Plan de seguridad y privacidad de la información

2021

@hospital alejandromaestre
hospital alejandro maestro sierra

Dirección: calle 7ª N° 9-276
Telefono 3205699724
Email: gerencia@hospitalariguani.gov.co
El Difícil -Magdalena

CONTENIDO

1. INTRODUCCIÓN..... 4
2 OBJETIVOS..... 5
2.1 GENERAL..... 5
2.2 ESPECIFICOS: 5
3 ALCANCE 5
4 MARCO LEGAL 6
5 NORMAS TÉCNICAS 6
6 DEFINICIONES 7
7 ESTRUCTURA DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN..... 11
7.1 FASE DE DIAGNOSTICO..... 11
7.2 FASE DE PLANIFICACION 11
7.3 FASE DE IMPLEMENTACION..... 13
7.4 FASE DE EVALUACION DE DESEMPEÑO 14
7.5 FASE DE MEJORA CONTÍNUA 15

INTRODUCCIÓN

Para la ESE Hospital Alejandro Maestre Sierra la información es un activo que cobra importancia en la optimización de sus procesos que se refleja en la satisfacción de los pacientes, por ende se hace necesario definir el proceso necesario para colocar en marcha la implementación del Modelo de Seguridad de La Información expedido por el Ministerio de Tecnología y Comunicaciones del Estado Colombiano.

La estrategia de Gobierno en Línea - GEL, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente

En el Plan Nacional de Desarrollo 2015-2018 se reconoce la seguridad y privacidad de la información, como un factor fundamental para la apropiación de las TIC; así mismo plantea un marco de seguridad necesario, que permita garantizar la prestación de servicios a los ciudadanos a través de las TIC, y que debe estar respaldado por unos planes, políticas y procedimientos orientados a preservar y minimizar el impacto a los activos de información de la entidad por eventos como fallas de seguridad, perdida del servicio y disponibilidad del servicio.

El Plan de Seguridad y Privacidad de la Información y Continuidad de TI para estar acorde con las buenas prácticas de seguridad y continuidad deberá ser actualizado periódicamente; así mismo recoger los cambios técnicos de la norma, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

La seguridad de la información garantiza que los responsables de la información sean capaces de gestionar la información de forma segura, independientemente del formato o soporte en el que se encuentra. Mediante el proceso de Gestión de TI y el modelo de seguridad y privacidad de la información y de continuidad de TI, se trabajará en el fortalecimiento de la seguridad de la información en el LA ESE, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación colombiana.

2 OBJETIVOS

2.1 GENERAL

Definir en el Plan de Seguridad y Privacidad de la Información, los lineamientos que respondan asertiva y oportunamente a eventos que afecten la seguridad de la información.

2.2 ESPECIFICOS:

- Definir las fases para diseñar, implementar y evaluar la Estrategia de Seguridad y privacidad de la Información.
- a la disminución de incidentes y requerimientos relacionados con la seguridad de la información.
- Facilitar la implementación de los lineamientos del Marco de Referencia de
- Seguridad de la Información de Gobierno en Línea, relacionados con la seguridad de la información.

3. ALCANCE

Este documento contempla la estructura de gobierno y los lineamientos principales para la seguridad y privacidad de la información en la ESE. Los lineamientos definidos en este documento deben ser conocidos y cumplidos por empleados, contratistas y todos los terceros que tengan acceso, almacenen, procesen o trasmitan información de la institución o sus pacientes.

La estructura del Plan se basa en la metodología propuesta por MINTIC para el componente de Seguridad y Privacidad de la Información. El presente plan, aplican a todos los procesos soportados por el proceso de Apoyo Tecnológico de la ESE.

4. MARCO LEGAL

- Ley 1757 de 2015. Disposiciones en materia de promoción y protección del derecho a la participación democrática
- Ley 1712 de 2014. Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional
- Ley 1437 de 2011. Código de Procedimiento Administrativo y de lo Contencioso Administrativo
- Ley 1341 de 2009. 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 de Espectro y se dictan otras disposiciones
- Ley 1266 de 2008. Disposiciones generales de habeas data y se regula el manejo de la información
- Ley 962 de 2005. Disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos
- Ley 594 de 2000. Dicta la Ley General de Archivos

@hospitalalejandromaestre
hospitalalejandromaestresierra
Dirección: calle 7° N° 9-378
Teléfono 3205600724
Email: gerencia@hospitalariguani.gov.co
El Difícil -Magdalena

- Ley 527 de 1999. Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones
- Decreto - Ley 019 de 2012. Normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública
- Decreto 415 de 2016. Lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones a través del posicionamiento de los líderes de áreas TI
- Decreto 1078 de 2015. Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Decreto 103 de 2015. Reglamenta parcialmente la Ley 1712 de 2014
- Decreto 2573 de 2014. Lineamientos generales de la Estrategia de GEL
- Decreto 333 de 2014. Reglamenta parcialmente la ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales
- Decreto 235 de 2010. Regula el intercambio de información entre entidades para el cumplimiento de funciones públicas
- Decreto 1151 de 2008. Lineamientos generales de la Estrategia de Gobierno en línea.

5. NORMAS TÉCNICAS

- ISO/IEC 27001- Seguridad de la Información
- ISO 31000 – Gestión de Riesgos

6. DEFINICIONES

- Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas,

soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- Análisis del impacto al negocio (BIA por sus siglas en inglés). Proceso del análisis de actividades las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas.
- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- Confidencialidad: La propiedad que esa información esté disponible y no sea divulgada a personas o procesos no autorizados.
- Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art3)
  - Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
  - Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
  - Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y

@hospitalalejandromaestre
hospital alejandro maestre sierra
Dirección: calle 7° N° 9-378
Teléfono 3205600724
Email: gerencia@hospitalariguani.gov.co
El Difícil -Magdalena

garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

- Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- Disponibilidad: La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.
- Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- Información Pública: Es aquella 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.
- Integridad: La propiedad de salvaguardar la exactitud e integridad de los activos de información.
- Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.
- Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.
- Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer

@hospitalalejandromaestre
hospital alejandro maestre sierra
Dirección: calle 7° N° 9-378
Teléfono 3205600724
Email: gerencia@hospitalariguani.gov.co
El Difícil -Magdalena

protección a los datos personales de los titulares tales como acceso controlado, cifrado etc.

- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- Seguridad de la información: Son todos los controles técnicos y metodológicos que permiten mitigar los riesgos a los que se expone la información.
- Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- Tecnología de la Información: (TI) Es el estudio, diseño, desarrollo, implementación, soporte y administración de los sistemas de información basados en computadoras, particularmente aplicaciones de software y hardware de computadoras".
- Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- Vulnerabilidad: Son la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño.

7. ESTRUCTURA DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La ESE Hospital Alejandro Maestre Sierra ha estructurado el Plan de Seguridad y Privacidad de la Información en concordancia con los marcos legal y conceptuales del Estado relacionadas con la Seguridad y privacidad de la Información y garantizará la Confidencialidad, Integridad y Disponibilidad de la Información presentados anteriormente, que permita cumplir con el objetivo definido en dicho plan, para esto se definen las actividades que se describen a continuación:

7.1 FASE DE DIAGNOSTICO

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información. Para esta fase tenemos como metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad.
- Realizar el diagnóstico de las condiciones en que se encuentran los activos de información administrados por la entidad.

Para ello, utilizaremos las siguientes herramientas publicadas en http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html :

- Herramienta de diagnostico
- Instructivo para el diligenciamiento de la herramienta
- Guía No 1 - Metodología de Pruebas de Efectividad

7.2 FASE DE PLANIFICACION

En esta fase se pretenderá cumplir con las siguientes metas:

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Se proyectará la Política de Seguridad y Privacidad de la información que estará contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección del LA ESE para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información.
La política contendrá una declaración general por parte de la Alta Dirección, donde se especifique sus objetivos, alcance, nivel de cumplimiento. La política será sometida a aprobación y será divulgada al interior del LA ESE. Se tomará de base la Guía 2 - Política General MSPI del Modelo de Seguridad y privacidad de la Información de MinTic.

La actualización de la política debe realizarse al menos una vez al año o cuando se evidencie que nuevas amenazas pueden afectar la Seguridad de la Información

en LA ESE, todos los cambios que surtan en la política debe ser aprobado y divulgado al interior de la entidad.

POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Se desarrollará un manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior del LA ESE; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información

En el manual de políticas de la entidad, se debe explicar de manera general, las políticas, los principios de seguridad y la normatividad pertinente. LA ESE deberá evaluar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación.

PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN.

Se desarrollarán y formalizarán los procedimientos que permitan gestionar la seguridad y privacidad de la información en cada uno de los procesos definidos en LA ESE.

Para desarrollar esta actividad utilizaremos, la Guía 3 - Procedimiento de Seguridad de la Información

ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La entidad debe definir mediante un acto administrativo (Resolución) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad.

Para desarrollar estas actividades, tomaremos la Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.

INVENTARIO DE ACTIVOS DE INFORMACIÓN.

Realizar el Inventario de los activos de información por parte de cada proceso, siendo el proceso de Apoyo Tecnológico quien recopila la información

generando un solo documento con todos los activos de la entidad, con el fin de definir la criticidad, sus propietarios, custodios y usuarios.

Para desarrollar estas actividades, tomaremos La Guía No 5 - Gestión De Activos.

IDENTIFICACIÓN, VALORACIÓN Y TRATAMIENTO DE RIESGOS.

El LA ESE deberá definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, así como la declaración de aplicabilidad. Para conseguir una integración adecuada entre el MSPI y la guía de gestión del riesgo emitida por el DAFP respecto a este procedimiento, se emplearán los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos por el LA ESE.

Para definir la metodología, la entidad hará uso de buenas prácticas vigentes tales como: ISO 27005, ISO 31000 y la Guía No 7 - Gestión de Riesgos emitida por el MinTIC.

Para la elaboración del plan de tratamiento de riesgos y la declaración de aplicabilidad, utilizaremos la Guía No 8 - Controles de Seguridad.

PLAN DE COMUNICACIONES.

La Entidad definirá un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad y privacidad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) del LA ESE.

Este plan será ejecutado, con el aval de la Gerencia, a todas las áreas del LA ESE.

Para estructurar dicho plan se utilizará la Guía No 14 – plan de comunicación, sensibilización y capacitación.

PLAN DE TRANSICIÓN DE IPV4 A IPV6.

Para llevar a cabo el proceso de transición de IPv4 a IPv6 en el LA ESE, se ejecutará la fase de planeación establecida en la Guía No 20 – Transición de IPv4 a IPv6 para Colombia que indica las actividades específicas a desarrollar.

7.3 FASE DE IMPLEMENTACION

PLANIFICACIÓN Y CONTROL OPERACIONAL.

La ESE deberá planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos.

La ESE deberá tener información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado, adicionalmente, deberá llevarse un control de cambios que le permitan tomar acciones para mitigar efectos adversos cuando sea necesario.

IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS.

Se deberá implementar el plan de tratamiento de riesgos de seguridad de la información, en el cual se identifica el control a aplicar para llevar cada uno de los riesgos a un nivel aceptable para la entidad, en donde la base para ejecutar esta actividad es la Guía No 8 - de controles de seguridad y privacidad del MSPI.

Es preciso tener en cuenta que la aplicación del control sobre los riesgos detectados debe estar aprobados por el dueño de cada proceso.

INDICADORES DE GESTIÓN.

El LA ESE deberá definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información.

Los indicadores buscan medir:

- Efectividad en los controles.
- Eficiencia del MSPI al interior de la entidad.
- Proveer estados de seguridad que sirvan de guía en las revisiones y la mejora continua.
- Comunicar valores de seguridad al interior de la entidad.
- Servir como insumo al plan de control operacional.

La Guía No 9 - Indicadores de Gestión, brinda información relacionada para poder llevar a cabo la realización de esta actividad.

PLAN DE TRANSICIÓN DE IPV4 A IPV6.

Se deberá generar el documento detallado con el plan de transición e implementación del protocolo IPv6 en la entidad.

Las guías de apoyo para esta labor son “Guía de Transición de IPv4 a IPv6 para Colombia” y “Guía de Aseguramiento del Protocolo IPv6”.

7.4 FASE DE EVALUACION DE DESEMPEÑO

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas. Se deberán obtener dos documentos:

PLAN DE REVISIÓN Y SEGUIMIENTO A LA IMPLEMENTACIÓN DEL MSPI.

En esta actividad la entidad debe crear un plan que contemple las siguientes actividades:

- Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
- Seguimiento a la programación y ejecución de las actividades de autorías
- internas y externas del MSPI.
- Seguimiento al alcance y a la implementación del MSPI.
- Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
- Medición de los indicadores de gestión del MSPI
- Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del MSPI)

Este plan deberá permitir la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas; deben ser medibles permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.

La Guía No 16 - Evaluación del Desempeño, brinda información relacionada para poder llevar a cabo la realización de esta actividad.

PLAN DE EJECUCIÓN DE AUDITORIAS

La entidad debe generar un documento donde se especifique el plan de auditorías para el MSPI, donde especifique la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes. Se debe llevar a cabo auditorías y revisiones independientes a intervalos planificados que permitan identificar si el MSPI es conforme con los requisitos de la organización, está implementado adecuadamente y se mantiene de forma eficaz; así mismo es necesario difundir a las partes interesadas, los resultados de la ejecución de las auditorías.

Es importante conservar la información documentada como evidencia de los resultados de las auditorías.

La Guía No 15 - Guía de Auditoría, brinda información relacionada para poder llevar a cabo la realización de esta actividad.

7.5 FASE DE MEJORA CONTÍNUA

En esta fase la Entidad debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.