TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Hospital Raúl Orejuela Bueno E.S.E. busca la implementación de las políticas dadas por el Departamento de Administrativo de la Función Pública con su estrategia MIPG y el Ministerio de las Tecnologías e Información en el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información; este pretende lograr en la institución y sus clientes internos, externos y partes interesadas la confianza en el manejo de la información garantizando para cada uno la privacidad, continuidad, integralidad y disponibilidad de los datos.

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

Generar un documento institucional guiado en los lineamientos de buenas prácticas en seguridad y Privacidad de la información.

2.2. OBJETIVOS ESPECÍFICOS

- Promover el uso de mejores prácticas de seguridad de la información en la institución.
- Optimizar la gestión de la seguridad de la información al interior de le entidad.
- Aplicar la legislación relacionada con la protección de datos personales.
- Optimizar el acceso a la información pública.

3. ALCANCE

El Plan 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 6)

- **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 2020-2024 “Te Queremos Sano”
El Hospital Raúl Orejuela Bueno E.S.E. cuenta con el Plan de Desarrollo Institucional para el período 2020-2024 denominado “Te Queremos Sano”, el cual fue presentado ante la Junta Directiva de la Entidad, y aprobado por esta mediante Acuerdo No. 017 del 30 de octubre de 2020.

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:

- **Eje Estratégico** 1. Calidad y Eficiencia en la Prestación de Servicios de Salud para todos y por todos.
- **Objetivo Estratégico:** Entregar a los usuarios internos y externos calidad, seguridad, eficiencia y calidez en los servicios de promoción y prevención, recuperación y la rehabilitación desde los diferentes niveles de complejidad de la E.S.E.
- **Objetivo Específico:** Mejorar la infraestructura física, tecnológica y de operación de 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:** Articular con operación en línea los componentes, módulos o interfaces del sistema de información que opera en la Entidad (Presupuesto Oficial, Jurídico, Facturación Hospitalaria, Promoción y Prevención, Cartera Hospitalaria, Inventarios, Farmacias, Activos Fijos, Nómina, Costos, Contabilidad General+NIIF, Historias Clínicas, Laboratorio Clínico, CRM).
- **Indicador:** Componentes, módulos o interfaces integrados en el sistema de información que opera en la Entidad.
- **Meta 2020-2024:** 100%.

9. EVALUACIÓN Y MONITOREO

Se monitoreará la efectividad de los controles establecidos para el cumplimiento de los objetivos de seguridad.

Controles como:

- Socialización de la Política de protección datos personales. Seguridad de la información sensible protegida por roles y permisos.
- Socialización de la política de seguridad de la información.
- Capacitación y sensibilización de manejo de usuario de los sistemas de información del hospital como son el correo y R-fast a todos los funcionarios que ingresan al hospital. Evidencia capacitación en talento humano.
- Número total de anomalías encontradas. Auditoria de seguimiento al uso correcto de licencias y software de la entidad. Revisión de los resultados de las auditorías internas.
- Número de personas con su respectivo rol definió después de un año evidencia correos o mesa de servicio donde se solicitan la creación de permiso y roles.
- La entidad ha definido lineamientos, normas y/o estándares para controlar el acceso de los usuarios las redes de comunicaciones. Como evidencia reglas de seguridad y dispositivos de seguridad de la red.
- La entidad ha definido lineamientos, normas y/o estándares para controlar el uso y el acceso a los sistemas de información, las aplicaciones y los depósitos de información con las que cuenta la entidad

10. DESCRIPCION DEL PLAN

El equipo de colaboradores y la Gerente del Hospital, se comprometen a garantizar la confidencialidad, seguridad e integralidad de la información de los usuarios y su familia, clientes internos y externos en cuanto a seguridad lógica y física de los activos de la información, fomento de canales de comunicación que garanticen acceso y transparencia de la información pública a través de uso adecuado de las TICS, cumpliendo con las disposiciones generales para la protección de datos, aportando al cumplimiento de la Misión, Visión y objetivos estratégicos de la institución.

Objetivos

- Cumplir con los principios de seguridad de la información
- Proteger los activos tecnológicos.

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes.
- Garantizar la continuidad del negocio frente a incidentes.

10.1. OBJETIVOS DE LA POLÍTICA DE GESTIÓN DE CALIDAD

- Garantizar la protección de datos personales de usuarios, clientes, proveedores y colaboradores, tanto en los medios físicos como electrónicos.

- Controlar el uso efectivo de equipos de cómputo que garantice la confidencialidad, seguridad e integralidad de la información de los usuarios.

10.2. ESTRATEGIAS

- Determinar posibles acciones correctivas derivadas de hallazgos identificados en la autoevaluación con respecto a la seguridad y privacidad de la información al interior de la entidad.
- Capacitar al personal interno en seguridad digital.

10.3. RECURSOS

- Humano: Gerente, Líderes de Proceso, Sistemas de Información.
- Físico: Infraestructura Tecnológica.

10.4. RESPONSABLES

- Gerente, Líderes de Proceso y Sistemas de Información

10.5. ACTIVIDADES

1. Gestión de Activos
2. Política de tratamientos de Datos
3. Política de seguridad de la información digital.
4. Custodia de la información
5. Seguridad física y ambiental
6. Relaciones con los proveedores
7. Aspectos de seguridad de la información en la gestión de continuidad del negocio.

10.6. IDENTIFICACIÓN DE RIESGOS

RIESGO	Software sin licencias y desactualización de las existentes
DESCRIPCION	Las licencias no sean renovadas en el tiempo pertinente o los usuarios instalen software ilegal.
CLASE	Riesgos de Cumplimiento.

CAUSAS	Desconocimiento de normas relacionadas con derechos de autor. Falta de Presupuesto. Falta de control en los usuarios y el manejo de Internet.
EFECTOS	Sanciones
IMPACTO	Impacto Legal
ZONA DE RIESGO	Baja
ACCIONES	Realizar visitas a las diferentes dependencias para revisar qué tipo de software está instalado y retirarlo de los equipos. Revisión de fecha de vencimiento de licencias. Montaje de Control específicos, software de monitoreo que permitan la limitación de Instalación de software no autorizado. Solicitar inclusión en el presupuesto la compra de licencias.
RESPONSABLES	Subgerencia Administrativa - Tecnología de la Información y Comunicaciones

RIESGO	Copias de Seguridad
DESCRIPCION	Custodia y administración de las copias de seguridad
CLASE	Riesgos Operativos
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	Impacto Operativo
ZONA DE RIESGO	Baja
ACCIONES	Creación de Protocolo de Copias de Seguridad. Realizar copias de seguridad periódicas. Respaldo de copias de seguridad en la nube.
RESPONSABLES	Subgerencia Administrativa - Tecnología de la Información y Comunicaciones

RIESGO	Daño en la infraestructura tecnológica
DESCRIPCION	Perdida de conexión a las bases de datos y recuperación de la Información
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	Impacto Operativo
ZONA DE RIESGO	Baja
ACCIONES	Copias de seguridad en la nube por si hay un desastre natural, antivirus y cortafuegos para evitar ataques cibernéticos

RESPONSABLES	Subgerencia Administrativa - Tecnología de la Información y Comunicaciones

RIESGO	Daño, deterioro, perdida de los recursos tecnológicos a cargo de funcionarios
DESCRIPCION	Perdida de conexión a las bases de datos y recuperación de la Información
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	Perdida de Información y suspensión de los servicios prestados.
IMPACTO	Impacto Operativo
ZONA DE RIESGO	Baja
ACCIONES	Copias de seguridad en la nube por si hay un desastre natural, antivirus y cortafuegos para evitar ataques cibernéticos Inclusión de Nuevos equipos al Cronograma de Mantenimientos
RESPONSABLES	Subgerencia Administrativa - Tecnología de la Información y Comunicaciones

RIESGO	Ausencia y/o deficiencia en los software y sistemas de información
DESCRIPCION	Perdida de conexión a las bases de datos y recuperación de la Información
CLASE	Riesgos Tecnológico
CAUSAS	Las licencias no sean renovadas en el tiempo pertinente o los usuarios instalen software ilegal. Desconocimiento de normas relacionadas con derechos de autor. Falta de Presupuesto. Falta de control en los usuarios y el manejo de Internet. Hace referencia a la falta de programas licenciados.
EFECTOS	Sanciones
IMPACTO	Impacto Operativo
ZONA DE RIESGO	Muy Baja
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
RESPONSABLES	Subgerencia Administrativa - Tecnología de la Información y Comunicaciones

RIESGO	Vulnerabilidad del sistema de información
DESCRIPCION	Perdida de conexión a las bases de datos y recuperación de la Información
CLASE	Riesgos Tecnológico
CAUSAS	Bajo nivel de seguridad para el acceso a la información. Cortafuegos inadecuados. Virus en los sistemas de información.

EFECTOS	Posibilidad que terceros entre de forma indebida o fraudulenta a los sistemas de información del hospital, para alterar, hurtar o dañar la información.
IMPACTO	Impacto Operativo
ZONA DE RIESGO	Muy Baja
ACCIONES	Fortalecimiento de los cortafuegos. Antivirus actualizado Seguridad de roles y contraseñas
RESPONSABLES	Subgerencia Administrativa - Tecnología de la Información y Comunicaciones

RIESGO	Fallas en las telecomunicaciones y fluido eléctrico
DESCRIPCION	Perdida de conexión a las bases de datos y recuperación de la Información
CLASE	Riesgos Tecnológico
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	Impacto Operativo
ZONA DE RIESGO	Muy Baja
ACCIONES	Mantenimiento periódico de la UPS y del sistema eléctrico. Redundancia en internet Actualmente el HROB cuenta con servicio contratado de internet de 150Mbps con el proveedor CLARO, este canal dedicado de internet actúa como principal para el Raúl Orejuela y todas sus 11 sedes; adicional, como contingencia se cuenta con el servicio de internet de 50Mbps contratado con PCNET.
RESPONSABLES	Subgerencia Administrativa - Tecnología de la Información y Comunicaciones

El plan está diseñado para cumplir la fase de determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad. Para realizar este paso los responsables del plan deben efectuar la recolección de la información con la ayuda de la guía de autoevaluación, guía de encuesta y guía metodológica de las pruebas de efectividad del MSPI.

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. PL3-TIC • Se actualiza por completo la información del plan
04	Enero de 2023	Todo	Dora López Serna	Se revisa todo el documento y no requiere actualización, lo cual continua con la misma versión 04.
04	Enero de 2024	Todo	Dora López Serna	Se revisa todo el documento y no requiere actualización, lo cual continua con la misma versión 04.

	NOMBRE	CARGO	FIRMA
ELABORÓ	Dora Isaura López Serna	Líder de Programa (Tecnologías y Técnicas de la Información)	*FIRMADO EL ORIGINAL*
REVISÓ	José Luis Quintero Santos	Subgerente Administrativo	*FIRMADO EL ORIGINAL*
	Yennifer Ayala S	Contratista Profesional	*FIRMADO EL ORIGINAL*
APROBÓ	Darwin Steven Zapata Forero	Gerente	*FIRMADO EL ORIGINAL*