HOSPITAL UNIVERSITARIO DE SINCELEJO E.S.E

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN PESI - FUSION

¡Un Hospital De Brazos Abiertos!

HOSPITAL UNIVERSITARIO DE SINCELEJO E.S.E

PROCESO: GESTIÓN ADMINISTRATIVA

SUBPROCESO: GESTIÓN DE LAS TICS

DOCUMENTO: PLAN

CÓDIGO: AGATIPL3

VERSIÓN No: 1

Aprobó: 22/01/2024
Nombre: Ruby Burgos Iglesias
Cargo: Gerente
Revisó: 18/01/2024
Nombre: Arnaldo Sánchez
Cargo: Subgerente Administrativo
Elaboró: 18/01/2024
Nombre: Oriana Corrales Peñates
Cargo: Gestor TICS

Tabla de Contenido

1. INTRODUCCIÓN

La seguridad de la información es una responsabilidad compartida de todos los niveles de la entidad del Hospital Universitario de Sincelejo ESE - FUSIONADO, que requiere del apoyo de todos ellos, facilitando la construcción de una entidad más transparente, colaborativo y participativo, en la interacción con el ciudadano, empresas privadas y demás entidades del estado, como se propone desde Gobierno en Línea.

A través del presente documento se busca la preservación de la confidencialidad, integridad y disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos; igualmente se basa en las recomendaciones técnicas establecidas en el Manual de la política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones (MinTIC), detalladas en el compendio denominado Modelo de Seguridad y Privacidad de la Información.

2. OBJETIVO

2.1.Objetivo General

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2024 – 2026.

2.2. Objetivos específicos

- Definir y establecer la estrategia de seguridad digital de la entidad.
- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información.
- Priorizar los proyectos a implementar para la correcta implementación del SGSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.
- Fortalecer las capacidades de gestión de TI en el Hospital Universitario de Sincelejo ESE y cada una de sus sedes aplicando buenas prácticas del modelo de gestión IT4+.

♦

3. ÁMBITO DE APLICACIÓN

El presente plan contempla la implementación y mejora continua de la seguridad de la información en todos los procesos del Hospital Universitario de Sincelejo ESE FUSIONADO acorde al Modelo de Seguridad y Privacidad de la Información (MSPI) definida por el MINTIC

4. DEFINICIONES

- **Gestión de TI:** Es una práctica, que permite operar, innovar, administrar, desarrollar y usar apropiadamente las tecnologías de la información (TI). A través de la gestión de TI, se opera e implementa todo lo definido por el gobierno de TI. La gestión de TI permite a una organización optimizar los recursos, mejorar los procesos de negocio y de comunicación y aplicar las mejores prácticas
- **MSPI:** Modelo de Seguridad y Privacidad de la Información - MSPI, está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la entidad, con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos
- **Instrumento de Evaluación MSPI:** Es una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente "Seguridad y Privacidad de la Información". Fue creada por el Ministerio de Tecnologías de la Información y las Comunicaciones con uso libre sin fines lucrativos.
- **PESI:** El plan estratégico de seguridad de la información determina los objetivos a cumplir para salvaguardar la información en sus pilares de confidencialidad, integridad y disponibilidad. Fuente:
- **PETI:** Plan Estratégico de TI, de acuerdo con el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI del Estado colombiano, el Plan Estratégico de las Tecnologías de la Información Y Comunicaciones, es el artefacto que se utiliza para

expresar la Estrategia de TI. El PETI hace parte integral de la estrategia de la institución y es el resultado de un adecuado ejercicio de planeación estratégica de TI.

- **Evaluación de riesgos:** Proceso global de identificación, análisis y estimación de riesgos
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos de información.
- **Política:** Conjunto de orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.
- **Política de Seguridad de la Información:** Conjunto de Directrices que permiten resguardar los activos de información.
- **Procedimiento:** Define los pasos para realizar una actividad específica. Evita que se aplique el criterio personal.
- **Riesgo:** Un efecto es una desviación de lo esperado: positivo o negativo Seguridad de la Información. El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.

5. RESPONSABLES

- **Comité de Sistema y de la Seguridad de la Información.**
  En el Comité de Sistemas y Seguridad de la Información, integrado con el comité de Gobierno en línea de la E.S.E., para soportar la administración y desarrollo de iniciativas sobre procesos TIC'S y seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de Seguridad de la Información a través de toda la organización y la planeación impulso de la estrategia de Gobierno en Línea.

- **Gestor TICS:**
  Profesional especializado encargado de liderar el proceso de FUSION en las dependencias de tecnologías de la información y las comunicaciones en cada una de las sedes del Hospital Universitario de Sincelejo ESE, Hospital regional de II nivel de San Marcos ESE, Hospital Regional de II nivel nuestra señora de las mercedes de corozal ESE, y la ESE San Juan de Betulia.

- **Profesional y Técnico en Sistemas.**
  Encargados de: Administración, Operación y el Mantenimiento de Redes de Datos y Voz, aseguramiento de la conectividad, implementación de soluciones de seguridad en los dispositivos de red. Administración de proveedores de telecomunicaciones, así como los servicios derivados de Internet como correo electrónico, servicio Web. Encargados de Diseñar y coordinar la ejecución de políticas y procedimientos relacionados con el mantenimiento de los equipos, soporte a usuario final tanto telefónico como de campo, actualización de sistemas operativos, software de usuario final, Dar mantenimiento a tablas, servicios e información consignada en bases de datos Administrativas y misionales.

6. CAPITULOS

6.1. MARCO NORMATIVO

A continuación, se relaciona el marco normativo relacionado con el Plan estratégico de Seguridad de la Información - PESI:

Marco Normativo	Descripción
Resolución 746 de 2022	Por el cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la resolución 500 de 2021
Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 090 de 2018	Por el cual establece plazo para que se inscriban las bases de datos que contengan datos personales.

Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Resolución 2710 octubre 2017	Por lo cual se establece lineamientos para la adopción del protocolo IPv6.
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
Documento Conpes 3854 de 2016	Política Nacional de Seguridad Digital.
Decreto 1083 de 2015	Por el cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, el cual incluye el Decreto 2573 de 2014 que establece los lineamientos generales de la Estrategia de Gobierno en Línea (Hoy Gobierno Digital).
Decreto 1078 de 2015	Por el cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, el cual incluye el Decreto 2573 de 2014, el cual establece los lineamientos generales de la Estrategia de Gobierno en Línea (Hoy Gobierno Digital).
Decreto 103 de 2015.	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

6.2. Análisis de la situación Actual

Apoyados en la herramienta “INSTRUMENTO DE EVALUACIÓN MSPI” se obtuvieron los resultados del análisis de brecha sobre la efectividad de los controles que se tienen actualmente en cada una de las sedes del Hospital Universitario de Sincelejo ESE con los siguientes resultados:

6.2.1. Sede Sincelejo

No.	EVALUACIÓN DE EFECTIVIDAD DE CONTROLES			
	Dominio	Calificación Actual	Calificación Objetivo	Evaluación De Efectividad De Control
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	90	100	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	80	100	**GESTIONADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	85	100	**OPTIMIZADO**
A.8	GESTIÓN DE ACTIVOS	90	100	**OPTIMIZADO**
A.9	CONTROL DE ACCESO	70	100	**GESTIONADO**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	80	100	**GESTIONADO**
A.12	SEGURIDAD DE LAS OPERACIONES	50	100	**EFECTIVO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	30	100	**REPETIBLE**
A.14	ADQUISICIÓN, DESARROLLO Y MANT ENIMIENTO DE SISTEMAS	60	100	**EFECTIVO**
A.15	RELACIONES CON LOS PROVEEDORES	90	100	**OPTIMIZADO**
A.16	GESTIÓN DE INCIDENTES D E SEGURIDAD DE LA INFORMACIÓN	70	100	**GESTIONADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	30	100	**REPETIBLE**
A.18	CUMPLIMIENTO	80	100	**GESTIONADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**65**	**100**	GESTIONADO

6.2.2. Sede Corozal

No.	EVALUACIÓN DE EFECTIVIDAD DE CONTROLES			
	Dominio	Calificación Actual	Calificación Objetivo	Evaluación de efectividad de control.
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	**GESTIONADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	50	100	**EFECTIVO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	60	100	**EFECTIVO**
A.8	GESTIÓN DE ACTIVOS	50	100	**EFECTIVO**
A.9	CONTROL DE ACCESO	50	100	**EFECTIVO**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	60	100	**EFECTIVO**
A.12	SEGURIDAD DE LAS OPERACIONES	50	100	**EFECTIVO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	30	100	**REPETIBLE**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	50	100	**EFECTIVO**
A.15	RELACIONES CON LOS PROVEEDORES	80	100	**GESTIONADO**

A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	50	100	**EFECTIVO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	30	100	**REPETIBLE**
A.18	CUMPLIMIENTO	70	100	**GESTIONADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**51**	**100**	**EFECTIVO**

6.2.3. Sede Betulia

No.	EVALUACIÓN DE EFECTIVIDAD DE CONTROLES			
	Dominio	Calificación Actual	Calificación Objetivo	Evaluación de efectividad de control
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	50	100	**EFECTIVO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	40	100	**REPETIBLE**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	50	100	**EFECTIVO**
A.8	GESTIÓN DE ACTIVOS	50	100	**EFECTIVO**
A.9	CONTROL DE ACCESO	50	100	**EFECTIVO**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	30	100	**REPETIBLE**
A.12	SEGURIDAD DE LAS OPERACIONES	30	100	**REPETIBLE**
A.13	SEGURIDAD DE LAS COMUNICACIONES	30	100	**REPETIBLE**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	30	100	**REPETIBLE**
A.15	RELACIONES CON LOS PROVEEDORES	50	100	**EFECTIVO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	30	100	**REPETIBLE**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	30	100	**REPETIBLE**
A.18	CUMPLIMIENTO	70	100	**GESTIONADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**39**	**100**	REPETIBLE

6.2.4. Sede San Marcos.

No.	EVALUACIÓN DE EFECTIVIDAD DE CONTROLES			
	Dominio	Calificación Actual	Calificación Objetivo	Evaluación de efectividad de control
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	90	100	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	70	100	**GESTIONADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	60	100	**EFECTIVO**
A.8	GESTIÓN DE ACTIVOS	70	100	**GESTIONADO**
A.9	CONTROL DE ACCESO	70	100	**GESTIONADO**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	60	100	**EFECTIVO**
A.12	SEGURIDAD DE LAS OPERACIONES	50	100	**EFECTIVO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	80	100	**GESTIONADO**

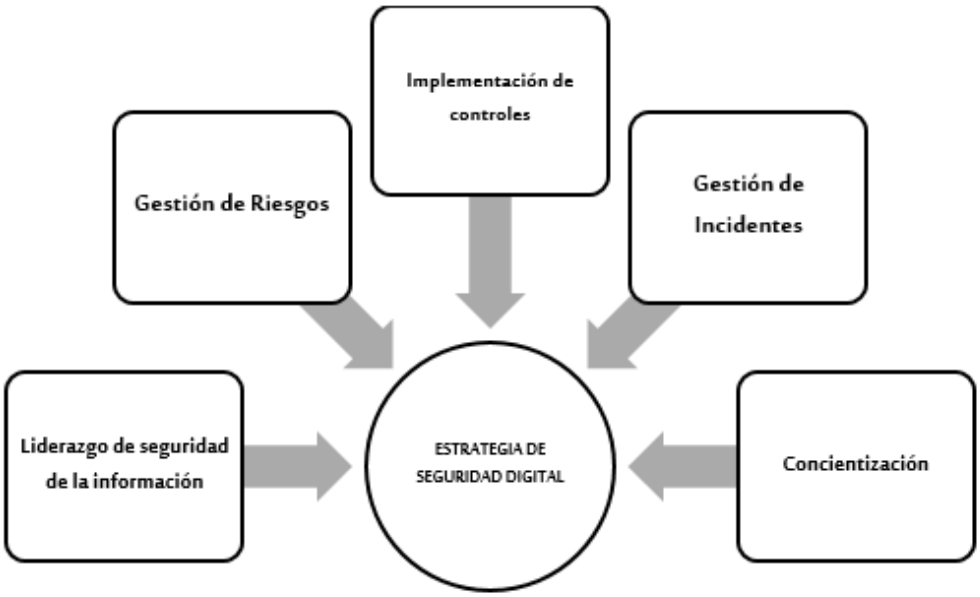
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	60	100	**EFECTIVO**
A.15	RELACIONES CON LOS PROVEEDORES	60	100	**EFECTIVO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	70	100	**GESTIONADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	60	100	**EFECTIVO**
A.18	CUMPLIMIENTO	70	100	**GESTIONADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**62**	**100**	**GESTIONADO**

Teniendo en cuenta los resultados obtenidos de la evaluación de efectividad de los controles de la seguridad de la información nos damos cuenta que la sede de Betulia necesita aplicar muchos controles de manera urgente para garantizar la calidad, integridad y disponibilidad de la información, de igual manera todas la sedes necesitan aplicar controles para asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

7. ESTRATEGIAS DE LA SEGURIDAD DE LA INFORMACION

El Hospital Universitario de Sincelejo ESE FUSIONADO define, implementa, evalúa y mejora las estrategias de seguridad de la información en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, con base en el Modelo de Seguridad y Privacidad de la Información -MSPI, así como en la política de riesgos de la entidad donde se incluye lo referente a seguridad de la información y lo establecido en el procedimiento de gestión de incidentes de seguridad de la información.

Dado lo anterior el Hospital Universitario de Sincelejo ESE FUSIONADO define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad de la información:



Estrategias de la Seguridad de la Información

- **Liderazgo de seguridad de la información**
  Certificar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes

dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.

- **Gestión de riesgos**
  Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.

- **Implementación de controles**
  Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.

- **Gestión de incidentes**
  Mantener una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

- **Concientización**
  Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.

8. CONTROL DE PORTAFOLIO DE PROYECTOS / ACTIVIDADES

A continuación se listan los proyectos para cada estrategia específica aplicables para todas las sedes del Hospital Universitario de Sincelejo ESE FUSIONADO:

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	PROYECTO 1: Desarrollar e implementar una política de seguridad PROYECTO 2: Definición de Roles y Responsabilidades de Seguridad de la Información.	Política de Seguridad Formalizada e Implementada. Definición de los Roles y Responsabilidades en Seguridad de la Información formalizados dentro de las políticas de seguridad.
Gestión de riesgos	PROYECTO 1: Identificar, valorar y clasificar los riesgos asociados a los activos de información PROYECTO 2: Definir planes de tratamiento de riesgos de seguridad	Matriz de riesgos de seguridad de la información. Definir planes de tratamiento de riesgos.
Concientización	PROYECTO 1: Establecer desde el inicio de cada año la planeación de sensibilización para todo el año. PROYECTO 2: Realizar jornadas de sensibilización a todo el personal. PROYECTO 3: Medir el grado de sensibilización a toda la Entidad.	1. Plan de Sensibilización 2. Evidencias de las actividades desarrolladas 3. Certificaciones de cursos 4. Resultado de las encuestas de medición

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Implementación de controles	CONTROL 1 Política de respaldos de información. CONTROL 2 Procedimiento de Gestión de Cambios. CONTROL 3 Clasificación de la información.	Política de respaldos de información. Procedimiento de Gestión de Cambios. Clasificación de la información.
Gestión de incidentes	PROYECTO 1: Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información. PROYECTO 2: Capacitar al personal en la gestión de incidentes de seguridad de la información.	1. Procedimiento de gestión de incidentes de seguridad formalizado. 2. Sesiones de capacitación desarrolladas.

9. CONTROL DE CRONOGRAMA DE ACTIVIDADES

A continuación, se presenta el componente operacional de este plan el cual incluye los proyectos de seguridad de la información:

Estrategia	Actividad	Descripción	Responsable	Fecha Inicio	Fecha Fin
Liderazgo de seguridad de la información	Fortalecer el modelo de seguridad y privacidad de la información	Establecer el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información a través del establecimiento de los roles y responsabilidades en seguridad de la información.	Gestor TICS	01/02/2024	29/02/2024
Gestión de riesgos	Identificar, evaluar, gestionar los riesgos de seguridad digital	Planificar y evaluar los riesgos de seguridad de la información más críticos dentro del Hospital Universitario de Sincelejo ESE buscando prevenir su materialización o reducir los efectos indeseados	Líderes de Sistemas de cada una de las sedes	01/03/2024	31/03/2024

Implementación de controles	Diseñar el componente de privacidad relacionado con la seguridad de los datos	De acuerdo con la identificación y evaluación de los riesgos, se debe proceder a efectuar un tratamiento de los riesgos con el objetivo de implementar los controles adecuados para minimizar los riesgos con su respectivo monitoreo	Líderes de Sistemas de cada una de las sedes	01/04/2024	30/04/2024
Gestión de incidentes	Contratar el servicio de gestión de eventos, monitoreo y respuesta a incidentes de seguridad	Contratar un proveedor externo el cual se encargue de monitorear las infraestructuras del de cada una de las sedes del Hospital y los sistemas de información, para detectar posibles amenazas, anomalías o intentos de intrusión o ataque. El objetivo de este proveedor es dar una respuesta inmediata y minimizar las posibles consecuencias	Gestor TICS	01/05/2024	31/05/2024

Concientización	Programar y desarrollar, conjuntamente con la oficina de Recursos Humanos, jornadas de sensibilización y capacitación de los funcionarios y contratistas de la entidad, sobre seguridad de la información y riesgos informáticos	Fortalecer la cultura del Hospital Universitario de Sincelejo ESE FUSIONADO en la seguridad de la información para funcionarios de planta, contratista, pasantes y sub-contratistas promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos a través de la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.	Líderes de Sistemas de cada una de las sedes	01/06/2024	31/08/2024

A continuación, se presenta el componente operacional de este plan el cual incluye los proyectos de seguridad de la información:

Estrategia	Actividad	Descripción	Responsable	Fecha Inicio	Fecha Fin
Liderazgo de seguridad de la información	Fortalecer el modelo de seguridad y privacidad de la información	Establecer el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información a través del establecimiento de los roles y responsabilidades en seguridad de la información.	Gestor TICS	01/02/2024	29/02/2024
Gestión de riesgos	Identificar, evaluar, gestionar los riesgos de seguridad digital	Planificar y evaluar los riesgos de seguridad de la información más críticos dentro del Hospital Universitario de Sincelejo ESE buscando prevenir su materialización o reducir los efectos indeseados	Líderes de Sistemas de cada una de las sedes	01/03/2024	31/03/2024
Implementación de controles	Diseñar el componente de privacidad relacionado con la seguridad de los datos	De acuerdo con la identificación y evaluación de los riesgos, se debe proceder a efectuar un tratamiento de los riesgos con el objetivo de implementar los controles adecuados para minimizar los riesgos con su respectivo monitoreo	Líderes de Sistemas de cada una de las sedes	01/04/2024	30/04/2024

Gestión de incidentes	Contratar el servicio de gestión de eventos, monitoreo y respuesta a incidentes de seguridad	Contratar un proveedor externo el cual se encargue de monitorear las infraestructuras del de cada una de las sedes del Hospital y los sistemas de información, para detectar posibles amenazas, anomalías o intentos de intrusión o ataque. El objetivo de este proveedor es dar una respuesta inmediata y minimizar las posibles consecuencias	Gestor TICS	01/05/2024	31/05/2024
Concientización	Programar y desarrollar, conjuntamente con la oficina de Recursos Humanos, jornadas de sensibilización y capacitación de los funcionarios y contratistas de la entidad, sobre seguridad de la información y riesgos informáticos	Fortalecer la cultura del Hospital Universitario de Sincelejo ESE FUSIONADO en la seguridad de la información para funcionarios de planta, contratista, pasantes y sub-contratistas promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos a través de la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.	Líderes de Sistemas de cada una de las sedes	01/06/2024	31/08/2024

10. RIESGOS Y CONTROLES

A continuación se realiza una descripción de riesgos a los que se expone la entidad al no implementar un Plan de Plan Estratégico de Seguridad de la Información.

Riesgos	Controles
Ausencia de políticas TICs	Existencia, implementación, desarrollo y evaluación de un Plan Estratégico de Seguridad de la Información
Falta de conocimiento y aplicación sobre las policitas TICS	
Falta de continuidad de los procesos asistencias y administrativos.	
Falta de confidencialidad, integridad y disponibilidad de la información	

11. CONTROL DE CAMBIOS

Fecha del Cambio	Versión	Descripción del Cambio	Responsable
17/01/2024	1	Creación documento bajo un sistema integrado de gestión de calidad	Oriana Corrales Peñates – Gestor TICS