no detectan el fallo.
2	**Baja**	Afecta el proceso de manera leve, los daños en el área daños mínimos, visibles a largo plazo y no hace falta intervenir o la intervención necesaria es mínima. Clientes perciben un ligero descontento.
3	**Moderado**	Causa un daño que afecta el proceso, requiere intervención oportuna. Implica consecuencias al interior de la organización. Indica reprocesos.
4	**Alta**	Causa un daño que afecta el flujo del proceso, visible y perceptible en el instante y requiere intervención inmediata. Compromete imagen y bienes de la organización. Implica consecuencias internas y externas a la Institución (Procesos legales por entes regulatorios).
5	**Muy Alta**	El proceso se bloquea por completo. Implica consecuencias internas y externas a la Institución. Total insatisfacción del cliente.

ESCALA DE VALORACIÓN DE LA DETECCIÓN / CONTROL DEL FALLO		
Valor	**Grado Daño**	**Percepción del proceso**
1	**Muy Alta**	Es detectable por toda la organización.
2	**Alta**	El fallo, aunque es obvio y fácilmente detectable, podría en alguna ocasión escapar inicialmente a un control, aunque sería detectado con toda seguridad a posterior.

ESCALA DE VALORACIÓN DE LA DETECCIÓN / CONTROL DEL FALLO		
Valor	**Grado Daño**	**Percepción del proceso**
3	**Medio**	El fallo es detectable y posiblemente no sea perceptible por los colaboradores o procesos cliente. Es probable que se detecte en las últimas fases del proceso.
4	**Baja**	El fallo es de tal naturaleza que resulta difícil detectarlo con los procedimientos establecidos hasta el momento.
5	**Muy bajo**	El fallo no puede detectarse. No existen controles o estos son inoperantes.

NIVEL DE RIESGO		
ZONA DE RIESGO	**OPCIONES DE MANEJO**	**DEFINICIÓN**
Riesgo bajo	**Asumir el riesgo**	No requiere acciones: Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el líder del proceso simplemente acepta la perdida residual probable y elabora dado el caso planes de contingencia para su manejo.
Riesgo medio	**Reducir el riesgo**	Requiere acciones: Asocia medidas para disminuir la probabilidad (medidas preventivas) y el impacto (medidas de protección), que implican menores esfuerzos en términos operativos y de costos. A manera de ejemplo se tiene: optimización de procedimientos, implementación de nuevos indicadores, etc.
Riesgo alto	**Evitar el riesgo**	Requiere acciones: Se refiere medidas orientadas a prevenir la materialización del riesgo; dicha opción se toma cuando es posible generar cambios importantes en los procesos, mejoramiento de actividades y controles, rediseño de los procesos, acciones de mejora, nuevos métodos de control de calidad, supervisión continua de procesos (auditorias).

10.7. IDENTIFICACIÓN DE RIESGOS

RIESGO	Posibilidad de uso indebido de la información
DESCRIPCION	Posibilidad de que se acceda, manipule y divulgue sin autorización la información del hospital
CLASE	Riesgo de corrupción, opacidad y fraude - sicof
CAUSAS	Bajo nivel de seguridad para el acceso a la información.
EFECTOS	Sanciones

IMPACTO	Corrupción
ZONA DE RIESGO	Extremo
ACCIONES	Socialización de las políticas de manejo de la información. FR36-GTH INDUCCIÓN GENERAL. CON REGISTRO ASISTENCIA.
RESPONSABLES	Subgerencia Administrativa - Tecnología de la Información y Comunicaciones

RIESGO	Posibilidad de pérdida de información por no realizar custodias y administración de las copias de seguridad
DESCRIPCION	Custodia y administración de las copias de seguridad
CLASE	Riesgo operacional
CAUSAS	Problemas eléctricos y daño en los equipos de respaldo. Ataque Cibernético. Daño o Perdida de los equipos de respaldo externos.
EFECTOS	Perdida de información alojada en los servidores
IMPACTO	Económico y reputacional
ZONA DE RIESGO	Moderado
ACCIONES	Realizar copias de seguridad periódicas. BITACORA COPIAS DE SEGURIDA FR10-TIC
RESPONSABLES	Subgerencia Administrativa - Tecnología de la Información y Comunicaciones

RIESGO	Posibilidad de efecto dañoso a la estructura tecnológica
DESCRIPCION	No cumplimiento del cronograma de mantenimiento Preventivo.
CLASE	Riesgos Operativos

CAUSAS	• Falta y/o inadecuado mantenimiento de los recursos • Baja calidad de los recursos • Falta de capacitación sobre el adecuado uso de los recursos • Factores ambientales • Perdida de conexión a las bases de datos y recuperación de la Información • No cumplimiento del cronograma de mantenimiento Preventivo. • Desastres Naturales • Ataques Cibernéticos
EFECTOS	Perdida de Información y suspensión de los servicios prestados.
IMPACTO	Económico y reputacional
ZONA DE RIESGO	Alto
ACCIONES	Monitorear los mantenimientos a los recursos Instalación y verificación del antivirus. informe cada dos meses

RESPONSABLES	Subgerencia Administrativa - Tecnología de la Información y Comunicaciones

RIESGO	Posibilidad de efecto dañoso sobre los recursos tecnológicos a cargo de funcionarios
DESCRIPCION	Falta de mantenimiento en los recursos tecnológicos
CLASE	Riesgos Operativos
CAUSAS	• Falta y/o inadecuado mantenimiento de los recursos • Baja calidad de los recursos • Falta de capacitación sobre el adecuado uso de los recursos • Factores ambientales
EFECTOS	Daño perjudicial a los recursos tecnológicos
IMPACTO	Impacto Operativo
ZONA DE RIESGO	Bajo
ACCIONES	Monitoreo de los mantenimientos a los recursos. cronograma de mantenimientos.
RESPONSABLES	Subgerencia Administrativa - Tecnología de la Información y Comunicaciones

RIESGO	Posibilidad de ausencia y/o deficiencia en los software y sistemas de información
DESCRIPCION	Ausencia y/o deficiencia en los software y sistemas de información que afecta la operación y el manejo adecuado de la información
CLASE	Riesgo Operativos
CAUSAS	Desconocimiento de normas relacionadas con derechos de autor. Falta de Presupuesto. Falta de control en los usuarios y el manejo de Internet.
EFECTOS	Las licencias no sean renovadas en el tiempo pertinente o los usuarios instalen software ilegal.

IMPACTO	Impacto Operativo
ZONA DE RIESGO	Extremo
ACCIONES	Cualquier adquisición de software o Hardware, cuenta con el visto bueno de TIC, donde se garantiza que cumple con las necesidades del Hospital y es compatible con la infraestructura, se realizan los estudios previos con visto bueno de TIC. Solo se permite realizar instalación de software con el usuario administrativo de sistemas, monitores de software con herramienta Inventory Inventario de licencias revisión de fecha de vencimiento de licencias.
RESPONSABLES	Subgerencia Administrativa - Tecnología de la Información y Comunicaciones

RIESGO	Posibilidad de Vulnerabilidad del sistema de información
DESCRIPCION	Vulnerabilidad del sistema de información que puede comprometer la seguridad, confidencialidad, integridad y disponibilidad de los datos.
CLASE	Riesgo de corrupción, opacidad y fraude - sicof
CAUSAS	Bajo nivel de seguridad para el acceso a la información. Cortafuegos inadecuados. Virus en los sistemas de información.
EFECTOS	Posibilidad que terceros que entre de forma indebida o fraudulenta a los sistemas de información del hospital, para alterar, hurtar o dañar la información.
IMPACTO	Corrupción
ZONA DE RIESGO	Extremo
ACCIONES	Fortalecimiento de los cortafuegos. Informe de herramientas de seguridad de la información y accesos no autorizados. seguridad perimetral
RESPONSABLES	Subgerencia Administrativa - Tecnología de la Información y Comunicaciones

RIESGO	Posibilidad de fallas en las telecomunicaciones y fluido eléctrico
DESCRIPCION	Ocurrencia de fallas en las telecomunicaciones y en el suministro de fluido eléctrico que afectan la continuidad d ellos servicios y la operación institucional.
CLASE	Riesgos Operativos
CAUSAS	• Falta de disponibilidad del servicio por parte del proveedor • Falta de mantenimiento de los equipos y redes y deterioro de estas • Falta de protección ante pico de voltajes y/o interrupción del fluido eléctrico no planificado (Redundancia de Energía).
EFECTOS	Posibilidad de que se presenten fallas en las telecomunicaciones (internet, redes, intranet, servicio telefónico) o en el fluido eléctrico de la entidad para el desarrollo de sus operaciones
IMPACTO	Económico y reputacional
ZONA DE RIESGO	Moderado
ACCIONES	Verificación de las condiciones operativas de la UPS y del sistema eléctrico. Verificación de las antenas de comunicaciones, fibra óptica y dispositivos de comunicaciones para la transmisión de datos
RESPONSABLES	Subgerencia Administrativa - Tecnología de la Información y Comunicaciones

RIESGO	Posibilidad de humedad producida por sistemas de refrigeración inadecuados y filtraciones de agua
DESCRIPCION	Presencia de humedad por sistemas de refrigeración inadecuados o filtraciones de agua, que puede afectar la infraestructura, los equipos y los sistemas de información.
CLASE	Riesgo Operativos
CAUSAS	Diseño Inadecuado y deterioro de Tuberías, mal manejo y falta de mantenimiento de aires acondicionados, contaminación en el mismo sistema de aire.
EFECTOS	humedad producida por sistemas de refrigeración inadecuados y filtraciones de agua
IMPACTO	Económico y reputacional
ZONA DE RIESGO	Moderado
ACCIONES	Estudio de la infraestructura del edificio y realizar controles de prevención, con apoyo del SGSST e Infraestructura

RESPONSABLES	Subgerencia Administrativa - Tecnología de la Información y Comunicaciones

RIESGO	Posibilidad de Acceso no autorizados a las instalaciones del área tecnológica
DESCRIPCION	Acceso no autorizado a las instalaciones del área tecnológica que puede comprometer la seguridad de los equipos, la información y los sistemas.
CLASE	Riesgo Operativos
CAUSAS	Inadecuado control de acceso a las instalaciones Puertas no aptas para la seguridad
EFECTOS	Accesos no autorizados a las instalaciones del área tecnológica
IMPACTO	Económico y reputacional
ZONA DE RIESGO	Alto
ACCIONES	Se cuenta solo con 2 juegos de llaves, uno lo presenta el líder de Tics y la otra es el Subgerente Administrativo
RESPONSABLES	Subgerencia Administrativa - Tecnología de la Información y Comunicaciones

10.8. TRATAMIENTO Y SEGUIMIENTO DEL RIESGO

Se describen los controles o barreras a ser implementadas que fortalezcan las existes, con lo cual aportar y evitar la materialización del riesgo desde la reducción de la probabilidad y/o del impacto. Las acciones propuestas pueden en algunos casos significar actualización de protocolos o procedimientos documentados, adopción de mejores prácticas a través de referenciaciones realizas, fortalecimiento de buenas prácticas de seguridad del paciente, asesorías con expertos, entre otras.

Un aspecto de gran importancia es la definición de indicadores para determinar el impacto de las acciones realizadas, ya que no es suficiente cumplir las actividades propuestas sino también valorar como estas acciones permiten disminuir la probabilidad de ocurrencia o nivel de impacto del riesgo; es decir, el indicador mide la efectividad de las acciones frente a la mitigación del riesgo.

11. DOCUMENTOS RELACIONADOS Y DE REFERENCIA BIBLIOGRAFICA

- PO1-TIC “Política Protección de Datos”
- PO2-TIC “Política de Seguridad de la Información Digital”
- El documento tomo como referencia los documentos y lineamientos de El Ministerio de Tecnologías de la Información y las Comunicaciones: https://www.mintic.gov.co/portal/inicio/

12. CONTROL DE CAMBIOS DE LA INFORMACION DOCUMENTADA

No. Versión	Fecha Revisión / Actualización	Pagina	Solicitante	Cambios y/o modificaciones realizadas
01	Enero de 2019	Todo	Octavio Enrique Murillas Peña	Emisión del Documento
02	Enero de 2020	Todo	Octavio Enrique Murillas Peña	Actualización logo símbolos ICONTEC
03	Enero de 2021	Todo	Luisa Fernanda Arismendi Muñoz	Revisión y modificación
04	Enero de 2022	Todo	Luisa Fernanda Arismendi Muñoz	• Se actualiza plantilla de planes de proceso. • Se actualiza nuevo esquema de codificación de documentos. PL2-TIC • Se actualiza por completo la información del plan
04	Enero de 2023	Todo	Dora Isaura López	Se revisa todo el documento y no requiere actualización, lo cual continua con la misma versión 04
05	Enero de 2024	Todo	Dora Isaura López serna	• Se actualiza alcance del plan, al año 2024 • Se agrega en la Categoría de los Riesgos, los riesgos Gerenciales, de Corrupción, de Imagen, de Cumplimiento • Se actualiza la metodología de valoración del riesgo ítem 11.6.
06	Enero de 2025	Todo	Octavio E. Murillas Peña	• Se actualiza el plan de desarrollo

07	**Enero de 2026**	**Todo**	Octavio E. Murillas Peña	• Actualización de riesgos, acorde a la matriz de riesgos que se tiene por seguridad de la información.

	NOMBRE	CARGO	FIRMA
ELABORÓ	Octavio E. Murillas Peña	Líder de Programa (Tecnologías y Técnicas de la Información)	Ver Formato FR35-GCA Aprobación de la Información Documentada
REVISÓ	Alexander Trujillo Bejarano	Subgerente Administrativo	Ver Formato FR35-GCA Aprobación de la Información Documentada
	Camilo de la cruz	Contratista	Ver Formato FR35-GCA Aprobación de la Información Documentada
	Isabel Cristina Torres	Jefe de Calidad	Ver Formato FR35-GCA Aprobación de la Información Documentada
APROBÓ	Clara Inés Sánchez Perafan	Gerente	Ver Formato FR35-GCA Aprobación de la Información Documentada