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

JORGE LEMUS BELLO
GERENTE

GUAMAL – MAGDALENA
2024

Contenido

OBJETIVOS 3

OBJETIVO GENERAL 3

OBJETIVOS ESPECÍFICOS 3

ALCANCE 3

POLÍTICA DE SEGURIDAD DE LA INFORMACION 3

MARCO LEGAL 4

DEFINICIONES 4

DIRECCIONAMIENTO ESTRATEGICO DE LA E.S.E. HOSPITAL NUESTRA SEÑORA DEL CARMEN DE GUAMAL, MAGDALENA 7

MISIÓN 7

VISIÓN 7

CÓDIGO DE INTEGRIDAD 7

OBJETIVO DEL CÓDIGO DE INTEGRIDAD 8

ALCANCE DEL CÓDIGO DE INTEGRIDAD 8

VALORES DE INTEGRIDAD 8

MAPA DE PROCESO 8

ORGANIGRAMA 10

METODOLOGÍA Y OPERACIÓN DEL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 11

INTRODUCCIÓN

Mediante la definición del Plan de Tratamiento de Riesgos la E.S.E. Hospital Nuestra Señora del Carmen de Guamal, Magdalena, busca mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad, Perdida de Integridad y Perdida de Disponibilidad), en la información digital, evitando aquellas situaciones que impidan el logro Estratégicos del Hospital.

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes en los activos de información del Hospital, estas acciones son organizadas en forma de medias de seguridad denominados controles, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad.

Las anteriores medidas se definen teniendo en cuenta la información del análisis de riesgos, sobre la plataforma informática y las necesidades del Proceso de Gestión de la Infraestructura de TIC de la entidad hospitalaria, en cuanto a la seguridad de la información y proporciona las herramientas necesarias para definir cada una de las características de las medidas y la definición de los pasos a seguir para su ejecución.

OBJETIVOS

OBJETIVO GENERAL

Vincular la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información con la Metodología de riesgos del DAFP.

OBJETIVOS ESPECÍFICOS

Identificar los riegos, Amenazas y vulnerabilidades de seguridad y privacidad de la información

Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital de manera integral.

Reducir toda posibilidad de que una brecha o evento produzca determinado impacto bien en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad de la información.

ALCANCE

La gestión y el tratamiento de riesgos de seguridad y privacidad de la información, podrá será aplicada sobre cualquier proceso de la empresa, a cualquier sistema de información, Infraestructura informática o aspecto particular de control de la Entidad, a través de la metodología establecida para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formatos que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información, análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye implementación de controles, recomendaciones para su seguimiento, monitoreo y evaluación.

POLÍTICA DE SEGURIDAD DE LA INFORMACION

La Empresa Social del Estado Hospital Nuestra Señora del Carmen de Guamal Magdalena, mediante la política de Seguridad y Privacidad de la Información, protege, preserva la confidencialidad, integridad, disponibilidad, autenticidad, mediante una gestión de riesgos y la implementación de controles físicos y digitales previniendo así incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua.

MARCO LEGAL

- **Ley 1273 de 5 de enero de 2009:** Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones entre otras disposiciones.

- **Ley 23 de 1982:** Sobre derechos de autor

- **Ley Estatutaria 1266 de 2008:** Por la cual se dictan las disposiciones generales de hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Para conocer más de esta Ley,

- **Ley 1581 de 2012:** la cual se dictan disposiciones generales para la Protección de Datos Personales.

- **ISO IEC 27001-2013:** Estándares internacionales sobre tecnología de la información, técnicas de seguridad, Administración de seguridad de la información, los cuales proporcionan un marco de gestión de la seguridad de la información, utilizable por cualquier tipo de empresa.

- **ISO IEC 27002-2013:** Es un estándar para la seguridad de la información.

DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Política**: Son instrucciones mandatorios que indican la intención de la alta gerencia respecto a la operación de la organización respecto a un asunto determinado.

- **Recurso Informático:** Elementos informáticos (base de datos, sistemas operacionales, redes, equipos de cómputo, sistemas de información y comunicaciones) que facilitan servicios informáticos.

- **Administración del riesgo:** Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

- **Activo de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

- **Análisis de riesgos:** Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

- **Amenaza:** Es la causa potencial de una situación de incidente y no deseada por la organización.

- **Causa:** Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **Consecuencia:** Resultado de un evento que afecta los objetivos.

- **Criterios del riesgo:** Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

- **Control:** Medida que modifica el riesgo.

- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **Evaluación de riesgos:** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

- **Evento:** Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

- **Estimación del riesgo:** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

- **Evitación del riesgo:** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

- **Identificación del riesgo:** Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.

- **Impacto:** Cambio adverso en el nivel de los objetivos del negocio logrados.

- **Nivel de riesgo:** Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

- **Matriz de riesgos:** Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

- **Monitoreo:** Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

- **Propietario del riesgo:** Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

- **Riesgo Inherente:** Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

- **Riesgo Residual:** El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

- **Riesgo:** Efecto de la incertidumbre sobre los objetivos.

- **Riesgo en la seguridad de la información:** Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

- **Reducción del riesgo:** Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

- **Seguimiento:** Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se válida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

- **Tratamiento del Riesgo:** Proceso para modificar el riesgo" (Icontec Internacional, 2011).

- **Valoración del Riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

- **Vulnerabilidad:** Es aquella debilidad de un activo o grupo de activos de información.

- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

DIRECCIONAMIENTO ESTRATEGICO DE LA E.S.E. HOSPITAL NUESTRA SEÑORA DEL CARMEN DE GUAMAL, MAGDALENA

MISIÓN

Somos un hospital público de baja complejidad que ofrece servicios de salud con criterios de calidad, seguridad y oportunidad; contamos con un recurso humano idóneo comprometido con la mejora continua de los procesos asistenciales orientados hacia la satisfacción del usuario y su familia.

VISIÓN

En el 2023 seremos reconocidos como un hospital que ofrece servicios de salud oportunos y de calidad, apoyado en su equipo humano e infraestructura física y tecnológica, fijando como propósito el fortalecimiento de los servicios habilitados y dando apertura a nuevas estrategias de atención que permitan convertirnos en una institución eficiente y humanizada.

CÓDIGO DE INTEGRIDAD

El Código de Integridad es el principal instrumento de la Política de Integridad del MIPG, parte de la Dimensión de Talento Humano. El Decreto 1499 de 2017, en concordancia con el artículo 133 de la Ley 1753 de 2015 hizo extensiva su implementación diferencial a las entidades territoriales.

OBJETIVO DEL CÓDIGO DE INTEGRIDAD

Fomentar en los usuarios y funcionarios de la E.S.E la implementación de acciones de integridad que fortalezcan la cultura y clima organizacional, bajo acciones de servicio al usuario y su familia con eficacia y calidad humana

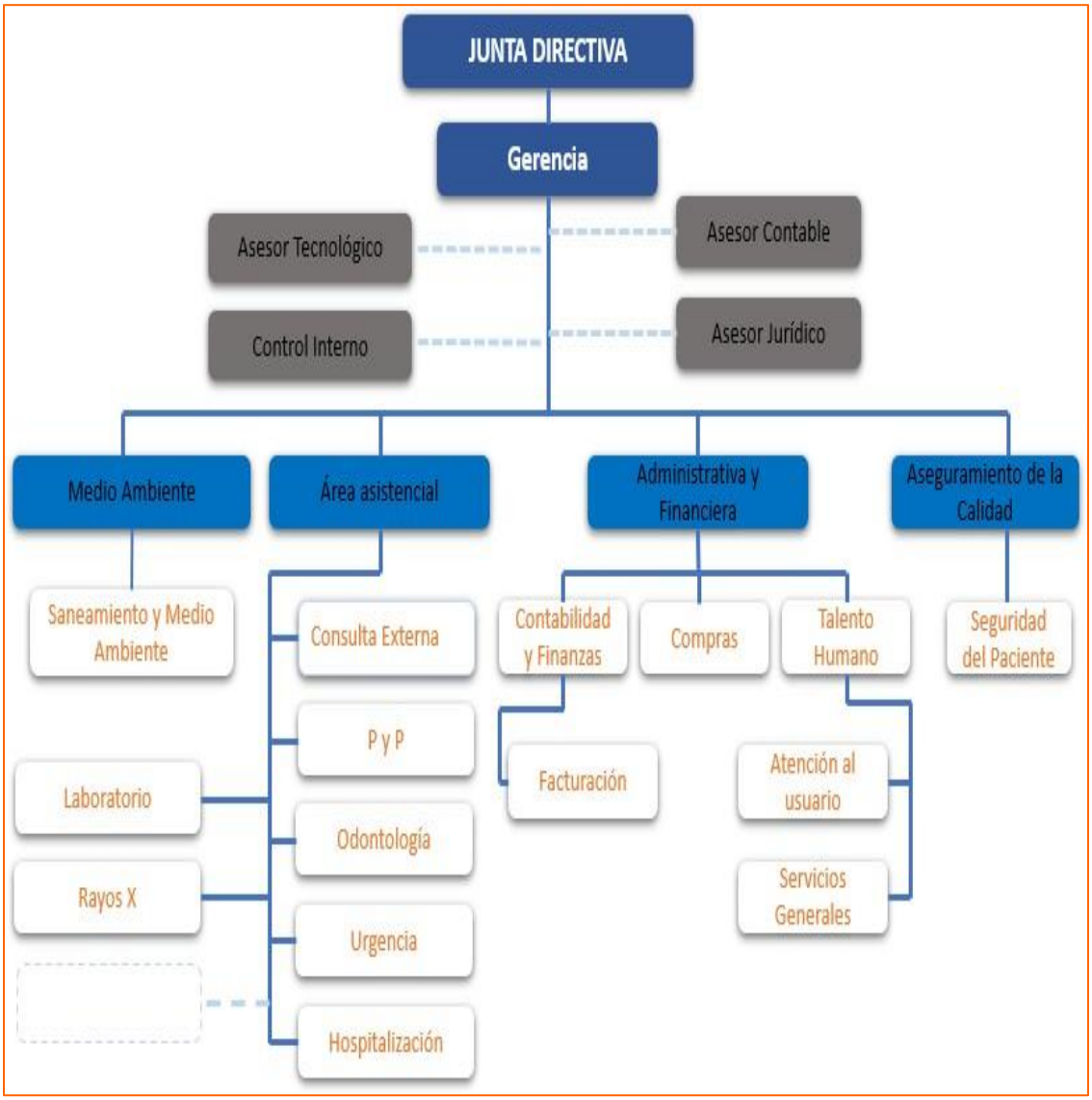
ALCANCE DEL CÓDIGO DE INTEGRIDAD

Los valores y lineamientos del presente Código serán asumidos y cumplidos de manera consciente y responsable por todos los servidores públicos y funcionarios vinculados a la E.S.E HOSPITAL NUESTRA SEÑORA DEL CARMEN y serán fomentados de manera especial por la Alta Dirección de la entidad, Equipo de Integridad y aliados claves como los comités en actividades de Talento Humano, interventores, líderes y coordinadores y jefes de áreas.

VALORES DE INTEGRIDAD

MAPA DE PROCESO

ORGANIGRAMA

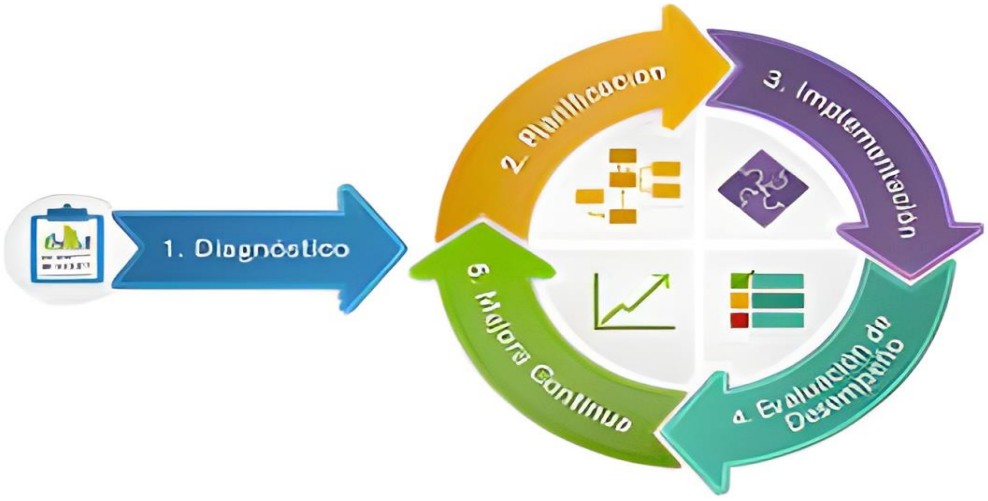


METODOLOGÍA Y OPERACIÓN DEL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la E.S.E. Hospital Nuestra Señora del Carmen de Guamal, Magdalena, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – Min TIC, a través de los decretos emitidos.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

1. Diagnosticar
2. Planear
3. Hacer
4. Verificar
5. Actuar



VALORACIÓN DEL RIESGO

Para la identificación y evaluación se toma como base el contexto estratégico que reconoce las situaciones de riesgo de origen interno y externo para la entidad; luego se procede a la identificación de los riesgos, reconociendo variables como agentes generadores, causas, efectos entre otros, para realizar posteriormente la calificación de los riesgos. A partir de los factores internos y externos, se determinan los agentes generadores del riesgo de seguridad y privacidad de la información sus causas y sus consecuencias: pérdida, daño, perjuicio o detrimento.
Para los riesgos de seguridad y privacidad se debe tener en cuenta:

IDENTIFICACIÓN DEL RIESGO

El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida.

IDENTIFICACIÓN DE LOS ACTIVOS

Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se debería llevar acabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo.

IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas) Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

IDENTIFICACIÓN DE CONTROLES EXISTENTES

Se debe realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo, la duplicidad de controles, además de esto mientras se identifican los controles se recomienda hacer una verificación para garantizar que los existentes funcionan correctamente.

IDENTIFICACIÓN DE LAS VULNERABILIDADES

Para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de amenazas comunes, la lista de inventario de activos y el listado de controles existentes. Se pueden identificar vulnerabilidades en las siguientes áreas:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión.
- Personal
- Ambiente físico
- Configuración del sistema de información.
- Hardware, software y equipos de comunicaciones.
- Dependencia de partes externas.

IDENTIFICACIÓN DE LAS CONSECUENCIAS

Para la identificación de las consecuencias es necesario tener:

- Lista de activos de información y su relación con cada proceso de la entidad.
- Lista de las amenazas y vulnerabilidades con respecto a los activos y su pertinencia.

NOTA: Una consecuencia puede ser la pérdida de la eficacia, condiciones adversas de operación, pérdida del negocio, reputación, daño, entre otros. Se deben identificar las consecuencias operativas de los escenarios de incidentes en términos de:

- Tiempo de investigación y reparación
- Pérdida de tiempo operacional
- Pérdida de oportunidad
- Salud y seguridad
- Costo financiero
- Imagen, reputación y buen nombre.

IDENTIFICACIÓN DEL RIESGO						
EVENTO		CAUSA DEL RIESGO		CONSECUENCIA	ACCIÓN	RESPONSABLES
RIESGO	DESCRIPCIÓN	CONTEXTO INTERNO	CONTEXTO EXTERNO			
	Interrupción de la operación del sistema de información	-Caída del sistema hacia los servidores Obsolescencia tecnológica de los equipos. daños por falta de mantenimiento en los equipos.	-Caída del fluido eléctrico -pérdida de señal a internet por parte de la red -Falta de equipos o servidores -Daños físicos por caídas de equipos o de alimentos	-Congestión o no continuidad en la atención por fallas en la red- -Perdida de información a causa de la contingencia. -Fallas en el proceso de facturación -eventos adversos con los pacientes que requieren del servicio	-Constante mantenimientos de equipos de cómputo. -Mantenimiento en la red y el sistema. -Mayor capacidad instalada. -Respaldo de base de datos ante perdida de información.	Sistemas Calidad Control Interno
	Instalación de cablerías en mal estado	-Uso de cablería incorrecta para su fin	-Deterioro de cables por excedo de uso. -Deterioro por agentes externos o animales roedores.	-Funcionalidad deficiente en los equipos. -Retraso en los procesos en la entidad.	Mantenimiento frecuente a equipos de cómputo e instalación eléctrica	Sistemas Calidad Control Interno

	Pérdida de información	-Fallas en las copias de seguridad. -Falta de sistemas para hacer los backup -Falta de Disco duros para realizar las copias d eseguridad	-Fallas en los fluidos eléctricos. -Fallas de los equipos de cómputo -Falta de conocimiento o para hacer los Backup	-Pérdida de información clasificada -Pérdida de base de datos personales.	-Implementación de un backup para la protección de datos personales -Capacitación al personal para el debido respaldo de datos personales	Sistemas Calidad
	Manipulación incorrecta de historia clínica	-Caída del sistema en los servidores -apagones en los equipos -	-Historias clínicas incompletas. -Datos suministrados erróneos -	-Retraso en la atención -Entrega de Historias clínicas incompletas	-Auditoria de historias clínicas. -capacitación a personal médico para correcto diligenciamiento de historias clínicas- -Buen estado de los equipos. -Mantenimiento de la red -correcta funcionalidad del sistema.	Sistemas Calidad