

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION



**SEGURIDAD Y
PRIVACIDAD DE
LA INFORMACIÓN**

ENERO 2023



POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

RTI-OT016

Versión:002
Fecha de emisión: 20/01/2022

1. OBJETIVO

Proteger la información de la E.S.E. Hospital Regional del Magdalena Medio teniendo en cuenta los principios de confidencialidad, integridad y disponibilidad de los datos y los activos.

2. ALCANCE

Comprende el modelo de seguridad y privacidad de la información que va desde la definición de las fases a desarrollar en el Plan hasta el cronograma establecido para la implementación de las guías correspondientes al de modelo establecido por el Ministerio TIC.

3. APLICABLE A

El plan de Seguridad y Privacidad de la Información aplica a todos los procesos Estratégicos, Misionales, de Apoyo y de Evaluación de la E.S.E Hospital Regional del Magdalena Medio.

4. RESPONSABLE

Subgerente Administrativa y Financiera
Profesional Especializado Unidad Funcional Subsistemas de Información

5. DEFINICIONES

- **Activo:** Se define como activo cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de Información:** Son todos los recursos representados en información que cada entidad recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentra en forma expresa escrita en papel, transmitida por cualquier medio electrónico o almacenada en equipos de cómputo incluyendo datos contenidos en registros, archivos, bases de datos, videos e imágenes.

Este tipo de activo representa los datos de la organización, información que tiene valor para los procesos del negocio, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil para la E.S.E. Hospital Regional del Magdalena Medio.

- **Amenaza:** Una causa potencial de ocurrencia de un incidente no deseado, el cual puede producir un daño a un sistema o a la Organización.
- **Autenticación:** Garantía de que una parte de una transacción informática no es falsa. La autenticación normalmente lleva consigo el uso de una contraseña, un certificado, un número de identificación personal u otra información que se pueda utilizar para validar la identidad en una red de equipos.
- **Comité de Calidad:** Instancia de nivel superior, que debe validar las políticas de seguridad de información, así como los procesos, procedimientos y metodologías específicas de seguridad de la información para el adecuado uso y administración de los recursos informáticos de la E.S.E Hospital Regional del Magdalena Medio.
- **Confidencialidad:** Propiedad de la información que determina que esté disponible solo a personas autorizadas.
- **Control de acceso:** Es el proceso de conceder permisos a usuarios o grupos de acceder a objetos datos tales como documentos carpetas e impresoras en la red.
- **Copia de respaldo:** Es un duplicado de nuestra información más importante, que realizamos para salvaguardar los documentos, archivos, fotos, etc., de nuestro ordenador.
- **Datos:** Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la E.S.E Hospital Regional del Magdalena Medio.
- **Dato Personal:** Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley.
- **Dato público:** 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.

- **Dato semiprivado:** Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.
- **Dato privado:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
- **Dato sensible:** 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.
- **Disponibilidad:** Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.
- **Evento de Seguridad de la Información:** Se considera un evento de seguridad de la información a cualquier situación identificada que indique una posible brecha en la política de seguridad y confidencialidad de la información o falla en los controles y/o protecciones establecidas.
- **Incidente de Seguridad de Información:** Se considera como incidente de seguridad de información, un acceso, el uso, divulgación, modificación o destrucción no autorizada de la información de la E.S.E Hospital Regional del Magdalena Medio y de sus usuarios, un impedimento en la operación normal de las redes, sistemas informáticos o cualquier otro que implique una violación a la política de seguridad informática.
- **Integridad:** Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento deben ser exactos.
- **MSPI: Modelo** de Seguridad y Privacidad de la Información.
- **Política de seguridad:** Es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad de la información.
- **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 [NTC-ISO/IEC 27000:2013]

- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas. [NTC-ISO/IEC 27002:2013]
- **Sistema de Información:** conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos.
- **Tratamientos de Datos:** Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consulta, interconexiones y transferencias.

6. CONDICIONES GENERALES

- Toda persona que ingrese a laborar en el área administrativa o asistencial de la E.S.E Hospital Regional del Magdalena Medio debe solicitar la creación de usuario al sistema de información a través del Formato Solicitud Usuario a Red y Acceso Aplicativo (MEDISOFT).
- Es responsabilidad de los usuarios identificar y cumplir las políticas de seguridad de la información de la E.S.E. Hospital Regional del Magdalena Medio.
- Los colaboradores de la E.S.E. Hospital Regional del Magdalena deben realizar el proceso de inducción en el manejo del aplicativo.

7. DESARROLLO

La E.S.E Hospital Regional del Magdalena Medio estructura el Plan de Seguridad y Privacidad de la Información en concordancia con los marcos legales y conceptuales del Estado relacionadas con la Seguridad y Privacidad de la Información, lo cual permite cumplir con el objetivo definido en este Plan, para esto se definen las siguientes fases:

• Fase I Diagnostico

Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

• Fase II Planificación (Planear)

Hace referencia a establecer el Modelo de Seguridad y Privacidad de la Información, en esta fase se debe establecer la política, los objetivos, procesos y

procedimientos de seguridad pertinentes para gestionar los activos y el riesgo buscando mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de la entidad.

• **Fase III Implementación (Hacer):**

Hace referencia a implementar u operar el MSPI, en esta fase se debe implementar y operar la política, los controles y procedimientos del MSPI.

• **Fase IV Evaluación de Desempeño (Verificar)**

Hace referencia a hacer seguimiento y revisión del MSPI, en esta fase se debe evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.

• **Fase V Mejora Continua (Actuar)**

Hace referencia a mantener y mejorar el MSPI, en esta fase de debe emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del MSPI y la revisión por la dirección, para lograr la mejora continua del MSPI.

La E.S.E. Hospital Regional del Magdalena Medio establece un cronograma de trabajo para un periodo de dos años (2022-2023) para la implementación de las guías del modelo de seguridad y privacidad de la información establecidas por el MINTIC.

Primer Año 2022			
Meta	Instrumento a utilizar	Tiempo	Fase
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad	Guía N°1: Herramienta de Diagnóstico del MSPI de MINTIC	Febrero - Abril	Fase I Diagnóstico
Identificar el nivel de madurez de seguridad y privacidad de la información en la entidad			
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.			
Política de Seguridad y Privacidad de la Información	Guía N°2: Política General MSPI	Abril - Mayo	Fase II
Procedimientos de seguridad de la información	Guía N°3: Procedimientos de Seguridad y Privacidad de la Información	Junio -Noviembre	
Roles y responsabilidades de seguridad y privacidad de la información	Guía N°4: Roles y responsabilidades de seguridad y privacidad de la información	Marzo - Mayo	
Segundo Año 2023			
Meta	Instrumento a utilizar	Tiempo	Fase
Integración del MSPI con el Sistema de Gestión documental	Guía N°6: Gestión Documental	Diciembre	Fase III Implementación
Implementación del plan de Tratamiento de riesgos	Guía N°7: Gestión de Riesgos	Marzo - Mayo	
Indicadores De Gestión	Guía N°9: Indicadores de Gestión SI	Marzo	
Plan de revisión y Seguimiento, a la implementación del MSPI	Guía N°16: Evaluación del desempeño	Julio - Noviembre	Fase IV Evaluación De Desempeño
Plan de Ejecución de Auditorías	Guía N°15: Guía de Auditoría	Julio - Noviembre	
Plan de mejora continua	Guía N°18: Mejora Continua	Junio, Diciembre primer año Junio	Fase V Mejora Continua

	POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	RTI-OT016
	Versión:002 Fecha de emisión: 20/01/2022	

Inventario de activos de información	Guía N°5: Gestión De Activos Guía N°20: Transición Ipv4 a Ipv6	Junio - Septie	Planificación
Identificación, Valoración y tratamiento de riesgo	Guía N°7: Gestión de Riesgos Guía N°8: Controles de Seguridad	Octubre - Dicie	
Plan de Comunicaciones	Guía N°14: Plan de comunicación,	Noviembre -	
Plan de diagnóstico de IPv4 a IPv6	Guía N°20: Transición IPv4 a IPv6	Octubre - Dicie	
Plan de Transición de IPv4 a IPv6	Guía N°19: Aseguramiento de protocolo IPv4_IPv6 Guía N°20: Transición Ipv4 a Ipv6	Diciembre	Fase III Implementación

8. DOCUMENTOS DE REFERENCIA

- Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Decreto 2578 de 2012: Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye “El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles” entre otras disposiciones.
- Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000.
 - Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.
- 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.
- 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.

- Decreto 612 de 2018: Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Norma ISO 27001: Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información.
- Modelo de Seguridad y Privacidad de la Información MINTIC.

9. SOCIALIZACIÓN

Una vez aprobado este documento, es responsabilidad del líder del macroproceso y el responsable del procesos garantizar su socialización en los grupos primarios que le aplique, y/o mediante la utilización de cualquiera de las herramientas desarrolladas por la institución para tal fin, dejando la evidencia respectiva, las cuales deben ser enviado como soporte al correo institucional sistemas@esehospitalrmm.gov.co.

9. CONTROL DE CAMBIOS

FECHA	VERSION	DESCRIPCION DEL CAMBIO
31-05-2019	001	Creación del Documento
20-01-2022	002	Se realiza cambio actualización en formato de calidad