CONTENIDO

1. DERECHOS DE AUTOR 3

2. AUDIENCIA 3

3. INTRODUCCION 3

Objetivo General 4

Objetivos Específicos 4

4. ALCANCE 5

5. MARCO LEGAL 5

6. ROLES Y RESPOSABILIDADES 6

5.1 Área de sistemas 6

5.2 Oficina asesora jurídica 6

5.3 Gestión del talento humano 7

5.4 Control interno 7

7. CONOCIMIENTO DE LA ESE 7

6.1 Misión 7

6.2 Visión 8

6.3 Principios organizacionales 8

6.4 Valores organizacionales 9

6.5 Objetivos estratégicos 9

8. MODELO DE SEGURIDAD MSPI 10

7.1 Diagnostico 11

7.1.1 Evaluaciones FURAG 11

7.2 Planificación 16

7.3 Implementación 17

7.4 Evaluación de desempeño 18

7.5 Mejora continua 18

9. GLOSARIO 19

10. REFERENCIAS 24

11. MODIFICACIONES 24

12. APROBACIÓN 24

1. DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en el compendio de las normas técnicas colombianas NTC ISO/IEC 27000 vigentes, así como a los anexos con derechos reservados por parte de ISO/ICONTEC

2. AUDIENCIA

El Modelo de Privacidad y Seguridad de la Información está orientado a la **ESE HOSPITAL SAN JUAN DE DIOS DE YARUMAL** y son de obligatorio cumplimiento en los procesos que sean referenciados en el Alcance y por todos los servidores públicos, proveedores, ciudadanos, terceros y demás personas vinculadas que hacen parte de dichos procesos.

3. INTRODUCCION

El objetivo del Modelo de Seguridad y Privacidad de la Información - MSPI es capacitar a la organización para mantener la privacidad, integridad y disponibilidad de la información, asegurando así la privacidad de los datos.
a través de la implementación de un proceso de gestión del riesgo que proporcione seguridad a los involucrados en la correcta administración de riesgos.

La **ESE HOSPITAL SAN JUAN DE DIOS DE YARUMAL**, mediante la puesta en marcha de un modelo de seguridad y privacidad de la información, aspira a asegurar el logro de los objetivos fundamentales y la misión de la institución. Esto abarca la propia transparencia de la administración pública, y la entidad dicta las directrices para implementar las mejores prácticas de seguridad para evitar incidentes de efecto adverso, reconociendo la infraestructura esencial en la entidad. Además, fomenta un intercambio más efectivo de la información pública, respetando las leyes vinculadas a la salvaguarda de datos personales, consiguiendo el respeto a los derechos de los propietarios de los datos (privacidad) y mejorando el trabajo de acceso a la información pública.

La organización y puesta en marcha del Modelo de Seguridad y Privacidad de la Información - MSPI, en la organización, se encuentra determinada por las metas y objetivos, los requerimientos de seguridad, los procedimientos misioneros y la magnitud y organización de la Entidad.

Este documento se diseñó siguiendo las directrices del Ministerio de las TIC en el contexto de la estrategia de Tecnologías de la Información, conocido como Modelo de Seguridad y Privacidad de la Información. Este modelo incluye la recolección de las mejores prácticas a nivel nacional e internacional para el diagnóstico, planificación, ejecución, administración y mejora constante del MSPI; además, para mantenerse en consonancia con las mejores prácticas de seguridad, se adoptaron como referencia un conjunto de
que el Ministerio de las TIC dispone.

Para la creación de todos los productos y entregables de las distintas fases del ciclo de vida del MSPI, se utilizan como guías e instructivos proporcionados por el Ministerio de las TIC, junto con los documentos del marco de referencia de Arquitectura Empresarial.

Objetivo General

Definir las directrices, procesos y controles para asegurar la gestión, y supervisión de la seguridad y privacidad de los datos de la ESE HOSPITAL SAN JUAN DE DIOS DE YARUMAL

Objetivos Específicos

- Ofrecer directrices para la puesta en marcha de la administración de la seguridad y privacidad de los datos.
- Asignar funciones y responsabilidades para asegurar la protección y confidencialidad de la información.
- Fomentar la implementación de prácticas óptimas de seguridad de la información, como medida para la implementación del concepto de Seguridad Digital.
- Alinear el Modelo de Seguridad y Privacidad de la Información con el Marco de Referencia de Arquitectura Empresarial de TI.
- Ofrecer directrices para la aplicación de mejores prácticas de seguridad que aseguren la privacidad, privacidad y acceso a la información.

- Orientar a la Entidad para la elaboración de una política de privacidad que respete los datos personales de los titulares.
- Optimizar la gestión de la información al interior ESE HOSPITAL SAN JUAN DE DIOS DE YARUMAL.
- Contribuir al aumento de la claridad en la administración pública.
- Gestionar los riesgos de seguridad digital con el objetivo de aumentar la confianza de los diversos interesados en la utilización del ambiente digital y en la protección de los recursos de información de la ESE.

4. ALCANCE

Este Plan de Seguridad y Privacidad de la Información, aplica a todos los funcionarios de la ESE HOSPITAL SAN JUAN DE DIOS DE YARUMAL, a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad y terceras partes, que usen activos de información que sean propiedad de la Empresa.

5. MARCO LEGAL

Con el objeto de mitigar los riesgos relacionados con la autenticidad, la integridad, la disponibilidad, la confidencialidad y la trazabilidad de la información, se debe prever cualquier incidente que viole el marco normativo legal vigente en Colombia, en materia de políticas de seguridad de la información, entre otras, a lo establecido en las siguientes disposiciones legales: Marco normativo de buenas prácticas para el tratamiento de la información:

- Ley 527 de 1999 Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se dictan otras disposiciones.
- Ley 1273 de 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- Ley 1952 de 2019 Por medio de la cual se expide el Código General Disciplinario, se derogan la Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011, relacionadas con el derecho disciplinario.
- Decreto Nacional 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto Nacional 103 de 2015 Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto Mintic 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 Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Recomendaciones y buenas prácticas de los estándares adoptadas por el ICONTEC NTC/ISO 27001 y NTC/ISO 27002.

6. ROLES Y RESPOSABILIDADES

5.1 Área de sistemas

Es responsabilidad del área de TIC´s de la ESE HOSPITAL SAN JUAN DE DIOS DE YARUMAL, la implementación, aplicación, seguimiento y autorizaciones por parte de los directivos y comité del Modelo de Seguridad y Privacidad de la Información en las diferentes áreas y procesos de la Entidad, además garantiza el apoyo y el uso de la Política de Seguridad de la información como parte de su herramienta de gestión, la cual debe ser aplicada de forma obligatoria por todos los funcionarios para el cumplimiento de los objetivos misionales de la empresa.

5.2 Oficina asesora jurídica

- Ofrecer orientación a los procedimientos de la entidad en asuntos legales y jurídicos que requieran acciones ante las autoridades pertinentes vinculadas a la seguridad y privacidad de la información.
- Ofrecer orientación al Comité Institucional de Gestión y desempeño institucional sobre asuntos normativos, legales y jurídicos actuales que requieran acciones ante las autoridades pertinentes vinculadas a la seguridad y privacidad de la información.

- Comprobar que los contratos o acuerdos de ingreso que por competencia sean susceptibles de suscribir los procesos, posean cláusulas de derechos de autor.
  confidencialidad y omisión de la información, dependiendo del caso, según sea el caso.
- Representar a la organización en procedimientos legales frente a las autoridades pertinentes vinculadas con la seguridad y privacidad de la información.
- Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.

5.3 Gestión del talento humano

- Controlar y salvaguardar la información de datos personales del personal de planta de la entidad, en concordancia con la normatividad vigente
- Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.

5.4 Control interno

La Oficina de control interno es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de este modelo de seguridad y privacidad de la información establecidos por este modelo y por las normas, procedimientos y prácticas que de ella surjan

7. CONOCIMIENTO DE LA ESE

6.1 Misión

Somos un Hospital referente en la Subregión Norte del departamento de Antioquia, comprometido con el mejoramiento de la salud de la población de Yarumal y municipios inmediatos. Brindando atención médica integral y accesible en servicios de baja y mediana complejidad, priorizando un enfoque humanizado que satisface las necesidades de los usuarios y sus familias. Nuestro compromiso es promover el

bienestar a través de prácticas médicas actualizadas, el uso de tecnología de innovación y un talento humano competente, garantizando así una mejor calidad de vida en las comunidades.

6.2 Visión

Para el año 2028 la ese Hospital San Juan de Dios de Yarumal será una institución líder en la prestación de servicios de salud de baja y mediana complejidad; humanizada, íntegra, reconocida por sus resultados, con altos estándares de calidad en sus servicios, competitiva, sostenible financieramente, con un excelente talento humano. Guiada por principios de responsabilidad social, comprometida con el desarrollo tecnológico y la mejora continua.

6.3 Principios organizacionales

- **Calidez Humana:** Es el principio fundamental a implementar por todos los colaboradores del Hospital para fortalecer la empatía, relacionamiento y acompañamiento con los usuarios y familiares que acceden a los diferentes servicios en salud.
- **Eficiencia:** Es la mejor utilización social y económica de los recursos administrativos, técnicos y financieros disponibles para una oportuna, adecuada y suficiente prestación de los servicios en salud.
- **Accesibilidad:** Es la posibilidad que tienen los usuarios para acceder a los servicios de salud desde la diversidad de enfoques diferenciales.
- **Oportunidad:** Es la posibilidad que tienen los usuarios de obtener servicios que requieren en el menor tiempo posible sin retrasos que pongan en riesgo su vida o su salud.
- **Integralidad:** Los servicios de salud en la E.S.E Hospital San Juan de Dios de Yarumal se brindan de manera pertinente y de alta calidad centrados en el usuario y su familia, mediante la secuencia lógica y racional de actividades basadas en el conocimiento científico y sin interrupciones innecesarias, permitiendo una interacción responsable, consciente y colaborativa entre los pacientes, sus cuidadores y el personal asistencial.
- **Participación social:** Establece el compromiso de la Institución, de involucrarse en iniciativas comunitarias para mejorar la salud y el bienestar integral de la población. Esto implica colaborar en programas de prevención, educación y promoción de la salud.
- **Liderazgo:** Es la capacidad constante de mejoramiento continuo para dar respuesta a los retos y necesidades de servicios en salud en el territorio,

inspirando colaborativamente a diferentes actores y a la organización, para el cumplimiento de las metas propuestas.

- **Innovación:** Fomentar la adopción de nuevas tecnologías y enfoques para mejorar la eficacia del cuidado y la eficiencia operativa.

6.4 Valores organizacionales

Humanidad: Abarca el compromiso genuino de tratar a cada paciente con respeto, empatía y dignidad. Este valor enfatiza la importancia de conectar con las personas a un nivel emocional, brindando atención integral que reconoce sus necesidades físicas, emocionales y sociales. Al fomentar un ambiente humano, se promueve un servicio cálido y acogedor, donde cada individuo se siente valorado y apoyado en su proceso de atención médica.
Calidad: Ofrecer una atención que cumpla con altos estándares de eficacia y seguridad. Implica el uso de prácticas basadas en evidencia, la capacitación continua del personal y la mejora constante de los servicios.
Servicio: Promover la empatía, la comunicación efectiva y la resolución de problemas, creando un ambiente de confianza y respeto en el que la comunidad se siente valorada y bien atendida.
Inclusión: Permitir el acceso equitativo a los servicios de salud para todas las personas, sin importar su origen, condición socioeconómica o características individuales. Implica crear un entorno donde cada paciente se sienta bienvenido y valorado, garantizando que las barreras físicas, sociales y culturales sean eliminadas. Al fomentarla, el Hospital se compromete a ofrecer atención accesible y de calidad, asegurando que todos los miembros de la comunidad puedan participar plenamente en su cuidado y bienestar.
Integridad: es un elemento central de la construcción de capital social y de generación de confianza de la ciudadanía con las Empresas Sociales del Estado. La integridad es una característica personal, que en el sector público también se refiere al cumplimiento de la promesa que cada servidor le hace al Estado y a la ciudadanía de ejercer a cabalidad su labor con compromiso, respeto, honestidad, diligencia y justicia.

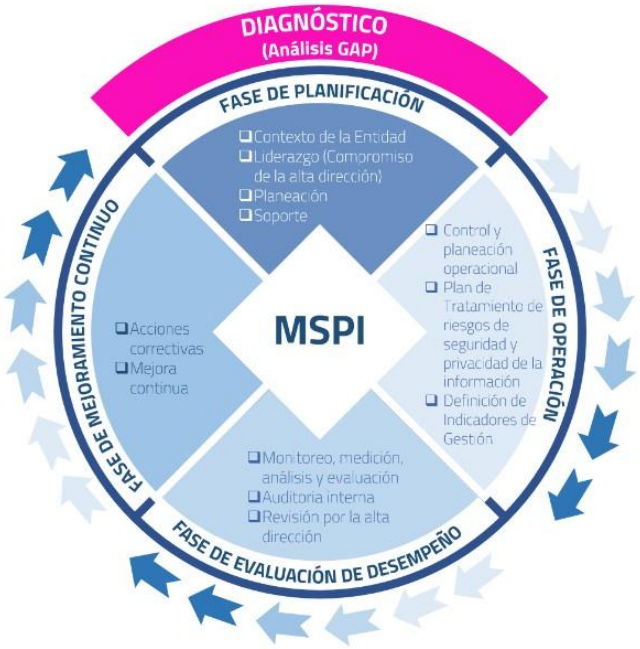
6.5 Objetivos estratégicos

- Inspirar en la E.S.E Hospital San Juan de Dios de Yarumal el respeto por la dignidad humana, desarrollando el potencial integral del talento humano dentro de una cultura del servicio y acompañamiento entre todos los grupos de valor.

- Optimizar las capacidades organizacionales de la E.S.E Hospital San Juan de Dios de Yarumal con la implementación de herramientas de gestión que fortalezcan el desempeño institucional, la sostenibilidad económica y el buen gobierno.
- Prestar servicios de salud íntegros, oportunos y sostenibles centrados en el paciente, con adhesión a guías y protocolos basados en evidencia científica, en una infraestructura renovada que posibilite la alta complejidad, buscando siempre mejorar la calidad de vida de la población atendida.
- Modernizar tecnológicamente la E.S.E Hospital San Juan de Dios de Yarumal para el fortalecimiento sus capacidades de interacción en el mercado de la salud, mejorando la competitividad de sus procesos desde la innovación y gestión el conocimiento.

8. MODELO DE SEGURIDAD MSPI

El modelo de seguridad y privacidad de MSPI de la estrategia de gobierno digital explora los siguientes ciclos de acción, que incluyen cinco (5) pasos para permitir que las entidades gestionen adecuadamente la seguridad y la privacidad de sus activos de información.



Fuente: Mintic https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

7.1 Diagnostico

En esta etapa se determina el estado presente de la **ESE HOSPITAL SAN JUAN DE DIOS DE YARUMAL** en relación con las exigencias del Modelo de Seguridad y Privacidad de la Información.

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad.

7.1.1 Evaluaciones FURAG

Plan de mejora que se dio al hacer la evaluación del **FURAG** vigencia 2023.

POLÍTICAS DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL		
POL08: SEGURIDAD DIGITAL		
RECOMENDACIONES	**ALTERNATIVA DE MEJORA**	**MEJORA A IMPLEMENTAR (PLAZOS)**
Almacenar las copias de respaldo en un lugar aislado, en un segmento diferente de red a la de servidores y equipos.	DISEÑAR ESTRATEGIAS PARA CUSTODIAR LA INFORMACIÓN DE LA INSTITUCIÓN.	LIDER SISTEMAS – GESTIÓN DOCUMENTAL
Contar con un Plan de Recuperación de Desastres DRP, definido, documentado e implementado para todos los procesos.	ACTUALIZAR PETI Y VINCULAR PROCEDIMIENTO.	LIDER SISTEMAS
Designar un área o responsable de la seguridad digital.	DIALOGAR CON GERENCIA PARA SEÑALAR RESPONSABILIDADES.	LIDER SISTEMAS – ALTA DIRECCIÓN
Implementar el Modelo de Seguridad y Privacidad de la Información (MSPI).	DOCUMENTAR EL MODELO	LIDER SISTEMAS – CALIDAD.
Realizar análisis de vulnerabilidades para Portal Web, Sede electrónica y Servicios expuestos en Internet.	SE REALIZAN ACCIONES DE SEGURIDAD PERIMETRAL, ANTIVIRUS Y NIVEL ABSTRACCIÓN DEL SISTEMA (PERFILES). CONTINUAR AVANZANDO.	LIDER SISTEMAS
Realizar análisis de vulnerabilidades de seguridad a los activos de información de su infraestructura en Nube Pública/Privada.	SE REALIZAN AYUDAS DIAGNOSTICAS. NECESARIO IMPLEMENTAR SUIT	LIDER SISTEMAS – ÁREA SIAU
Realizar análisis de vulnerabilidades de seguridad a los activos de información en su infraestructura On Premise.	CONOCER LA MATERIA Y EMPEZAR A IMPLEMENTAR	LIDER SISTEMAS
Realizar pruebas de respaldo a las copias de seguridad de la información de los aplicativos misionales, estratégicos, soporte y de mejora, de manera programada para asegurar la disponibilidad de los datos en caso de Ransomware, de manera coordinada con los responsables del proceso.	DAR INICIO A PERIODOS DE PRUEBAS. CAPACITAR EL PERSONAL DE LA ENTIDAD.	LIDER SISTEMAS
Separar los equipos que realizan las copias de respaldo de la información, del software e imágenes de los sistemas de la red de servidores y computadores.	SE CUENTA CON DOS SERVIDORES NAS ALMACENAN INFORMACIÓN – COPIAS. PROYECTAR CON	LIDER SISTEMAS

	GERENCIA LA CUSTODIA DE LA INFORMACIÓN.	
Tener documentados e implementados procedimientos para copias de respaldo y de restauración de la información, del software e imágenes de los sistemas.	DOCUMENTAR PROCEDIMIENTO.	LIDER SISTEMAS - CALIDAD
Verificar y asegurar que los proveedores y contratistas de la entidad cumplan con las políticas de ciberseguridad internas.	CAPACITAR A GRUPOS DE INTERES DE LA INSTITUCIÓN.	LIDER SISTEMAS

POLÍTICAS DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL		
POL07: GOBIERNO DIGITAL		
RECOMENDACIONES	**ALTERNATIVA DE MEJORA**	**CADENA DE RESPONSABILIDAD**
Automatizar los trámites inscritos por la entidad en el Sistema Único de Información de Trámites (SUIT).	REALIZAR MESA DE TRABAJO CON PROCESO DE SIAU PARA SINCRONIZAR ACCIONES PERTINENTES AL PROCEDIMIENTO.	LIDER SISTEMAS - SIAU
Capacitar a los contratistas de la entidad en temáticas de la Política de Gobierno Digital.	ACTUALIZAR POLÍTICA Y REALIZAR MESA DE TRABAJO CON PROCESO DE TALENTO HUMANO PARA VINCULAR ACCIONES.	LIDER SISTEMAS – TALENTO HUMANO
Capacitar a los grupos de valor e interés en el uso de los medios digitales dispuestos para acceder a la oferta institucional y para interactuar con la entidad, en temáticas como acceso a información publicada en la sede electrónica; uso de canales de atención virtual; gestión de PQRSD a través de la sede electrónica; acceso a trámites y servicios digitales dispuestos por la entidad a través de su sede electrónica; participación en la gestión institucional a través de medios digitales; entre otras.	ACTUALIZAR POLÍTICA Y REALIZAR MESA DE TRABAJO CON PROCESO DE TALENTO HUMANO PARA VINCULAR ACCIONES.	LIDER SISTEMAS – SIAU – TALENTO HUMANO
Capacitar a los servidores públicos de la entidad en temáticas de la Política de Gobierno Digital.	ACTUALIZAR POLÍTICA Y REALIZAR MESA DE TRABAJO CON PROCESO DE TALENTO HUMANO PARA VINCULAR ACCIONES.	LIDER SISTEMAS – TALENTO HUMANO
Caracterizar los usuarios de los trámites total o parcialmente en línea de la entidad.	ACTUALIZAR PÁGINA WEB Y REALIZAR SEGUIMIENTO A SUS MOVIMIENTOS.	LIDER SISTEMAS
Digitalizar los trámites inscritos por la entidad en el Sistema Único de Información de Trámites (SUIT).	REALIZAR MESA DE TRABAJO CON PROCESO DE SIAU PARA SINCRONIZAR ACCIONES PERTINENTES AL PROCEDIMIENTO.	LIDER SISTEMAS
Disponer en línea los Otros Procedimientos Administrativos (OPAS) de la entidad inscritos en el Sistema Único de Información de Trámites (SUIT).	REALIZAR MESA DE TRABAJO CON PROCESO DE SIAU PARA SINCRONIZAR ACCIONES PERTINENTES AL PROCEDIMIENTO.	LIDER SISTEMAS
Disponer en línea los trámites de la entidad inscritos en el Sistema Único de Información de Trámites (SUIT).	REALIZAR MESA DE TRABAJO CON PROCESO DE SIAU PARA SINCRONIZAR ACCIONES PERTINENTES AL PROCEDIMIENTO.	LIDER SISTEMAS
Evaluar la implementación de lineamientos en materia de datos en la entidad.	REALIZAR ENCUESTAS ENTRE LOS COLABORADORES PARA MEDIR EL DESEMPEÑO DE LOS DATOS INSTITUCIONALES.	LIDER SISTEMAS

Formular, aprobar en el Comité de Gestión y Desempeño Institucional, incluir en el Plan Estratégico de Tecnologías de la Información de la entidad y ejecutar proyectos de transformación digital.	ACTUALIZAR PLAN Y PRESENTARLO AL COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO.	LIDER SISTEMAS
Generar o actualizar los conjuntos de datos abiertos propios de la entidad.	ACTUALIZAR PÁGINA WEB	LIDER SISTEMAS
Habilitar funcionalidades que permitan a los usuarios hacer seguimiento en línea del estado de los trámites total o parcialmente en línea de la entidad.	ACTUALIZAR PÁGINA WEB	LIDER SISTEMAS
Hacer uso de estrategias como cursos en línea dispuestos en su sede electrónica, talleres o capacitaciones virtuales o presenciales, entre otras, para capacitar a los grupos de valor e interés en el uso de los medios digitales dispuestos para acceder a la oferta institucional y para interactuar con la entidad.	ACTUALIZAR PAGINA WEB Y VINCULAR ACCIONES PERTINENTES.	LIDER SISTEMAS
Identificar cuáles de los datos maestros de la entidad son datos de referencia.	AVANZAR EN EL CARGUE DE INFORMACIÓN EN LA PÁGINA WEB	LIDER SISTEMAS
Implementar acciones para que los trámites total o parcialmente en línea de la entidad cumplan con todos los criterios de usabilidad web.	ACTUALIZAR PÁGINA WEB	LIDER SISTEMAS
Implementar estrategias de mejora de los trámites parcialmente en línea de la entidad para aumentar el número de usuarios satisfechos con su uso.	ACTUALIZAR PÁGINA WEB	LIDER SISTEMAS
Incluir a grupos de valor e interés como la ciudadanía, sociedad civil, academia, sector privado, entre otros, en ejercicios de participación para la toma de decisiones sobre la implementación de la Política de Gobierno Digital en la entidad.	REALIZAR MESA DE TRABAJO CON PROCESO DE SIAU PARA SINCRONIZAR ACCIONES PERTINENTES AL PROCEDIMIENTO.	LIDER SISTEMAS - SIAU
Publicar en la sección transparencia y acceso a la información pública del portal web información actualizada sobre.	ACTUALIZAR PÁGINA WEB	LIDER SISTEMAS
Publicar en la sección transparencia y acceso a la información pública del portal web información actualizada sobre datos abiertos, para lo cual deberán contemplar las excepciones establecidas en el título 3 de la presente ley.	ACTUALIZAR PÁGINA WEB	LIDER SISTEMAS
Publicar en la sección transparencia y acceso a la información pública del portal web información actualizada sobre directorio de entidades del sector,	ACTUALIZAR PÁGINA WEB	LIDER SISTEMAS

agremiaciones, asociaciones, entidades del sector, grupos étnicos y otros grupos de interés.		

7.2 Planificación

En esta etapa se establecen las actividades y procesos que el plan de seguridad y privacidad de la información ha establecido para la entidad. Este plan debe estar en consonancia con el propósito misional institucional e incluir las medidas a nivel de seguridad y privacidad de la información, empleando un método de administración del riesgo.

Para esta etapa, la Entidad tiene que determinar el alcance del MSPI, estableciendo los límites en los que se aplicará la seguridad y privacidad de la información en la Entidad, con una perspectiva basada en procesos.

Para llevar a cabo la etapa, la entidad debe desarrollar actividades y estrategias considerando los procesos que influyen en la realización de los objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros vinculados e interacciones del MSPI con otros procesos.

Los objetivos y resultados esperados de la fase de Planeación son:

OBJETIVOS	RESULTADOS
Automatizar los trámites inscritos por la entidad en el Sistema Único de Información de Trámites (SUIT).	Registro de toda la información requerida en el SUIT y actualización del mismo.
Capacitar a los contratistas y servidores públicos de la entidad en temáticas de la Política de Gobierno Digital.	Realización de capacitaciones
Capacitar a los grupos de valor e interés en el uso de los medios digitales	Realización de capacitaciones
Evaluar la implementación de lineamientos en materia de datos en la entidad.	Realización de encuestas
Plan Estratégico de Tecnologías de la Información de la entidad y ejecutar proyectos de transformación digital.	Actualización del plan estratégico
Actualizar Pagina web	Actualización de página web y nuevas funcionalidades
Realizar copias de seguridad de la información de la entidad	Realización de copias con su respectivo formato de evidencia
Contar con plan de recuperación de desastres	Actualización del PETI y creación del plan de recuperación de desastres

Designar responsable de la seguridad digital	Designación de área o personal responsable de la seguridad digital
Implementar modelo de seguridad y privacidad de la información	Creación de modelo
Realizar análisis de vulnerabilidades, a los servicios internos y servicios expuestos a internet	Realización de pruebas de vulnerabilidades
Segmentar equipos de la red principal	Realización de segmentación
Capacitar al personal del hospital en temas de seguridad digital	Realización de capacitaciones

7.3 Implementación

En esta etapa, la entidad tiene que planear, poner en marcha y supervisar los procedimientos requeridos para satisfacer los requisitos de seguridad y privacidad de la información, lo que le facilite la ejecución de las acciones establecidas en el plan de gestión de riesgos. La entidad debe contar con pruebas documentadas de los procedimientos realizados de acuerdo a lo previsto, además, debe poseer un control de modificaciones que le facilitarían tomar medidas para atenuar efectos adversos cuando se requiera.

Para esta etapa, la entidad tiene la obligación de poner en marcha el plan de gestión de riesgos de seguridad de la información, donde se determina el control a implementar para reducir cada uno de los riesgos a un nivel que sea aceptable para ella. Es importante recordar que la implementación de los controles sobre los riesgos identificados necesita la aprobación del líder de cada procedimiento y del Comité Institucional de Seguridad y Privacidad de la ESE.

La entidad debe definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información.
Algunos indicadores a medir:

- Efectividad en los controles.
- Eficiencia del MSPI al interior de la entidad.
- Proveer estados de seguridad que sirvan de guía en las revisiones y la mejora continua.
- Comunicar valores de seguridad al interior de la entidad.
- Servir como insumo al plan de control operacional.

Objetivos

Poner en marcha de todos los procesos mencionados en la fase de planeación.

Resultados

Evidencias documentas de la implementación de todos los procesos necesarios para el gobierno digital y seguridad digital de la ESE y asi cumplir con la normativa vigente.

7.4 Evaluación de desempeño

En esta etapa es necesario establecer los procedimientos de monitoreo y seguimiento para la puesta en marcha del MSPI, basándose en los resultados obtenidos por los indicadores de seguridad de la información, con el fin de confirmar la efectividad, eficiencia y efectividad de las acciones ejecutadas por la Entidad en relación al MSPI.

En esta fase, la Entidad debe crear un plan que contemple las siguientes actividades:

- Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
- Seguimiento a la programación y ejecución de las actividades de auditorías internas y externas del MSPI.
- Seguimiento al alcance y a la implementación del MSPI.
- Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
- Revisiones de acciones o planes de mejora

Objetivos

- Revisar y hacer seguimiento a la implementación del MSPI
- Ejecutar auditorías.

Resultados

- Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por el Comité Institucional de Seguridad y Privacidad del ESE.
- Documento con el plan de ejecución de auditorías, revisado y aprobado por la Alta Dirección.

7.5 Mejora continua

En esta etapa, la organización necesita consolidar los resultados logrados en la etapa de evaluación de desempeño, con el fin de elaborar el plan de mejora constante en seguridad y privacidad de la información, implementando las medidas adecuadas para minimizar las debilidades detectadas.

En esta fase la entidad debe definir y haber ejecutado el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño.

- Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.
- Resultados del plan de ejecución de auditorías al MSPI.
- La Entidad debe efectuar los ajustes a los entregables, controles y procedimientos del MSPI. Dando como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por el Comité Institucional de Seguridad y Privacidad de la ESE.

Objetivos

- Mejorar y retroalimentar de manera continua
- Capacitar en temas de interés

Resultados

- Evidencias de las mejoras continuas
- Comunicación constante con las partes involucradas en el proceso

9. GLOSARIO

Acceso a los Datos Públicos:

Derecho esencial que implica la capacidad de todos los individuos para conocer la existencia y acceder a la información pública que está en manos o bajo el control de entidades obligadas. (Artículo 4 de la Ley 1712 de 2014).

Activo:

Respecto a la seguridad de la información, hace referencia a cualquier datos o componente vinculado con su manejo (sistemas, soportes, edificios, personas...) que represente un valor para la organización. (ISO/IEC 27000).

Activo de Información:

Respecto a la privacidad de la información, hace referencia al recurso que alberga datos públicos que el individuo responsable genere, obtenga, adquiera, modifique o supervise en su calidad de tal.

Archivo:

Conjunto de documentos, independientemente de su fecha, forma y medio material, acumulados en un proceso natural por un individuo o entidad pública o privada, durante su administración, mantenidos en ese orden para servir como prueba e información a la persona o institución que los genera y a los ciudadanos, o como fuentes de la historia. Además, puede interpretarse como la entidad encargada de la administración, la información, la investigación y la cultura. (Ley 594 de 2000, art3)

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:

Procedimiento sistemático, autónomo y registrado para recopilar pruebas de auditoría y, obviamente, para establecer el nivel en el que se satisfacen los criterios de auditoría. (ISO/IEC 27000).

Autorización:

Permiso previo, explícito e informado del titular para realizar el procesamiento de datos personales (Ley 1581 de 2012, artículo 3).

Bases de Datos Personales:

Conjunto ordenado de información personal que sea objeto de tratamiento (Artículo 3 de la Ley 1581 de 2012).

Ciberseguridad:

Capacidad del Estado para reducir el grado de peligro al que se encuentran sometidos los ciudadanos, frente a amenazas o sucesos de índole cibernética.

Ciberespacio:

Se refiere al entorno físico y virtual que incluye ordenadores, sistemas informáticos, programas informáticos (software), redes de telecomunicaciones, datos e información que se emplea para la interacción entre los usuarios.

Control:

Las políticas, procedimientos, prácticas y estructuras organizativas ideadas para reducir los riesgos de seguridad de la información a un nivel inferior al nivel de riesgo aceptado. También se emplea el término control como sinónimo de protección o contramedida. En una versión más sencilla, se refiere a una medida que altera el riesgo.

Datos Abiertos:

Se refiere a todos los datos primarios o sin procesar, que se presentan en formatos estándar e interoperables que permiten su acceso y reutilización. Estos datos están custodiados por entidades públicas o privadas que desempeñan funciones públicas y están disponibles para cualquier ciudadano, de manera libre y

sin limitaciones, con el objetivo de que terceros puedan reutilizarlos y generar servicios derivados de estos.

Datos Personales:

Cualquier dato vinculado o que pueda estar relacionado con una o varias personas naturales específicas.

Datos Personales Públicos:

Es la información que no tenga un carácter semiprivado, privado o sensible. Se consideran datos públicos, entre otros, los datos relacionados con el estado civil de los individuos, su profesión u oficio, y su condición de comerciante o de funcionario público. Dado su carácter, los datos públicos pueden encontrarse, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, así como en fallos judiciales debidamente ejecutoriados que no se encuentren bajo 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 consideran datos delicados aquellos que comprometen la privacidad del Titular o cuyo mal uso puede provocar su discriminación, como aquellos que desvelen el origen racial o étnico, el enfoque político, las creencias religiosas o filosóficas, la afiliación a sindicatos, organizaciones sociales, de derechos humanos o que fomenten los intereses de cualquier partido político o que aseguren 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 lista los controles implementados por el Sistema de Gestión de Seguridad de la Información - SGSI, de la organización después de los procesos de evaluación y tratamiento de riesgos y su justificación, además de la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000)

Derecho a la Intimidad:

Derecho básico cuyo fundamento es la existencia y disfrute de una trayectoria única en cada individuo, libre de la intervención del poder estatal o de las intervenciones arbitrarias de la sociedad, que le brinda a dicho individuo la total realización 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:

Se refiere a la información que, al estar en poder o custodia de un individuo obligado en su condición de tal, pertenece al ámbito personal, individual y privado o semiprivado de una persona o entidad. Por lo tanto, su acceso podrá ser restringido o prohibido, siempre y cuando se trate de las circunstancias legítimas y necesarias y los derechos individuales o privados establecidos en el artículo 18 de la Ley 1712 de 2014. (artículo 6)

Información Pública Reservada:

Se refiere a la información que, al estar en poder o custodia de un individuo obligado en su calidad de tal, está prohibida de acceder a la ciudadanía por perjudicar los intereses públicos y bajo el cumplimiento de todos los requisitos establecidos en el artículo 19 de la Ley 1712 de 2014. (Artículo 6 de la Ley 1712 de 2014)

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.

MRAE:

Marco de Referencia Arquitectura Empresarial.

MSPI:

Modelo de Seguridad y Privacidad de la Información.

Mecanismos de protección de datos personales:

Lo representan las diversas opciones disponibles para las entidades receptoras para brindar protección a los datos personales de los titulares, como el acceso regulado, el anonimato o el 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 marco de este documento, se entiende por privacidad el derecho que poseen todos los propietarios de la información respecto a la información que concierne a datos personales y la información clasificada que estos hayan proporcionado o mantenido en manos de la entidad en el contexto de las responsabilidades que a ella le corresponde desempeñar. Esto genera en las entidades que reciben el Manual de GEL la constante obligación de salvaguardar dicha información conforme al marco legal en vigor.

Protocolo IPV4:

La versión 4 del Protocolo de Internet, es la cuarta versión del Protocolo de Internet (IP). Un protocolo de conexión de redes fundamentado en Internet, que se implementó por primera vez en la creación de ARPANET, en 1983. Como se define en el RFC 791

Protocolo IPv6:

Es la versión 6 del Protocolo de Internet (IP), responsable de guiar y encaminar los paquetes en la red. Su desarrollo comenzó en 1998 con la finalidad de conectar redes; fue creado para sustituir al Protocolo de Internet versión 4 (IPv4) RFC 791, que a partir de 2016 se está poniendo en práctica en la mayoría de dispositivos que utilizan Internet.

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 aplicada por los Responsables o Encargados del tratamiento de datos personales que, a solicitud de la Superintendencia de Industria y Comercio, deben tener la capacidad de evidenciar a dicha entidad de control que han puesto en marcha medidas adecuadas y eficaces para acatar lo estipulado en la Ley 1581 de 2012 y sus reglamentos correspondientes.

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, art3).

Riesgo:

Posibilidad que una amenaza específica pueda aprovechar una debilidad para provocar una pérdida o perjuicio en un recurso de información. Normalmente se percibe como una mezcla de la probabilidad de un suceso y sus repercusiones. (EN/ISO 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 SGS:

Conjunto de componentes interconectados o enlazados (estructura organizativa, políticas, organización de actividades, responsabilidades, procesos, procedimientos y recursos) que emplea una entidad para definir una política y metas de seguridad de la información y lograr estas metas, apoyándose en un enfoque de administración y mejora constante. (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 acción o grupo de acciones relacionadas con datos personales, como la recopilación, almacenaje, utilización, circulación o supresión. (Artículo 3 de la Ley 1581 de 2012).

Trazabilidad:

Calidad que posibilita que todas las acciones llevadas a cabo sobre la información o un sistema de gestión de la información estén indudablemente vinculadas a una persona o entidad. (EN/ISO 27000).

Vulnerabilidad:

Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

10. REFERENCIAS

- https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf
- https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/
- https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237907_maestro_mspi.pdf

11. MODIFICACIONES

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	29/04/2025	Creación documento

12. APROBACIÓN

ELABORÓ	REVISÓ	APROBACIÓN
Gustavo Adolfo Gomez Lopez	Yenny Alexandra Herrera	Daniel Alcides Vergara
Cargo: Auxiliar sistemas	Cargo: Coordinadora de Calidad	Cargo: Gerente