HOSPITAL DEL SARARE
Empresa Social del Estado

Plan de Privacidad y Seguridad de la Información.

Proceso de apoyo- Gestión de las tecnología e información - Gestión de las TIC's.

Sistema Integrado de Gestión

WWW.HOSPITALDELSARARE.GOV.CO

Evolucionamos pensando en Usted

CONTENIDO

INTRODUCCION

La ESE HOSPITAL DEL SARARE, identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la entidad, razón por la cual es necesario que la ESE establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Por tal razón se adopta el Modelo de seguridad y privacidad de la información MSPI bajo los lineamientos del Ministerio de las TIC's a través de la estrategia de gobierno en línea, bajo las mejores prácticas para su diagnóstico, planificación, implementación, mantenimiento y mejoramiento continuo.

La planificación del Modelo de seguridad y privacidad de la información MSPI en el Hospital del Sarare E.S.E debe responder a los requisitos legales vigentes en Seguridad de la información, objetivos y metas institucionales, al tamaño de la entidad, las necesidades y expectativas de las partes interesadas y los requisitos del Sistema integrado de gestión SIG.

El Modelo de seguridad y privacidad de la información MSPI debe llevarnos preservación de la confidencialidad, integridad, disponibilidad de la información, garantizando la privacidad y protección de la misma, implementando un proceso de administración de los riesgos que brinde confianza a todas las partes interesadas.

La seguridad de la información es una prioridad para LA ESE y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas

1. OBJETIVO.

- Definir las actividades para la implementación del Modelo de Seguridad y Privacidad de la Información MSPI del Hospital del Sarare.

2. ALCANCE.

- Será aplicable a todos los procesos estratégicos, misionales, de apoyo, funcionarios y contratistas que tengan acceso, creen, procesen, transmitan o resguarden información de la institución de nuestros usuarios**.**

3. DEFINICIONES.

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **Activos de información:** Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.

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

- **Confidencialidad**: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- **Control:** Es toda actividad o procesos encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

- **Disponibilidad**: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- **Evento de seguridad de la información**: Se considera un Evento de Seguridad de la Información a cualquier situación identificada que indique una posible brecha en la Política de Información o falla en los controles y/o protecciones establecidas.

- **Incidente de seguridad de la información:** Un incidente de seguridad de la información se define como un acceso, uso, divulgación, modificación o destrucción no autorizada de la información y de sus usuarios; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política de Información.

- **Información:** Información almacenada o procesada física o digitalmente " Bases de datos, archivos de datos, contratos, acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, material de formación o capacitación, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos de recuperación, registros de auditoria e información archivada).

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

- **Propietario/responsable de activo de información**: Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

- **Servicio:** Es cualquier acto o desempeño que una persona puede ofrecer a otra que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

- **Seguridad de la Información**: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

- **Usuario:** Es el nombre (o alias) que se le asigna a cada persona para ser identificado por el servidor, de esta manera el proveedor de Internet o de correo electrónico lo identifica, es única en cada servidor, y cada usuario tiene asignado una contraseña para poder acceder a su cuenta.
- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la

información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera

4. DESARROLLO METODOLOGICO

Se requiere prevenir y reducir los efectos indeseados a la hora de materializarse un riesgo que afecte un activo de la información, procurar la mejora continua, definir acciones para tratar los riesgos de seguridad de la información y evaluar la eficacia de las acciones tomadas; el Hospital del Sarare E.S.E identificará y clasificará los activos de la información, los riesgos de seguridad de la información y definirá las acciones a tomar bajo los lineamientos definidos por MINTIC y los establecidos en el Manual de administración de los riesgos DIR-00-M03 del Hospital del Sarare E.S.E y de acuerdo al Sistema de la información y privacidad de la Información.

Las actividades estarán definidas bajo el enfoque del ciclo de mejoramiento continuo PHVA:

Ilustración 1 – Marco del Sistema de la seguridad y privacidad de la información
Fuente: PHVA: Procedimiento lógico y por etapas para la mejora continua-Safetya.com

MARCO LEGAL

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 1078 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.”

decreto 612 de 2018: “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.”

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos

personales.

4.1 DIAGNOSTICO

4.1.1 EVALUACIÓN INICIAL

Determinar el estado actual, nivel madurez y cumplimiento de los requisitos del Modelo de gestión de seguridad y privacidad de la información de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC en el Hospital del Sarare E.S.E.

4.1.2 COMPRENSIÓN DE LA ORGANIZACIÓN Y ANALISIS DE CONTEXTO

Realizar un análisis del entorno y permita establecer el Contexto estratégico del Hospital del Sarere E.S.E en cuanto a los factores externos e internos de la Entidad, el cual evalúe aquellos elementos que pueden influir en las capacidades en el cumplimiento de los objetivos del MPSI en el desarrollo de las actividades que realiza la Entidad en el desarrollo de su misión.

4.1.3 DETERMINACIÓN DE ALCANCE Y OBJETIVOS DEL MSPI

4.1.4 PARTES INTERESADAS

Identificar y determinar las partes interesadas internas o externas del Hospital del Sarare E.S.E que pueden influir directamente en la seguridad y privacidad de la información de la Entidad o que pueden verse afectados en caso de que estas se vean comprometidas y a su vez determinar las necesidades y/o expectativas (intereses), requisitos legales, reglamentarios y contractuales que estos tienen en relación con la seguridad y privacidad de la información. Con el fin de garantizar que la implementación del Modelo de seguridad y privacidad de la información MSPI abarca el cumplimiento de dichas necesidades y expectativas.

4.1.5 ALCANCE Y OBJETIVOS MSPI

Determinar los objetivos y límites de aplicabilidad del MSPI en el marco del modelo de operación por procesos del Hospital del Sarare E.S.E donde se establezca los procesos y recursos tecnológicos en los que se realizará la implementación del MSPI.

4.1.6 LIDERAZGO

TRD.322.1.28.126

La alta dirección muestra su liderazgo y compromiso con el MSPI mediante el comité institucional de gestión y desempeño, el cual tendrá funciones claramente definidas en todo lo relacionado con la seguridad y privacidad de la información, adoptando, implementando, manteniendo y mejorando continuamente el MSPI, el cual será soportado mediante la actualización del acto administrativo. Con el propósito de garantizar el éxito de su implementación, que permita dar cumplimento entre otras, a las siguientes acciones:

- Establecer y publicar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información.
- Garantizar la adopción de los requisitos del MSPI en los procesos de la Entidad,
- Comunicar en la Entidad la importancia del MSPI.
- Planear y disponer de los recursos necesarios (presupuesto, personal, tiempo, etc.) para la adopción del MSPI.
- Asegurar que el MSPI consiga los resultados previstos.
- Realizar revisiones periódicas de la adopción del MSPI; dos veces por año y en las que el gerente deberá estar presente.

4.1.8 POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Realizar la política general de seguridad y privacidad de la información que establezca la base del comportamiento de los funcionarios, contratistas y terceros sobre la información obtenida, generada o procesada por la Entidad.

4.1.9 ROLES Y RESONSABILIDADES DEL MSPI

Definir los roles y responsabilidades necesarios para la implementación, administración, operación, mantenimiento y mejora del Modelo de gestión seguridad y privacidad de la información MSPI los cuales se articularán de acuerdo a la estructura organizacional del Hospital el Sarare E.S.E y el modelo de operación por procesos, áreas o dependencias y comité institucional de gestión y desempeño. Estos roles y responsabilidades deberán ser integrados en la **Matriz de responsabilidad y autoridad del Sistemas Integrados de Gestión SGI - SGI-00-F09** los cuales deben ser adoptados, monitoreado su desempeño, reporte y seguimiento mediante el comité institucional de gestión y desempeño de la institución. Garantizar su socialización a todos los colaboradores de la institución.

Establecer el **rol del Oficial de seguridad y privacidad de la información** y definir el equipo humano necesario para coordinar la implementación del MSPI mediante acto administrativo; el responsable designado deberá ser incluido como miembro del comité de gestión institucional de gestión de desempeño con voz y voto y en el comité de control interno tendrá voz.

4.2 PLANIFICACIÓN

4.2.1 IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN E INFRAESTRUCTURA CRÍTICA

Estructurar una metodología que permita identificar y clasificar los activos de Información, teniendo en cuenta que son considerados activos de la información cualquier elemento que tenga valor para el Hospital del Sarare E.S.E en el contexto de la seguridad digital y son clasificados así:

- **Información:** Información almacenada o procesada física o digitalmente " Bases de datos, archivos de datos, contratos, acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, material de formación o capacitación, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos de recuperación, registros de auditoria e información archivada).

- **Software:** Aplicaciones, herramientas de desarrollo, utilidades

- **Hardware:** son activos físicos como, por ejemplo, equipos de cómputo y de comunicaciones, medios removibles, entre otros que por su criticidad son considerados activos de la información, no solo activos fijos)
- **Servicios:** Servicios de computación y comunicaciones, tales como Internet, correo electrónico, páginas de consulta, directorios compartidos e intranet, entre otros

- **Personas:** Aquellas personas que, por su conocimiento, habilidades, experiencia y criticidad para el proceso, son consideradas activos de la información.

Se implementará un mecanismo de recolección de los activos de información de los diferentes procesos y subprocesos del Hospital del Sarare E.S.E el cual debe tener en cuenta los siguientes requerimientos:

APARTADO	DESCRIPCIÓN
Proceso al que pertenece	Identificar el proceso al que pertenece el activo de la información de acuerdo al mapa de procesos
Subproceso al que pertenece	Identificar el subproceso al que pertenece el activo de la información de acuerdo al mapa de procesos

Responsable	Líder responsable del subproceso
Nombre del Activo	Nombre con el se conoce el activo de la información
Identificación o etiquetado	Se describe el número institucional con el cual se identifica el activo de información (Solo aplica para software, hardware, red de datos y equipos tecnológicos e informáticos).
Descripción del activo	Describir la información de valor que contiene el activo de información
Tipo de activo	El activo se clasifica según lo definido en este documento en el apartado 4.1.1
Contenedor	Son los medios de almacenamiento digitales empleados para guardar el activo de la información identificado.

4.2.1 GESTION Y CLASIFICACION DE LOS ACTIVOS

Una vez identificado y realizado el inventario de activos de la información deberá ser clasificado con base a los criterios de clasificación definidos en la guía 5: Gestión y Clasificación de los activos de MINTIC, de acuerdo a los siguientes criterios:

- **Según su Confidencialidad**:

Los activos de información son clasificados **por confidencialidad** cuando se requiere o no permisos para acceder a la información y su disponibilidad, esto determina cual información puede ser autorizada para ser revelada o no, a individuos, entidades o procesos.

CLASIFICACIÓN POR CONFIDENCIALIDAD	CRITERIO
INFORMACION PÚBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, económico, operativo y/o pérdida de imagen.

INFORMACION PÚBLICA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACIÓN PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

- **Según su integridad**

La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.

CLASIFICACIÓN POR INTEGRIDAD	CRITERIO
A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

- **Según su disponibilidad**

La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.

CLASIFICACIÓN POR DISPONIBILIDAD	CRITERIO
1 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económico, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
3 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

4.2.2 ADMINISTRACIÓN DE LOS RIESGOS

La administración de los riesgos se realizará bajo los lineamientos definidos Hospital del Sarare E.S.E en sus políticas; administración de los riesgos, gobierno digital, seguridad digital, seguridad informática, tratamiento de datos, trasparencia y acceso a la información, y se realizará de acuerdo a lo establecido en el **Manual de administración de los riesgos DIR-00-M03** el cual adopta la metodología de propuesta por el DAFP (2020) Guía de administra del riesgo y el diseño de controles en entidades públicas.

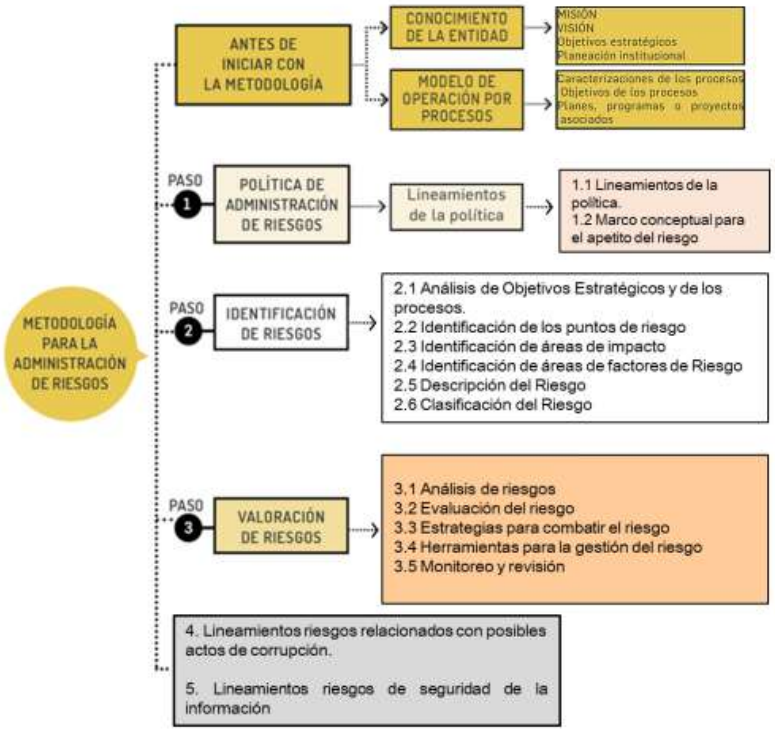

Ilustración 2: Modelo de administración del riesgo
Fuente: Guía de administración del riesgo y el diseño de controles en entidades públicas.

La administración de los riesgos asociados a la seguridad de la información se realizará en todos y cada uno de los procesos estratégicos, misionales, apoyo, control y seguimiento del Hospital del Sarare E.S.E mediante la construcción del Mapa de riesgos del proceso/subproceso que integrado los riesgos de seguridad de la información y la determinación de los respectivos planes de mejoramiento .

4.2.3 PLAN DE TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaborar el plan de tratamiento de los riesgos de seguridad y privacidad de la información que permita implementar cada una de las etapas definidas en el Manual de administración de los riesgos **DIR-00-M03 del Hospital del Sarare E.S.E** el cual permita identificar, evaluar, valorar, priorizar y controlar los riesgos de seguridad y privacidad de la información.

TRD.322.1.28.126

4.2.4 DOCUMENTACIÓN DEL MSPI

Elaborar documentación de operación (formatos de procesos, procedimientos y documentos debidamente definidos y establecidos) del Sistema de Gestión de seguridad de la información MSPI

- Procedimiento y/o guía de identificación y clasificación de activos de información.
- Procedimiento Continuidad del Negocio.
- Procedimientos operativos para gestión de TI
- Procedimiento para la gestión de eventos e incidentes de seguridad de la información
- Procedimiento para la gestión de vulnerabilidades de seguridad de la información.
- Entre otros que se identifique la necesidad.

En cuanto al control documental, auditorías internas y planes de mejoramiento y seguimiento institucional se regirán bajo los lineamientos determinados por el Sistema integrados de gestión SGI de la Institución.

4.2.5 COMPETENCIA, TOMA DE CONCIENCIA Y COMUNICACION

Con el fin de asegurar que todos los colaboradores del Hospital del Sarare E.S.E cuenten con los conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del modelo de seguridad y privacidad de la información, buscando concientizarlos al igual que las partes interesadas en la importancia de la protección de la información, se deben establecer las necesidades de capacitación y articularlas al Plan de capacitaciones Institucional PIC y al plan de capacitaciones y comunicaciones del Sistemas integrados de gestión SIG del Hospital del Sarare E.S.E.

Se deben Identificar las necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información e Integrarlas a la **Matriz de comunicaciones del sistema integrados de gestión SIG-01-F11**. Garantizar una correcta comunicación, sensibilización y concientización con respecto a la seguridad y privacidad de la información, en la que todos los colaboradores del Hospital del Sarare E.S.E estén al tanto de la política de seguridad y privacidad, conozcan su rol, responsabilidad y autoridad en el cumplimiento del MSPI, además de los beneficios y consecuencias al no dar cumplimiento a las políticas y lineamientos definidas en el Modelo de seguridad y privacidad de la información del Hospital del Sarare E.S.E.

4.2.7 PLANIFICACIÓN DE LOS CAMBIOS

TRD.322.1.28.126

Una vez identificado las necesidades de cambios que afecten la integridad del Sistema de seguridad de la Información se trataran de acuerdo a los lineamientos definidos por el Sistema Integrados de Gestión SGI en su **Procedimiento de gestión de los cambios SIG-01-P06**

4.2.8 PLAN DE DIAGNÓSTICO PARA LA TRANSICIÓN DE LA ENTIDAD DE IPV4 A IPV6.

Planificar las etapas de desarrollo de la evaluación de las condiciones iniciales en las que se encuentra el Hospital del Sarare E.S.E para realizar transición de IPV4 a IPV6.

4.3 IMPLEMENTACIÓN

4.3.1 EJECUCIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Ejecutar el plan de tratamiento de los riesgos transversales de seguridad de la información identificados en la fase de planificación que fue presentado en el comité de gestión y desempeño.

4.3.2 PLAN DE DIAGNÓSTICO PARA LA TRANSICIÓN DE LA ENTIDAD DE IPV4 A IPV6.

Ejecutar la planificación realizada para el desarrollo de la evaluación de las condiciones iniciales en las que se encuentra el Hospital del Sarare E.S.E para realizar transición de IPV4 a IPV6.

4.3.3 DETERMINACIÓN DE INDICADORES DEL MSPI

Definir los indicadores para medir la gestión del modelo de seguridad y privacidad de la información MSPI y establecer los mecanismos para su medición. Estos indicadores deben permitir verificar la eficacia y efectividad de los controles implementados para mitigar los riesgos de seguridad de la entidad, los cuales deben incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 “Protección de datos personales”, Ley 1712 de 2014 “Ley de Transparencia y Acceso a la Información Pública”, Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue.

4.3 EVALUACIÓN DEL DESEMPEÑO

4.3.1 SEGUIMIENTO, MEDICIÓN, ANALISIS Y EVALUACIÓN

Durante esta etapa se deben realizar seguimientos, medición, análisis y evaluación del MSPI para determinar los avances en la gestión, los logros de los resultados y metas propuestas durante la implementación del MSPI de acuerdo a lo establecido en la **Política institucional de evaluación y seguimiento** adoptada mediante resolución 248 del 14 de diciembre del 2020**.**

4.3.2 AUDITORIAS

El modelo de seguridad y de temas normativos y de cumplimiento de seguridad de la información aplicables a la entidad, será auditado de acuerdo con el plan de auditoria y seguimiento aprobado por la Alta Dirección. Las auditorías internas se deberán llevar a cabo para la revisión del Sistema de Gestión de Seguridad 'MSPI' de la Información implementado en la entidad, con la finalidad de verificar el cumplimiento de los requisitos; normativos y reglamentarios, los requisitos establecidos por MSPI, los, objetivos, controles, procesos y procedimientos del MSPI.

4.4 REVISIÓN POR LA DIRECCIÓN

El Modelo de seguridad y privacidad de la información debe ser revisado por la alta dirección la cual está representada por el comité Institucional de gestión y desempeño; revisará y evaluará los resultados obtenidos de la implementación del MSPI, frente a los requisitos técnicos y normativos; Seguridad y privacidad de la información, Seguridad digital, Política general de Seguridad y privacidad de la información, Manual de Políticas de Seguridad y Privacidad de la Información y así pueda determinar su conveniencia, adecuación y eficacia.

4.5 MEJORA CONTINUA

Una vez identificadas No conformidades y/o productos no conformes frente a los riesgos de seguridad y privacidad de la información se deben gestionar acorde a lo definido el **procedimiento de mejoramiento y seguimiento institucional SIG-01-P02** con el fin de realizar acciones correctivas, optimizar procesos o controles y mejorar el nivel de madurez del MSPI. Identificar las acciones asociadas a la mejora continua del MSPI y de los procesos.

5. BIBLIOGRAFÍA.

ISO/IEC 27001:2013
Anexo 1 Modelo de Privacidad y Seguridad de la información del MINTIC

6. CONTROL DE CAMBIOS

REVISIÓN N°	FECHA DE APROBACIÓN DD/MM/AA	DESCRIPCIÓN DE CAMBIOS
00	17-12-2021	Creación del Documento
	-	