PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PLA-SIN-01

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

Contenido

OBJETIVO 3
OBJETIVOS ESPECIFICOS 3
ALCANCE 3
DEFINICIONES 4
MARCO NORMATIVO 6
POLITICA DE GERENCIA TECNOLOGIAS DE LA INFORMACION Y COMUNICACION 8
METODOLOGIA 8
ESTABLECIMIENTO Y GESTIÓN DEL MSPI 10
IMPLEMENTACIÓN Y OPERACIÓN DEL MSPI 12
SEGUIMIENTO Y REVISIÓN DEL MSPI 12
REQUISITOS DE DOCUMENTACIÓN 13
RESPOSANBILIDADES DE LA DIRECCIÓN 14
GESTIÓN DE RECURSOS 14
AUDITORIAS INTERNAS DE MSPI 15
REVISION DEL MSPI POR LA DIRECCIÓN 15
MEJORA DEL MSPI 16
PLAN DE RUTA 17

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

OBJETIVO

Este documento busca lograr la implementación en la ESE Hospital Geriátrico y Ancianato San Miguel de las mejores prácticas promovidas por el Departamento Administrativo de la Función Pública a través de su estrategia MIPG y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Estas prácticas se enfocan en el diagnóstico, planificación, implementación, gestión y mejoramiento continuo del Modelo de Seguridad y Privacidad de la Información (MSPI).

El MSPI tiene como objetivo fortalecer la confianza de la institución y de sus clientes internos, externos y partes interesadas en el manejo de la información, garantizando la privacidad, continuidad, integridad y disponibilidad de los datos durante el año 2025.

OBJETIVOS ESPECIFICOS

- Establecer y aplicar controles de acceso sólidos para garantizar que únicamente el personal autorizado tenga acceso a la información de pacientes y registros médicos.
- Implementar políticas y procedimientos para la encriptación de datos sensibles, asegurando la protección de la información tanto en tránsito como en reposo.
- Desarrollar políticas de seguridad de la información específicas para el entorno geriátrico, comunicándolas eficazmente a todo el personal involucrado.
- Generar un documento institucional basado en los lineamientos de buenas prácticas en seguridad y privacidad de la información.
- Realizar programas periódicos de capacitación para el personal sobre el manejo seguro de información y la importancia de la seguridad de la información.
- Establecer un programa continuo de auditorías internas para evaluar la eficacia de los controles implementados en seguridad de la información.
- Implementar procesos periódicos de evaluación y revisión del programa de seguridad de la información para identificar oportunidades de mejora y ajustar las estrategias conforme a los cambios y necesidades del 2025.
- Optimizar el acceso y la transparencia de la información pública, garantizando el cumplimiento de las normativas vigentes.

ALCANCE

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

El Modelo de Seguridad y Privacidad de la Información (MSPI) tiene como propósito diagnosticar, analizar, definir y planear el manejo de la seguridad de la información en los procesos ejecutados en la ESE Hospital Geriátrico y Ancianato San Miguel.

Este modelo aplica a todos los niveles de la institución, incluyendo a sus funcionarios, contratistas, proveedores, operadores y cualquier persona o entidad que, en cumplimiento de sus funciones, comparta, utilice, recolecte, procese, intercambie o consulte información de la institución. Asimismo, abarca a los entes de control y entidades relacionadas que accedan a la información del hospital bajo los lineamientos del MSPI.

DEFINICIONES

- **Activo de información**: Cualquier recurso de alta validez que contiene información vital para el hospital y que debe ser protegido.
- **Amenaza**: Causa potencial de un daño a un activo de información, capaz de atentar contra su seguridad.
- **Análisis de riesgos**: Proceso sistemático que utiliza información disponible para identificar peligros y estimar riesgos.
- **Antivirus**: Software diseñado para detectar, bloquear y eliminar virus informáticos o códigos maliciosos.
- **Ataque**: Acción destinada a interrumpir o dañar un activo de información, afectando su confiabilidad, disponibilidad e integridad. Representa la materialización de una amenaza.
- **Causa**: Razón que origina un riesgo.
- **Código malicioso**: Software diseñado para ejecutar acciones dañinas, como robar información, aprovechar recursos informáticos o dañar sistemas. Ejemplos: virus, gusanos, troyanos y spyware.
- **Controles**: Mecanismos para monitorear y gestionar actividades sospechosas que puedan afectar los activos de información.
- **Diseño de red segura**: Estructura de red con medidas de seguridad que minimizan los riesgos de intrusión.
- D**isponibilidad**: Propiedad que garantiza que la información esté accesible y utilizable únicamente por personas autorizadas.
- **DMZ (Zona Desmilitarizada)**: Segmento de red que aloja servicios accesibles desde redes inseguras como Internet.

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

- **Estándar de seguridad**: Conjunto de normas diseñadas para ofrecer soluciones sistemáticas en áreas específicas del conocimiento.
- **Firewall**: Software o hardware que restringe accesos no autorizados a redes o sitios web.
- **Impacto**: Consecuencias negativas que genera una amenaza al materializarse.
- **Incidente de seguridad de la información**: Evento inesperado que puede comprometer la seguridad de la información.
- **Ingeniería social**: Manipulación psicológica para obtener acceso no autorizado a sistemas o información.
- **Integridad**: Propiedad de mantener la exactitud y estado completo de los activos de información.
- **Intrusos**: Personas que intentan acceder sin autorización a sistemas informáticos mediante técnicas específicas.
- **ISO (International Organization for Standardization)**: Organización internacional de estándares.
- **Metodología**: Conjunto sistemático de reglas o métodos para cumplir con normas o estándares específicos.
- **Plan de contingencia**: Estrategia operativa que prevé, controla y minimiza impactos negativos en situaciones de emergencia.
- **Phishing**: Técnica de sustracción de datos personales mediante redes falsas o sitios fraudulentos.
- **Probabilidad de ocurrencia**: Posibilidad de que un evento específico ocurra.
- **Propietario del riesgo sobre el activo**: Persona encargada de gestionar un riesgo específico.
- **PSE (Proveedor de Servicios Electrónicos)**: Sistema que facilita pagos electrónicos a través de Internet.
- **Red de datos**: Infraestructura diseñada para la transmisión e intercambio de información.
- **Red privada virtual (VPN)**: Red restringida a usuarios autorizados que utiliza recursos de acceso público para extender redes privadas.
- **Repudio**: Negación de haber participado en una comunicación o interacción.

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

- **Responsables del activo**: Personas encargadas de proteger un activo de información.
- **Riesgo inherente**: Grado de incertidumbre natural de una actividad, sin medidas de control.
- **Riesgo residual**: Riesgo que persiste tras implementar medidas de seguridad.
- **Riesgo**: Grado de exposición que permite que una amenaza afecte un activo de información.
- **Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información (ISO/IEC 27000:2018).
- **Seguridad física**: Controles para proteger equipos contra amenazas físicas, como incendios o inundaciones.
- **Seguridad lógica**: Herramientas y medidas informáticas para controlar accesos a sistemas.
- **Teletrabajo**: Modalidad de trabajo remoto utilizando medios telemáticos.
- **Vulnerabilidad**: Debilidad en un activo o sistema que puede ser explotada por una amenaza.
- **Wi-Fi (Wireless Fidelity)**: Tecnología de red inalámbrica para comunicación a distancia basada en el estándar 802.11.

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.
- Título 9 - 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
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática.

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad Pagina 9 de 12

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- 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.

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- 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

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- 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.

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

POLITICA DE GERENCIA TECNOLOGIAS DE LA INFORMACION Y COMUNICACION

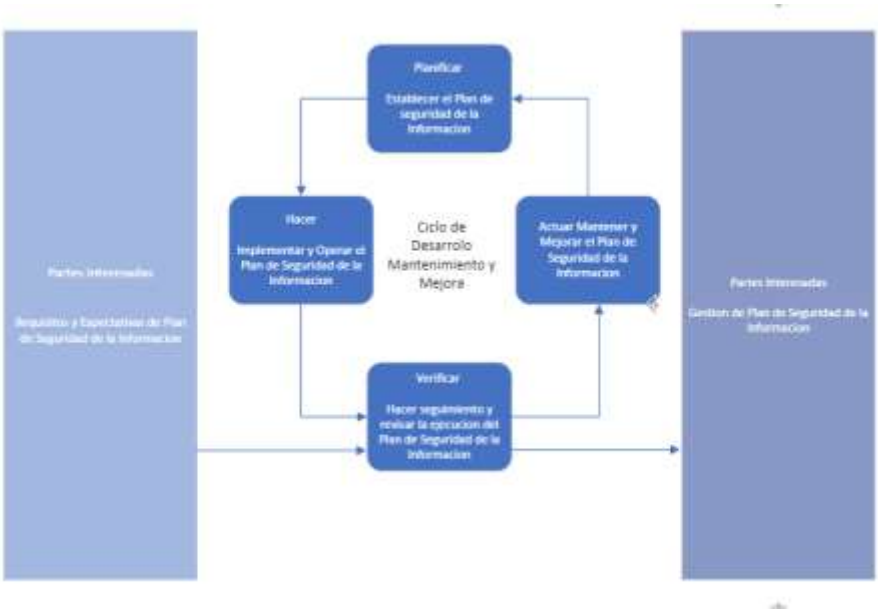
El equipo de colaboradores y el Gerente de la ESE Hospital Geriátrico y Ancianato San Miguel se comprometen a garantizar la confidencialidad, seguridad e integridad de la información de los usuarios, sus familias, y los clientes internos y externos.

Este compromiso incluye la protección de los activos de información mediante la implementación de medidas de seguridad lógica y física, así como el fomento de canales de comunicación que aseguren el acceso y la transparencia de la información pública. Todo esto se realiza a través del uso adecuado de las Tecnologías de la Información y las Comunicaciones (TICs), en cumplimiento con las disposiciones generales para la protección de datos, contribuyendo al logro de la Misión, Visión y los objetivos estratégicos de la institución.

METODOLOGIA

Para el desarrollo del proyecto, será esencial la participación activa de miembros directivos y representantes de las áreas misionales. Esto permitirá garantizar que toda la información relevante de la entidad esté disponible de manera oportuna, asegurando además que la iniciativa tenga un alcance transversal en toda la institución. De este modo, se evitará que el proyecto dependa exclusivamente de la oficina o área de TI.

Con el propósito de estructurar y ejecutar esta estrategia de manera efectiva, se utilizará como base el modelo PHVA (Planear, Hacer, Verificar, Actuar). Este enfoque asegurará un ciclo continuo de mejora y facilitará la implementación sistemática de las medidas necesarias para fortalecer la seguridad y privacidad de la información, como se detalla en la siguiente imagen:



Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

FASE	DESCRIPCION
PLANIFICAR (Establecer el Plan de Seguridad de la Información).	Definir la política, los objetivos, procesos y procedimientos de seguridad necesarios para gestionar los activos y mitigar riesgos. Este paso busca mejorar la seguridad de la información, garantizando que los resultados estén alineados con las políticas y objetivos globales de la organización.
HACER (Implementar y Operar).	Poner en marcha la política de seguridad, junto con los controles, procesos y procedimientos establecidos en el Sistema de Gestión de Seguridad de la Información (SGSI). Este proceso incluye la operación y monitoreo continuo para asegurar la efectividad del sistema.
VERIFICAR (Hacer seguimiento y revisar el Plan de Seguridad de la Información).	Realizar evaluaciones periódicas, medir el desempeño del sistema comparándolo con la política y los objetivos de seguridad establecidos, y analizar la experiencia práctica. Los resultados deben ser reportados a la dirección para su revisión y ajustes necesarios.
ACTUAR (Mantener y mejorar el Plan de Seguridad de la Información).	Tomar acciones correctivas y preventivas basadas en los resultados de las auditorías internas y las revisiones realizadas por la dirección. Estas acciones están orientadas a lograr la mejora continua del Plan de Seguridad del Sistema de Gestión de Seguridad de la Información (MSPI), asegurando su alineación con los objetivos organizacionales y su efectividad frente a nuevos riesgos.

Para planear y gestionar la implementación del Plan de Seguridad y Privacidad de la Información (PSPI), se conformará un grupo interdisciplinario liderado por el responsable de seguridad de la información del hospital. Este líder tendrá la responsabilidad de:

Definir y comunicar los perfiles y responsabilidades de cada integrante del equipo.

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

Identificar y asignar a las personas más idóneas para desempeñar cada rol dentro del grupo de trabajo.

A continuación, se presenta un modelo basado en la guía del MinTIC que describe la estructura y composición recomendada para los miembros del equipo de seguridad y privacidad de la información.



ESTABLECIMIENTO Y GESTIÓN DEL MSPI

La E.S.E. Hospital Geriátrico y Ancianato San Miguel realizará los esfuerzos necesarios para establecer y gestionar un Sistema de Gestión de Seguridad de la Información (MSPI) efectivo y alineado con sus objetivos estratégicos. Las acciones principales incluyen:

1. Definición del alcance y los límites del MSPI

- Delimitar las características del servicio que presta la organización, su estructura interna, ubicación, activos de información y tecnología.
- Incluir detalles claros y justificación de cualquier exclusión dentro del alcance del MSPI.

2. Definición de la política del MSPI

La política del MSPI debe:

- Proveer un marco de referencia para establecer objetivos y una dirección general de principios para la seguridad de la información.
- Considerar los requisitos internos, legales, reglamentarios y las obligaciones contractuales en materia de seguridad.
- Estar alineada con el contexto organizacional estratégico y de gestión del riesgo.
- Establecer criterios claros para evaluar riesgos.
- Ser aprobada formalmente por la dirección.

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

3. Enfoque organizacional para la valoración del riesgo

Para gestionar los riesgos, se deberá:

- Adoptar una metodología adecuada a los requisitos legales, reglamentarios y organizacionales del MSPI.
- Establecer criterios para la aceptación de riesgos y definir niveles aceptables.
- Seleccionar una metodología que permita resultados comparables y reproducibles.

Identificación y análisis de riesgos

- Identificar los activos del MSPI y los propietarios de dichos activos.
- Detectar amenazas potenciales y vulnerabilidades que podrían ser aprovechadas por estas.
- Evaluar los impactos derivados de la pérdida de confidencialidad, integridad y disponibilidad.
- Analizar y evaluar los riesgos basándose en:
    - Impactos potenciales de una falla de seguridad.
    - Probabilidad de ocurrencia considerando amenazas, vulnerabilidades y controles existentes.
    - Estimación de niveles de riesgo.

4. Tratamiento de riesgos

- Determinar si los riesgos son aceptables o requieren tratamiento.
- Evaluar y seleccionar acciones para tratar los riesgos, tales como:
    - Implementar controles adecuados.
    - Aceptar riesgos de manera informada.
    - Evitar riesgos.
    - Transferir riesgos a terceros (aseguradoras, proveedores, etc.).

5. Selección de controles y aprobación de riesgos residuales

- Seleccionar controles basados en el proceso de valoración y tratamiento de riesgos.
- Obtener aprobación de la dirección sobre los riesgos residuales y la autorización para operar el MSPI.

6. Declaración de aplicabilidad

Elaborar una declaración de aplicabilidad que incluya:

- Los objetivos de control y controles implementados.
- Controles excluidos y la justificación de dichas exclusiones.

7. Sensibilización y apropiación del MSPI

Diseñar e implementar un plan para sensibilizar y capacitar a todos los miembros de la entidad sobre el MSPI, asegurando su compromiso y apropiación del sistema.

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

IMPLEMENTACIÓN Y OPERACIÓN DEL MSPI

La ESE Hospital Geriátrico y Ancianato San Miguel realizara esfuerzos para:

- Formular un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información.
- Implementará el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluye considerar la financiación y la asignación de funciones y responsabilidades.
- Implementará los controles seleccionados para cumplir los objetivos de control.
- Definirá cómo medir la eficacia de los controles o grupos de controles seleccionados y especificar cómo se usarán estas mediciones para valorar su eficacia para producir resultados comparables y reproducibles.
- Implementará programas de formación y de toma de conciencia.
- Gestionará la operación del MSPI.
- Gestionará los recursos del MSPI.
- Implementará procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad.
-

SEGUIMIENTO Y REVISIÓN DEL MSPI

La E.S.E. Hospital Geriátrico y Ancianato San Miguel deberá:

- Ejecutar procedimientos de seguimiento, revisión y otros controles para:
    - Detectar rápidamente errores en los resultados del procesamiento.
    - Identificar con prontitud los incidentes e intentos de violación a la seguridad, tanto los que tuvieron éxito como los que fracasaron.
    - Posibilitar que la dirección determine si las actividades de seguridad delegadas a las personas o implementadas mediante tecnología de la información se están ejecutando de manera esperada.
    - Ayudar a detectar eventos de seguridad e impedir incidentes mediante indicadores.
    - Determinar si las acciones tomadas para solucionar un problema de violación a la seguridad fueron eficaces.
- Emprender revisiones regulares de la eficacia del MSPI, asegurando el cumplimiento de la política y los objetivos del MSPI, así como la revisión de los controles de seguridad, considerando:
    - Resultados de auditorías de seguridad.

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

  - Incidentes registrados.
  - Mediciones de eficacia.
  - Sugerencias y retroalimentación de las partes interesadas.
- Medir la eficacia de los controles para verificar el cumplimiento de los requisitos de seguridad.
- Revisar las valoraciones de los riesgos a intervalos planificados y actualizar el nivel de riesgo residual y aceptable, teniendo en cuenta cambios en:
  - El hospital.
  - La tecnología.
  - Los objetivos y procesos del hospital.
  - Las amenazas identificadas.
  - La eficacia de los controles implementados.
  - Eventos externos, como cambios en el entorno legal o reglamentario, obligaciones contractuales y el clima social.
- Realizar auditorías internas del MSPI en los intervalos planificados.
- Llevar a cabo revisiones periódicas del MSPI por parte de la dirección, garantizando que el alcance siga siendo adecuado y que se identifiquen mejoras en el proceso de MSPI.
- Actualizar los planes de seguridad con base en las conclusiones de las actividades de seguimiento y revisión.
- Registrar acciones y eventos que puedan tener impacto en la eficacia o el desempeño.

MANTENIMIENTO Y MEJORA DEL MSPI
Regularmente el Hospital Geriátrico y Ancianato San Miguel deberá:

• Implementar las mejoras identificadas en el MSPI.
• Emprender las acciones correctivas y preventivas adecuadas, aplicando las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y las de la propia organización.
• Comunicar las acciones y mejoras a todas las partes interesadas, con un nivel de detalle apropiado a las circunstancias y en donde sea pertinente, llegar a acuerdos sobre cómo proceder.
• Asegurar que las mejoras logran los objetivos previstos.

REQUISITOS DE DOCUMENTACIÓN

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

La documentación del MSPI incluirá registros detallados de las decisiones tomadas por la dirección, asegurando que las acciones sean trazables a dichas decisiones y a las políticas establecidas por la alta dirección. Además, los resultados registrados deberán ser reproducibles y accesibles.

Esta documentación se realizará conforme a las directrices y guías establecidas por MinTIC para la implementación y gestión del MSPI, garantizando el cumplimiento de los requisitos y la coherencia con las mejores prácticas de seguridad de la información.

RESPOSANBILIDADES DE LA DIRECCIÓN

La dirección de la ESE Hospital Geriátrico y Ancianato San Miguel brindará evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del MSPI de la siguiente manera:

- Estableciendo y aprobando la política del MSPI.
- Asegurando la definición de los objetivos y planes estratégicos del MSPI.
- Estableciendo y asignando las funciones y responsabilidades relacionadas con la seguridad de la información.
- Comunicando de manera efectiva a toda la organización la importancia de cumplir con los objetivos de seguridad de la información, la conformidad con la política de seguridad, las responsabilidades legales, y la necesidad de una mejora continua en el sistema.
- Proporcionando los recursos necesarios para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar el MSPI.
- Decidiendo los criterios para la aceptación de riesgos y estableciendo los niveles de riesgo aceptables.
- Asegurando que se lleven a cabo auditorías internas del MSPI de manera periódica.
- Realizando revisiones regulares del MSPI por parte de la dirección para garantizar su eficacia y adecuación a las necesidades de la organización.

GESTIÓN DE RECURSOS

La ESE Hospital Geriátrico y Ancianato San Miguel determinará y suministrará los recursos necesarios para:

- Establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar el MSPI.
- Asegurar que los procedimientos de seguridad de la información brindan el soporte adecuado a los requisitos de la institución.
- Identificar y cumplir con los requisitos legales, reglamentarios y las obligaciones de seguridad contractuales.
- Mantener un nivel adecuado de seguridad mediante la correcta implementación y aplicación de todos los controles establecidos.
- Realizar revisiones periódicas cuando sea necesario y reaccionar de manera apropiada a los resultados obtenidos, tomando medidas para mejorar la eficacia del MSPI cuando sea necesario.

Formación, toma de conciencia y competencia

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

El hospital debe asegurar que todo el personal asignado a responsabilidades dentro del MSPI sea competente para realizar las tareas que se les asignen, mediante:

- La determinación de las competencias necesarias para el personal que lleve a cabo actividades que afecten directamente al MSPI.
- La provisión de formación continua o la adopción de otras acciones (como la contratación de personal competente) para satisfacer las necesidades de competencias.
- La evaluación periódica de la eficacia de las acciones emprendidas en términos de formación y mejora.
- El mantenimiento adecuado de registros relacionados con la educación, formación, habilidades, experiencia y calificaciones del personal involucrado en la gestión de la seguridad de la información.

AUDITORIAS INTERNAS DE MSPI

La ESE Hospital Geriátrico y Ancianato San Miguel deberá llevar a cabo auditorías internas del MSPI a intervalos planificados, con el fin de determinar si los objetivos de control, los controles, los procesos y los procedimientos del MSPI:

- Cumplen con los requisitos establecidos en la presente norma, así como con la legislación y reglamentaciones pertinentes.
- Cumplen con los requisitos identificados en materia de seguridad de la información.
- Están debidamente implementados y se mantienen de manera eficaz.
- Tienen un desempeño que está en línea con lo esperado.

REVISION DEL MSPI POR LA DIRECCIÓN

La dirección del hospital deberá revisar el MSPI del hospital al menos una vez al año, con el fin de asegurar su conveniencia, suficiencia y eficacia. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de realizar cambios en el MSPI, incluidos la política de seguridad y los objetivos de seguridad.

Información para la revisión

Las entradas para la revisión por la dirección incluirán:

- Resultados de las auditorías y revisiones del MSPI.
- Retroalimentación de las partes interesadas.
- Nuevas técnicas, productos o procedimientos que se puedan utilizar en la organización para mejorar el desempeño y eficacia del MSPI.
- Estado de las acciones correctivas y preventivas.
- Vulnerabilidades o amenazas no tratadas adecuadamente en la valoración previa de los riesgos.
- Resultados de las mediciones de eficacia.
- Acciones de seguimiento resultantes de revisiones anteriores por la dirección.
- Cualquier cambio que pueda afectar al MSPI.
- Recomendaciones para mejoras.

Resultados de la revisión

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

Los resultados de la revisión por la dirección incluirán cualquier decisión y acción relacionada con:

- La mejora de la eficacia del MSPI.
- La actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.
- La modificación de los procedimientos y controles que afectan la seguridad de la información, según sea necesario, para responder a eventos internos o externos que puedan tener un impacto en el MSPI, incluidos cambios en:
    - Los requisitos de la organización.
    - Los requisitos de seguridad.
    - Los procesos de la institución que afectan los requisitos del negocio existentes.
    - Los requisitos reglamentarios o legales.
    - Las obligaciones contractuales.
    - Los niveles de riesgo y/o niveles de aceptación de riesgos.
    - Los recursos necesarios.
    - La mejora en la eficacia de los controles.

MEJORA DEL MSPI

La E.S.E. Hospital Geriátrico y Ancianato San Miguel deberá mejorar continuamente la eficacia del MSPI mediante:

- El uso de la política de seguridad de la información.
- Los objetivos de seguridad de la información.
- Los resultados de la auditoría.
- El análisis de los eventos a los que se les ha hecho seguimiento.
- Las acciones correctivas y preventivas, y la revisión por la dirección.

Acción correctiva

La E.S.E. Hospital Geriátrico y Ancianato San Miguel deberá actuar para eliminar la causa de las no conformidades asociadas con los requisitos del MSPI, con el fin de prevenir que vuelvan a ocurrir. El procedimiento documentado para la acción correctiva debe definir los requisitos para:

- Identificar las no conformidades.
- Determinar las causas de las no conformidades.
- Evaluar la necesidad de acciones para asegurar que las no conformidades no vuelvan a ocurrir.
- Determinar e implementar la acción correctiva necesaria.
- Registrar los resultados de la acción tomada.
- Revisar la acción tomada.

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

Acción preventiva

La E.S.E. Hospital Geriátrico y Ancianato San Miguel determinará acciones para eliminar la causa de las no conformidades potenciales con los requisitos del MSPI y evitar que ocurran. Las acciones preventivas tomadas deben ser apropiadas al impacto de los problemas potenciales. El procedimiento documentado para la acción preventiva debe definir los requisitos para:

- Identificar no conformidades potenciales y sus causas.
- Evaluar la necesidad de acciones para impedir que las no conformidades ocurran.
- Determinar e implementar la acción preventiva necesaria.
- Registrar los resultados de la acción tomada.
- Revisar la acción preventiva tomada.

PLAN DE RUTA

ACTIVIDAD	2025											
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Planeación de al Implementación del MSPI												
Definición de políticas genéricas de seguridad												
Implementación dispositivo de seguridad perimetral												
Implementación MSPI												
Gestión y operación MSPI												
Mantenimiento y mejora MSPI												
Auditoría interna												
Revisión del MSPI por la dirección												
Mejora MSPI												

Actualizado por:	Revisado por:	Aprobado por:
ORIGINAL FIRMADO	**ORIGINAL FIRMADO**	**ORIGINAL FIRMADO**
Milton Ediws Bautista Cardona **Sistemas e información**	Brenda Ospina **Profesional Gestión y Mejora**	Oscar Erazo Castro **Subgerente Administrativo y Financiero**
Fecha:16/01/2025	**Fecha:16/01/2025**	**Fecha:16/01/2025**

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA DE VIGENCIA
01	Creación del plan	Enero 2023

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

02	Actualización Plan	Enero 2024
03	Actualización Plan	Enero 2025

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”