PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PSPI

2020 - 2024

HOSPITAL DEL ROSARIO ESE IAMI
CAMPOALEGRE - HUILA

TABLA DE CONTENIDO

1. Introducción

La E.S.E Hospital del Rosario busca afrontar los retos del negocio con una infraestructura digital moderna, robusta y segura, capaz de sacar provecho de la llamada cuarta revolución industrial "La transformación digital", En general, el cambio obligatorio desde la simple digitalización a la innovación basada en combinaciones de tecnologías está obligando a las empresas a reexaminar la forma de hacer negocios. Por lo que para el hospital se debe dar prioridad a la seguridad de la información, cumpliendo los lineamientos de los estándares ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines y el ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls como complemento a los requisitos de seguridad, los cuales consisten en preservar la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de un proceso de gestión de riesgo, para lo cual, se busca estar alineados con las exigencias del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, (MinTic).

El grupo de necesidades de información lo conforman el conjunto de requerimiento de información, activos y datos que se necesitan para la ejecución de las estrategias, el cumplimiento de sus objetivos y metas del negocio. Existen diferentes fuentes de información a tener en cuenta en la construcción del Plan Estratégico de Tecnologías de la Información y Comunicación – PETIC, finalmente en éste se consignan todas las iniciativas y oportunidades tecnológicas de la institución, considerando su estado actual y definiendo un estado futuro que se construye a partir de la puesta en marcha de diferentes esfuerzos, proyectos, programas, iniciativas y compromisos.

La información es un activo vital para el éxito y la continuidad de negocio del Hospital, el aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización; siendo necesario planear e implementar un sistema de gestión de seguridad de la información que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que están sometidos los activos de información del hospital.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno Digital, permite alinearse a los siguientes componentes y habilitadores:

TIC para el Estado: Tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las TIC. Así mismo, busca fortalecer las competencias T.I. de los servidores públicos, como parte fundamental de la capacidad institucional.

TIC para la Sociedad: tiene como objetivo fortalecer la sociedad y su relación con el Estado en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, políticas y normas, y la identificación de soluciones a problemáticas de interés común.

Arquitectura: Busca fortalecer las capacidades de gestión de T.I. de las entidades públicas, a través de la definición de lineamientos, estándares y mejores prácticas contenidos en el Marco de Referencia de Arquitectura Empresarial del Estado.

Seguridad y Privacidad: Busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del Estado, garantizando su buen uso y la privacidad de los datos, a través de un Modelo de Seguridad y Privacidad de la Información.

Servicios Ciudadanos Digitales: Busca facilitar y brindar un adecuado acceso a los servicios de la administración pública haciendo uso de medios digitales, para lograr la autenticación electrónica, interoperabilidad y carpeta ciudadana, esto será posible a través de la implementación del Modelo de Servicios Ciudadanos Digitales.

El presente documento es el resultado de la actualización correspondiente a la vigencia 2021.

2. Objetivo

Planear e implementar las estrategias para la gestión de seguridad y privacidad de la Información en el Hospital del Rosario que permitan minimizar los riesgos de pérdida de activos de la información, alineadas a las directrices emanadas por MinTIC y acordes con las necesidades del hospital.

2.1. Objetivos específicos

- Realizar un diagnóstico de la situación actual de seguridad de la información mediante auditorías para identificar las brechas del sistema y los aspectos a mejorar.
- Definir un plan de trabajo para lograr la implementación del modelo de seguridad y privacidad de la información en el hospital.
- Comunicar e implementar la estrategia de seguridad de la información.
- Definir las responsabilidades relacionadas con el manejo de la seguridad de la información.
- Establecer una metodología de gestión de la seguridad de la información clara y estructurada.
- Optimizar la gestión de la seguridad de la información con base en la gestión de procesos.
- Reducir el riesgo de pérdida, robo o corrupción de información.
- Reducir el riesgo de pérdida de confidencialidad, integridad y disponibilidad de los activos de información.
- Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios y de las operaciones necesarias de negocio tras incidentes de gravedad.
- Definir el plan para la transición de IPv4 a IPv6.

3. Alcance

El MSPI tiene como finalidad el diagnóstico, análisis, definición y planeación del manejo de la seguridad de la información en los procesos que se ejecutan en el Hospital, aplica a todos los niveles del hospital, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del hospital compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los entes de control, entidades relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación.

Este documento indica cuáles serán las labores que realizará el hospital con el objetivo de lograr el 100% de la implementación del MSPI al interior de todos los procesos del hospital, definiendo plazos anuales.

4. Glosario de términos

- **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, pen-drives).
- **Controles**: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera 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.
- **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**: es la secuencia de acciones que tienen como finalidad la obtención de información, el fraude o el acceso no autorizado a sistemas informáticos, y que ha implicado en algún momento 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 Organization 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.
- **Pphishing**: 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 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 como resultado de la aplicación de 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.

- **Sistema de Gestión de Seguridad de la información SGSI**: permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001:2013.

- **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.

5. Marco normativo

Ley 39 de 1981. Sobre microfilmación y certificación de archivos.

Ley 527 de 1999. Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones, así mismo introduce el concepto de equivalente funcional, firma electrónica como mecanismos de autenticidad, disponibilidad y confidencialidad de la información.

Ley 594 de 2000. "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".

Ley 1273 de 2009. Ley la cual se crea y se protege el bien jurídico de la información y los datos personales.

Ley 1341 de 2009. "Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones".

CONPES 3670 de 2010. "Lineamientos de Política para la continuidad de los programas de acceso y servicio universal a las Tecnologías de la Información y las Comunicaciones".

CONPES 3701 de 2011. "Lineamientos de Política para Ciberseguridad y Ciberdefensa" Ley 872 de 2003. "Por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios".

Ley 1581 de 2012. Ley Estatutaria por la cual se reglamenta el artículo 15 de la Constitución política, relativo a la intimidad personal y el Habeas Data, a través de esta norma se dictan disposiciones generales para la protección de datos personales.
Decreto 2609 de 2012. Por el cual se dictan disposiciones en materia de gestión documental y gestión documental electrónica.

Decreto 2693 de 2012. Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

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 103 de 2015. Por la cual se reglamenta parcialmente la ley 1712 de 2014 y se dictan otras disposiciones, en cuanto a la publicación y divulgación de la información.

Resolución 2710 de 2017. Por la cual se establecen lineamientos para la adopción del protocolo IPv6.
CONPES 3995 de 2020. Política nacional de confianza y seguridad digital, política nacional que tiene como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital.

Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

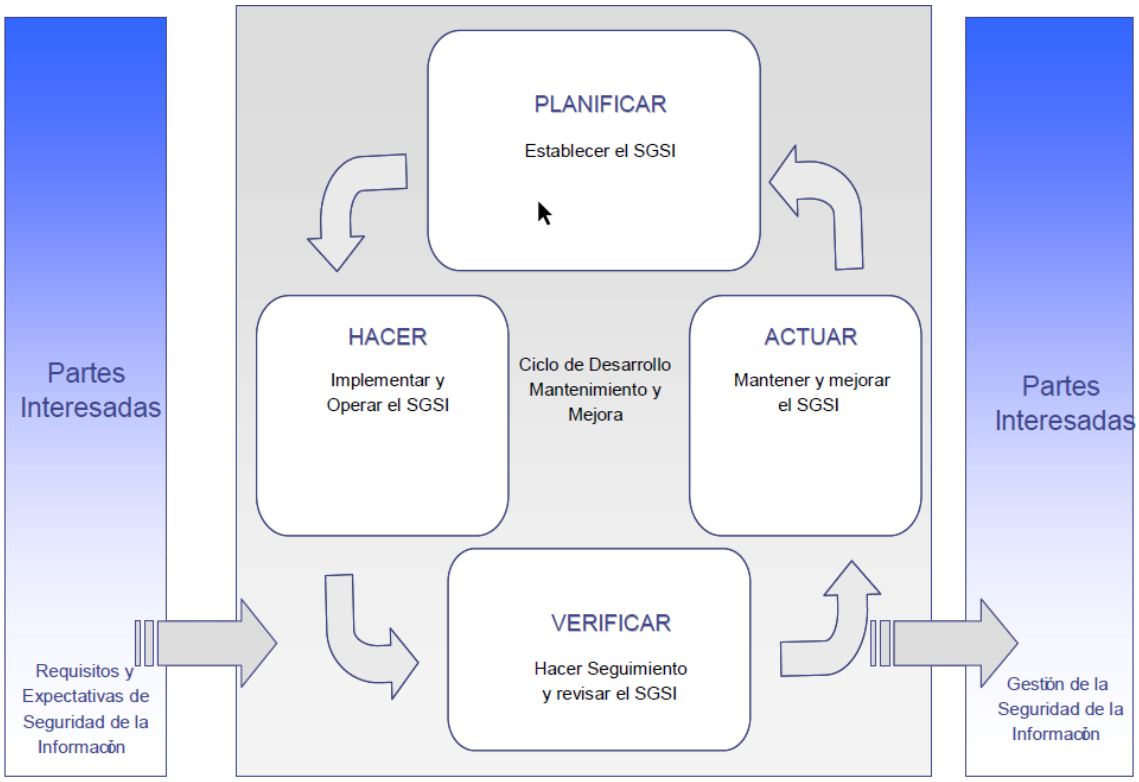
6. Política de Gerencia Tecnologías de Información y Comunicación

Estamos comprometidos en satisfacer las expectativas tanto de los usuarios externos como internos de la tal manera que los diferentes procesos adopten buenas prácticas que permitan garantizar la confiabilidad, oportunidad, confidencialidad, seguridad y acceso a la información.

7. Requisitos generales

Para el desarrollo del proyecto al cual deben pertenecer miembros directivos y representantes de las áreas misionales, con el propósito de asegurar que toda la información más 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:



Modelo **PHVA aplicado al MSPI**

FASE	DESCRIPCIÓN
PLANIFICAR (establecer el MSPI)	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 el MSPI)	Implementar y operar la política, los controles, procesos y procedimientos del MSPI
VERIFICAR (hacer seguimiento y revisar el MSPI)	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 MSPI)	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.

Para planear y gestionar la implementación del MSPI 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.

8. Establecimiento y gestión del MSPI

8.1. Establecimiento del MSPI

El hospital realizará 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:
    - 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 alineada con el contexto organizacional estratégico de gestión del riesgo en el cual tendrá lugar el establecimiento y mantenimiento del 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.
    - 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.

8.2. Implementación y operación del MSPI

El hospital:

- Formulará 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 van a usar estas mediciones con el fin de valorar la eficacia de los controles 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.

8.3. Seguimiento y revisión del MSPI

El hospital 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, y de esta manera impedir incidentes de seguridad mediante el uso de 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 el cumplimiento de la política y objetivos del MSPI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.
- 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 del MSPI.

8.4. Mantenimiento y mejora del MSPI

Regularmente el hospital 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.

9. 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.

10. Responsabilidades de la dirección

La dirección del hospital 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.

10.1. Gestión de recursos

Provisión de recursos

El hospital 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.

11. Auditorías internas del MSPI

El hospital 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.

12. Revisión 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.
- Las obligaciones contractuales.
- Los niveles de riesgo y/o niveles de aceptación de riesgos.
- Los recursos necesarios.
- La mejora a la manera en que se mide la eficacia de los controles.

13. Mejora del MSPI

Mejora continua

El hospital 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 emprender acciones para eliminar la causa de no conformidades asociadas con los requisitos del MSPI, con el fin de prevenir que ocurran nuevamente.

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.

14. Plan de trabajo

ID	Actividad	2021												2022												2023												2024		
		Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Enero	Febrero	Marzo
MSPI01	Planeación de la implementación MSPI																																						
MSPI02	Definición de políticas genéricas de seguridad																																						
MSPI03	Implementación dispositivo de seguridad perimetral																																						
MSPI04	Implementación MSPI																																						
MSPI05	Gestión y operación MSPI																																						
MSPI06	Mantenimiento y mejora MSPI																																						
MSPI07	Auditoría interna																																						
MSPI08	Revisión del MSPI por la dirección																																						
MSPI09	Mejora MSPI																																						

Nelson Leonardo Fierro González
Gerente E.S.E. Hospital del Rosario