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 7
POLITICA DE GERENCIA TECNOLOGIAS DE LA INFORMACION Y COMUNICACION 8
METODOLOGIA 8
ESTABLECIMIENTO Y GESTION DEL MSPI 10
IMPLEMENTACIÓN Y OPERACIÓN DEL MSPI 12
SEGUIMIENTO Y REVISIÓN DEL MSPI 13
MANTENIMIENTO Y MEJORA DEL MSPI 14
REQUISITOS DE DOCUMENTACIÓN 14
RESPOSANBILIDADES DE LA DIRECCIÓN 15
GESTIÓN DE RECURSOS 15
AUDITORIAS INTERNAS DE MSPI 16
REVISION DEL MSPI POR LA DIRECCIÓN 16
MEJORA DEL MSPI 17
PLAN DE RUTA 18

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

OBJETIVOS ESPECIFICOS

- Establecer y aplicar controles de acceso sólidos para garantizar que solo 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 y comunicarlas eficazmente a todo el personal.
- Generar un documento institucional guiado en lineamientos de buenas prácticas en seguridad y Privacidad de la información.
- Realizar programas regulares de capacitación para el personal sobre prácticas seguras de manejo de información y concienciación sobre la importancia de la seguridad de la información.
- Establecer un programa regular de auditorías internas para revisar y evaluar la eficacia de los controles de seguridad de la información.
- Implementar procesos regulares de evaluación y revisión del programa de seguridad de la información para identificar áreas de mejora y ajustar las estrategias según sea necesario.
- Optimizar la labor de acceso a la información pública.

ALCANCE

El Modelo de Seguridad y Privacidad de la Información (MSPI) pretende diagnosticar, analizar, definir y planear el manejo de la seguridad de la información en los procesos ejecutados en el Hospital, aplica a todos los niveles del hospital, a todos sus funcionarios, contratistas, proveedores, operadores y aquellos que, en razón de cumplir sus funciones y las del hospital compartan, utilicen, recolecten, intercambien o consulten su información, así como a los entes

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”

de control, entidades relacionadas que accedan, recolecten, procesen, intercambien o consulten su información.

DEFINICIONES

• **Activo de información**: aquello que es de alta validez y que contiene información vital del hospital que debe ser protegida.

• **Amenaza**: Es la causa potencial de un daño a un activo de información. Es toda aquella acción o elemento capaz de atentar contra la seguridad de la información.

• **Análisis de riesgos**: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

• **Antivirus:** Software encargado de detectar, bloquear y eliminar virus informáticos o código malicioso.

• **Ataque**: Es la acción de interrumpir o dañar un activo de información con el objetivo de causar problemas de confiabilidad, disponibilidad e integridad; también se puede afirmar que es cuando se materializa una amenaza de seguridad.

• **Causa**: Razón por la cual el riesgo sucede.

• **Código malicioso**: Software diseñado para ejecutar acciones maliciosas (como provocar daños al software de la computadora, robar información almacenada en un sistema informático, aprovechar recursos informáticos para efectuar otras acciones perjudiciales para el usuario) y que incluye programas como virus, gusanos, troyanos y spyware. Puede utilizar como vía de diseminación, el correo electrónico, sitios de internet, redes, dispositivos móviles, dispositivos removibles (por ejemplo, pendrives).

• **Controles**: mecanismos utilizados para monitorear y controlar acciones consideradas sospechosas y que pueden afectar a los activos de información.

• **Diseño de Red Segura:** Definición de un esquema de red aplicando medidas de seguridad informática, que una vez implementadas minimizan los riesgos de una intrusión

• **Disponibilidad:** Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

• **DMZ**: Una DMZ o una zona desmilitarizada, es un segmento de red específico, en el cual se ubican servicios específicos de red que son públicos a redes poco seguras como Internet.

• **Estándar de seguridad:** Conjunto de normas o modelos diseñados con la finalidad de brindar soluciones de sistemáticas a un área del conocimiento específico.

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”

• **Firewall**: Un firewall o también llamados corta fuego, es un software o hardware que restringe el acceso a sitios web o una red sin autorización de acceso.

• **Impacto**: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

• **Incidente de seguridad de la información**: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

• **Incidente de seguridad:** Un incidente de seguridad es cualquier acción que atente

• **Ingeniería social:** secuencia de acciones que pretenden obtener información, fraude o acceso no autorizado a sistemas informáticos, y que ha implicado la manipulación psicológica de personas.

• **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

• **Intrusos:** Es una Persona que intenta acceder a un sistema informático sin autorización, a través de técnicas y/o métodos informáticos que se lo permitan. ISO: (International Organización for Standardization). Organización internacional de estándares

• **Metodología**: Es un conjunto de reglas o métodos organizados de forma sistémica con el objetivo de lograr el cumplimiento de una norma o un estándar.

• **Plan de contingencia:** Es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.

• **Phishing**: Wi-phishing, sustracción de datos personales a través de falsas redes públicas de acceso Wi-Fi.

• **Probabilidad de ocurrencia**: Posibilidad de que se presente una situación o evento específico.

• **Propietario del riesgo sobre el activo**: Persona responsable de gestionar el riesgo.

• **PSE:** Proveedor de Servicios Electrónicos, es un sistema centralizado por medio del cual las empresas brindan a los usuarios la posibilidad de hacer sus pagos por Internet.

• **Red de Datos**: Es aquella infraestructura o red de comunicación que se ha diseñado específicamente a la transmisión de información mediante el intercambio de datos.

• **Red Privada virtual VPN**: Sistema de telecomunicación consistente en una red de datos restringida a un grupo cerrado de usuarios, que se construye empleando en parte o totalmente

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 recursos de una red de acceso público, es decir, es una extensión de la red privada de una organización usando una red de carácter público.

• **Repudio**: Denegación, por una de las entidades implicadas en un a comunicación, de haber participado en la totalidad o en parte de dicha comunicación.

• **Responsables del Activo**: Personas responsables del activo de información.

• **Riesgo Inherente**: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

• **Riesgo Residual**: Nivel de riesgo remanente por aplicar medidas de seguridad sobre el activo.

• **Riesgo**: Grado de exposición de un activo que permite la materialización de una amenaza.

• **Riesgos**: Es la posibilidad de que una amenaza aproveche una vulnerabilidad y dañe un activo de información. Departamento de seguridad.

• **Seguridad de la Información**: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO/IEC 27000:20184). SGSI: Siglas del Sistema de Gestión de Seguridad de la Información.

• **Seguridad física:** Controles externos al ordenador, que tratan de protegerlo contra amenazas de naturaleza física como incendios, inundaciones, entre otros. SGSI: Sistema de gestión de la seguridad de la información,

• **Seguridad lógica**: Conjunto de medidas de seguridad y herramientas informáticas de control de acceso a los sistemas informáticos.

• **Teletrabajo**: El teletrabajo es un nuevo sistema de organización del trabajo en que la persona trabajadora desarrolla una parte importante de su trabajo fuera de la empresa y por medios telemáticos.

• **Vulnerabilidad**: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada.

• **Wi-Fi (Wireless Fidelity o fidelidad sin cables)**: Es una red de ordenadores sin utilización de cables equivalente a la tecnología inalámbrica 802.11 para comunicación a distancia.

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”

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.
- 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

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”

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.

POLITICA DE GERENCIA TECNOLOGIAS DE LA INFORMACION Y COMUNICACION

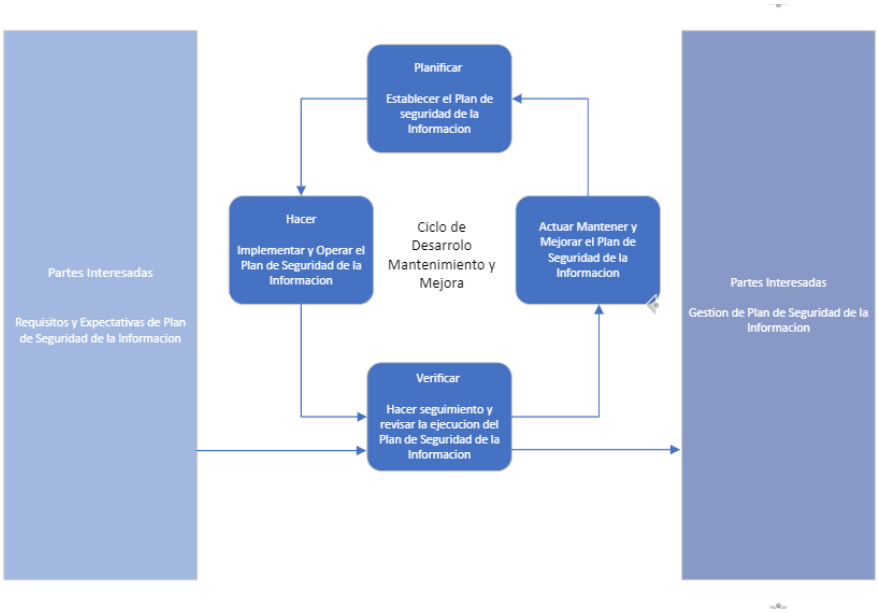
El equipo de colaboradores y el Gerente de La ESE Hospital Geriátrico y Ancianato San Miguel se comprometen a garantizar la confidencialidad, seguridad e integralidad de la información de los usuarios y su familia, clientes internos y externos en cuanto a seguridad lógica y física de los activos, fomento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

METODOLOGIA

Para desarrollar el proyecto al que deben pertenecer miembros directivos y representantes de las áreas misionales, para asegurar que toda la información relevante de la entidad esté disponible oportunamente. De esta forma se busca asegurar que sea una iniciativa de carácter transversal al hospital, y que no dependa exclusivamente de la oficina o área de TI.

Para llevar a cabo este propósito, se basará la estrategia en el modelo PHVA como se muestra 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 Plan de Seguridad de la Información)	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 una organización
HACER (Implementar y Operar)	Implementar y operar la política, los controles, procesos y procedimientos del MSPI
VERIFICAR (Hacer seguimiento y revisar el Plan de Seguridad de la Informacion)	Evaluar donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, reportando los resultados a la dirección para su revisión.
ACTUAR (Mantener y mejorar el Plan de Seguridad de la Información)	Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna la revisión por la dirección, para lograr

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 mejora continua del Plan de seguridad del MSPI.

Para planear y gestionar la implementación del Plan de seguridad y Privacidad (PSPI) de la información se contará con un grupo interdisciplinario que será liderado por el responsable de seguridad de la información del hospital quien deberá entregar y dar a conocer los perfiles y responsabilidades de cada persona al grupo de trabajo e identificar las personas idóneas para asignar cada rol.

A continuación, se muestra un modelo tomado de la guía de MinTIC correspondiente a los miembros del equipo de seguridad y privacidad de la información.



ESTABLECIMIENTO Y GESTION DEL MSPI

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

- Definir el alcance y límites del MSPI en términos de las características del servicio que presta el organismo, su estructura interna, su ubicación, sus activos de información, tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance.
- Definir una política de MSPI en términos de las características del servicio que presta el organismo, su estructura interna, sus activos de información y tecnología; que:

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"

- Incluya un marco de referencia para fijar objetivos y establezca un sentido general de dirección y principios para la acción con relación a la seguridad de la información.
- Tenga en cuenta los requisitos del organismo, los legales o reglamentarios y las obligaciones de seguridad contractuales.
- Este alineado con el contexto organizacional estratégico de gestión del riesgo en el que se establecerá y mantendrá el MSPI.
- Establezca los criterios contra los cuales se evaluará el riesgo. Haya sido aprobada por la dirección.
- Definir el enfoque organizacional para la valoración del riesgo, teniendo en cuenta:
- Identificar una metodología de valoración del riesgo que sea adecuada al MSPI y a los requisitos reglamentarios, legales y de seguridad de la información de la organización, identificados.

- Desarrollar criterios para la aceptación de riesgos e identificar los niveles de riesgo aceptables.
- Seleccionar una metodología para la valoración de riesgos que asegure que las valoraciones produzcan resultados comparables y reproducibles.
- Identificar los riesgos
- Identificar los activos dentro del alcance del MSPI y los propietarios de estos activos de información.
- Identificar las amenazas a estos activos.
- Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas.
- Identificar los impactos que la perdida de confidencialidad, integridad y disponibilidad puede tener sobre estos activos.
- Analizar y evaluar los riesgos.
- Valorar el impacto que podría causar una falla en la seguridad, sobre el organismo, teniendo en cuenta las consecuencias de la pérdida de confidencialidad, integridad o disponibilidad de los activos.
- Valorar la posibilidad realista de que ocurra una falla en la seguridad, considerando las amenazas, las vulnerabilidades, los impactos asociados con estos activos, y los controles implementados actualmente.

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”

- Estimar los niveles de los riesgos.
- Determinar la aceptación del riesgo o la necesidad de su tratamiento a partir de los criterios previamente establecidos.
- Identificar y evaluar las opciones para el tratamiento de los riesgos. Las posibles acciones incluyen:
- Aplicar los controles apropiados
- Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos.
- Evitar riesgos
- Transferir a otras partes los riesgos asociados con el negocio ej. Aseguradoras, proveedores, etc.
- Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.
- Los controles a seleccionar e implementar deben cumplir los requisitos identificados en el proceso de valoración y tratamiento de riesgos.
- Obtener la aprobación de la dirección sobre los riesgos residuales propuestos.
- Obtener autorización de la dirección para implementar y operar el MSPI.
- Elaborar una declaración de aplicabilidad, la declaración de aplicabilidad debe incluir:
- Los objetivos de control y los controles.
- Los objetivos de control y los controles que ya se hayan implementado.
- La exclusión de cualquier objetivo de control y controles y la justificación para su exclusión.
- Elaborar un plan de sensibilización y apropiación del MSPI para toda la entidad.

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.

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”

- 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 ESE 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 en la forma esperada.
- Ayudar a detectar eventos de seguridad e impedir incidentes con 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 (que incluyen cumplir la política y objetivos del MSPI, y revisar los controles de seguridad) considerando los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de las partes interesadas.

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”

- Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.
- Revisar las valoraciones de los riesgos a intervalos planificados y revisar el nivel de riesgo residual y riesgo aceptable identificado, teniendo en cuenta los cambios en:

→ El hospital
→ La tecnología
→ Los objetivos y procesos del hospital
→ Las amenazas identificadas.
→ La eficacia de los controles implementados.
→ Eventos externos, tales como cambios en el entorno legal o reglamentario, en las obligaciones contractuales, y en el clima social.
→ Realizar auditorías internas del MSPI a intervalos planificados.
→ Emprender una revisión del MSPI, realizada por la dirección, en forma regular para asegurar que el alcance siga siendo suficiente y que se identifiquen mejoras al proceso de MSPI.
→ Actualizar los planes de seguridad para tener en cuenta las conclusiones de las actividades de seguimiento y revisión.
→ Registrar acciones y eventos que podrían 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

La documentación del MSPI incluirá registros de las decisiones de la dirección, asegurar que las acciones sean trazables a las decisiones y políticas de la alta dirección, y que los resultados registrados sean reproducibles.
Esta documentación se realizará conforme a las guías dispuestas por MinTIC para el MSPI.

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”

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 la política del MSPI.
• Asegurando que se establezcan los objetivos y planes del MSPI.
• Estableciendo funciones y responsabilidades de seguridad de la información.
• Comunicando a la organización la importancia de cumplir los objetivos de seguridad de la información y de la conformidad con la política de seguridad de la información, sus responsabilidades bajo la ley, y la necesidad de la mejora continua.
• Brindando los recursos suficientes para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un MSPI.
• Decidiendo los criterios para aceptación de riesgos y los niveles de riesgo aceptables.
• Asegurando que se realizan auditorías internas del MSPI.
• Efectuando las revisiones por la dirección, del MSPI.

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 apoyo a los requisitos de la institución.
• Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales.
• Mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados.
• Llevar a cabo revisiones cuando sea necesario, y reaccionar apropiadamente a los resultados y en donde se requiera mejorar la eficacia del MSPI. Formación, toma de conciencia y competencia.

El hospital debe asegurar que todo el personal al que se le asigne responsabilidades definidas en el MSPI sea competente para realizar las tareas exigidas, mediante:

• La determinación de las competencias necesarias para el personal que ejecute el trabajo que afecta el MSPI.
• El suministro de formación o realización de otras acciones (ej. Contratación de personal competente) para satisfacer las necesidades.
• La evaluación de la eficacia de las acciones emprendidas.
• El mantenimiento de registros de la educación, formación, habilidades, experiencia y calificaciones.

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”

AUDITORIAS INTERNAS DE MSPI

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

• Cumplen los requisitos de la presente norma y de la legislación o reglamentaciones pertinentes.
• Cumplen los requisitos identificados de seguridad de la información.
• Están implementados y se mantienen eficazmente.
• Tienen un desempeño acorde con lo esperado.

REVISION DEL MSPI POR LA DIRECCIÓN

La dirección del hospital deberá revisar el MSPI del hospital una vez al año, para asegurar su conveniencia, suficiencia y eficacia. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del 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 auditorias y revisiones del MSPI.
• Retroalimentación de las partes interesadas.
• Técnicas, productos o procedimientos que se pueden usar 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 resultante de revisiones anteriores por la dirección.
• Cualquier cambio que pueda afectar el MSPI.
• Recomendaciones para mejoras.

Resultados de la revisión

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 pueden tener impacto en el MSPI, incluidos cambios a:
• Los requisitos de la organización
• Los requisitos de seguridad
• Los procesos del organismo que afectan los requisitos del negocio existentes.
• Los requisitos reglamentarios o legales.

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”

• Las obligaciones contractuales.
• Los niveles de riesgo y/o niveles de aceptación de riesgos.
• Los recursos necesarios.
• Mejora a la medida de la eficacia de los controles.

MEJORA DEL MSPI
El Hospital Geriátrico 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

El hospital deberá actuar para eliminar la causa de no conformidades asociadas con los requisitos del MSPI, para prevenir que vuelvan a ocurrir.
El procedimiento documentado para la acción correctiva debe definir requisitos para:
• Identificar las no conformidades
• Determinar las causas de las no conformidades.
• Evaluar la necesidad de acciones que aseguren que las no conformidades no vuelven a ocurrir.
• Determinar e implementar la acción correctiva necesaria.
• Registrar los resultados de la acción tomada.
• Revisar la acción tomada.

Acción preventiva

El Hospital determinará acciones para eliminar la causa de 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 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.

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”

PLAN DE RUTA

ACTIVIDAD	2024											
	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
Jhonny Torres **Sistemas e Información**	María del Mar Medina Osorio **Auxiliar Gestión y Mejora**	Carolina Osorio Gonzalez **Subgerente Administrativa y Financiera**
Fecha:22/01/2024	**Fecha:22/01/2024**	**Fecha:22/01/2024**

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA DE VIGENCIA
01	Creación del plan	Enero 2023
02	Actualización Plan	Enero 2024

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”