

E.S.E. HOSPITAL CARISMA

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN**

Elabora Carlos Arcila Ospina

Medellín, Enero de 2019

## Contenido

1. OBJETIVO: .....	3
1.1. Objetivos Específicos: .....	3
2. ALCANCE: .....	3
3. DEFINICIONES: .....	4
4. JUSTIFICACION .....	4
5. ANTECEDENTES .....	7
5.2. Políticas de seguridad de información: .....	7
5.3. Levantamiento de inventarios de activos de información: .....	8
5.4. Elaboración de matriz de riesgos: .....	8
5.5. Plan de tratamiento de riesgos .....	8
5.6. Plan de socialización .....	8
5.7. Modelo de Seguridad y privacidad de la información .....	9
6. ACTIVIDADES: .....	9
6.1 Actualizar Inventario de activos de información .....	9
6.2. Socializar boletines informativos de seguridad .....	9
6.3. Proveedores críticos .....	10
6.4. Riesgos de activos críticos: .....	10
6.5. Respaldo de información .....	10
6.6. Etiquetado de documentos .....	10

## **1. OBJETIVO:**

Identificar y ejecutar actividades orientadas a fortalecer el aseguramiento de los servicios de TI y la información que genera u obtiene la E.S.E. Hospital CARISMA, para preservar la confidencialidad, integridad y disponibilidad de la información relacionada con los usuarios en el marco de la Ley 1448 de 2011.

### **1.1. Objetivos Específicos:**

1.2. Fortalecer el aseguramiento de los servicios de TI y la información suministrada o relacionada con los pacientes, mediante la medición de la Implementación del Modelo de Seguridad y Privacidad de la Información.

1.3. Fomentar en los procesos de la Entidad, la gestión de riesgos de seguridad de la información, con base en los activos críticos previamente identificados y las acciones para mitigar el riesgo.

1.4. Ejecutar actividades en el marco de una metodología de gestión de la seguridad, para establecer un modelo de madurez aplicable y repetible.

1.5. Definir y socializar políticas, lineamientos, buenas prácticas y recomendaciones para establecer cultura en Seguridad de la Información en la Entidad.

## **2. ALCANCE:**

La E.S.E. Hospital CARISMA, en el marco de la implementación de la Ley 1448 de 2011, genera, obtiene, almacena, ofrece, intercambia, divulga y actualiza información clasificada, reservada y pública, relacionada con pacientes, sus funcionarios, contratistas y/o terceros contratados por operadores.

Esta información se considera un activo de valor para la Entidad ya que registra y soporta sus actuaciones en un contexto histórico, frente a las partes interesadas como lo son:

- Pacientes
- Entidades Nacionales
- Entidades territoriales
- Sociedad y comunidad nacional
- Cliente interno – E.S.E. Hospital CARISMA

### 3. DEFINICIONES:

**Confidencialidad:** Propiedad que impide la divulgación de información a personas o sistemas no autorizados.

**Disponibilidad:** Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

**Integridad:** garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.

**Seguridad:** Protección de los activos de información, contra amenazas que garanticen la continuidad del negocio, minimizando el riesgo y maximizando las oportunidades de la E.S.E. Hospital CARISMA

### 4. JUSTIFICACION

Adicionalmente el Estado colombiano cuenta con normatividad vigente que obliga el adecuado tratamiento de la información manejada por la Entidad en términos de confidencialidad, integridad y disponibilidad. Entre otras se citan:

- Ley 1437 de 2011, Capítulo IV, “utilización de medios electrónicos en el procedimiento administrativo”.  
“Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos.”
- Ley 1581 de 2012, g) Principio de seguridad:  
“La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.”
- Ley 1581 de 2012, Artículo 17, ítem d: “Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”.

- Ley 1712 de 2014, “principio de transparencia”:

“Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley.”

- Ley 1712 de 2014, artículo 7: “Disponibilidad de la información”

“En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten.”

- Ley 1712 de 2014 -Título III “Excepciones acceso a la información”

“Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito.”

- Decreto 2573 de 2014:

“Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea...” donde se encuentra como componente el modelo de Seguridad y Privacidad de la Información.

- Decreto 1413 de 2017, artículo 2.2.17.6.6, “Seguridad de la información.”

“Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información.”

- Decreto 1413 de 2007, artículo 2.2.17.6.1, “Responsable y encargado del tratamiento”:

“Los operadores de servicios ciudadanos digitales serán responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente y encargados del tratamiento respecto de los datos que otras entidades le proporcionen.”

- Artículo 2.2.17.6.3, “Responsabilidad demostrada”.

“Los operadores de servicios ciudadanos digitales deberán adoptar medidas apropiadas, efectivas y verificables que le permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, deben crear e implementar un Programa Integral de Gestión de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales.”

- Decreto 1413 de 2007, artículo 2.2.17.6.5, “Privacidad por diseño y por defecto”:

“Los operadores de servicios ciudadanos digitales deberán atender las buenas prácticas y principios desarrollados en el ámbito internacional en relación con la protección y tratamiento de datos personales que son adicionales a la Accountability, y que se refieren al Privacy by design (PbD) y Privacy Impact Assessment (PIA), cuyo objetivo se dirige a que la protección de la privacidad y de los datos no puede ser asegurada únicamente a través del cumplimiento de la normativa, sino que debe ser un 'modo de operar de las organizaciones, y aplicarlo a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y a las empresas en relación con la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador.”

- Decreto 1413 de 2017, artículo 2.2.17.5.10, “Derechos de los usuarios de los servicios ciudadanos digitales”:

“

1. Registrarse de manera gratuita eligiendo al operador de servicios ciudadanos digitales de su preferencia entre aquellos que estén vinculados por el articulador.
2. Aceptar, actualizar y revocarlas autorizaciones para recibir información, comunicaciones y notificaciones electrónicas desde las entidades públicas a su elección a través de los servicios ciudadanos digitales.
3. Hacer uso responsable de los servicios ciudadanos digitales a los cuáles se registre.
4. Interponer peticiones, quejas, reclamos y solicitudes de información en relación con la prestación a los servicios ciudadanos digitales.

5. Elegir y cambiar libremente el operador de servicios ciudadanos digitales.
  6. Solicitar en cualquier momento, y a través de cualquiera de los medios de atención al usuario, su retiro de la plataforma de servicios en cuyo caso podrá descargar su información a un medio de almacenamiento propio.”
- Decreto 1413 de 2017, artículo 2.2.17.2.1.1 “Descripción de los servicios ciudadanos digitales,  
1.5 servicio de interoperabilidad:  
Cualquier desarrollo en el marco de los servicios ciudadanos digitales especiales deberá hacer uso de o estar soportado en los servicios ciudadanos digitales básicos cuando lo requieran.”
  - Decreto 612 de 2018, artículo 1. “Integración de planes institucionales y estratégico. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web.”
  - Conpes 3854 de 2016, objetivo general “Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país”.

Por lo anterior, la E.S.E. Hospital CARISMA debe emprender acciones orientadas a la protección de la información que gestiona, realizando la identificación y tratamiento de riesgos de la información de los activos críticos que la soportan, de manera que se establecen y realiza el seguimiento a dichas acciones en el marco del plan de acción y del Sistema Integrado de Gestión.

## **5. ANTECEDENTES**

### **5.2. Políticas de seguridad de información:**

La E.S.E. Hospital CARISMA, se adoptan las políticas de Seguridad de la Información de cumplimiento por parte de directivos, funcionarios, usuarios y terceros que accedan a la información de la E.S.E. Hospital CARISMA, usen equipos informáticos y de comunicaciones, interactúen con

herramientas tecnológicas y/o servicios informáticos y/o ingresen de manera física o lógica a las instalaciones de la E.S.E. Hospital CARISMA.

### **5.3. Levantamiento de inventarios de activos de información:**

En el marco del Sistema Integrado de Gestión y el Subsistema de Gestión de Seguridad de la Información, en procesos de la Entidad se estará realizando el levantamiento de los activos de información con base en el procedimiento de “generación del inventario de activos de información” de gestión documental. Este insumo permitirá, dar cumplimiento a lo establecido en la Ley 1712 de 2014, respecto a la generación y publicación de los siguientes productos:

- Registro de activos
- Índice de información clasificada o reservada
- Esquema de publicación

Esta actividad facilitará la identificación, clasificación y valoración de criticidad de activos tipo información, software y hardware en los procesos, bajo una metodología documentada y aprobada por la Entidad que permitirá su actualización periódica, la cual es desarrollada por el equipo de seguridad de la información y se apoya la gestión para su aprobación por parte del proceso de gestión documental.

### **5.4. Elaboración de matriz de riesgos:**

Teniendo en cuenta las actividades ejecutadas en periodos anteriores, la Oficina de recursos Informáticos generará la matriz de riesgos de seguridad de la información, Identificando riesgos de seguridad de la Información, conforme a la Metodología de Administración Gestión de Riesgos de la E.S.E. Hospital CARISMA, lo que permitirá relacionar los activos críticos identificados por los procesos y los riesgos aplicables, según sea el caso.

### **5.5. Plan de tratamiento de riesgos**

En el marco de la metodología de riesgos establecida por la Oficina Asesora Desarrollo Organizacional de la E.S.E. Hospital CARISMA, se construirán los planes de tratamiento para cada riesgo identificado, cuyo nivel de riesgo residual fuera superior a bajo.

### **5.6. Plan de socialización**



La Oficina de recursos Informáticos, establecerá y ejecutará un plan de sensibilización, mediante el cual se generarán boletines informativos enviados masivamente articulados con la Oficina de Comunicaciones.

### **5.7. Modelo de Seguridad y privacidad de la información**

Oficina de recursos Informáticos, deberá realizar dos (2) mediciones de la evaluación de la implementación del Modelo de Seguridad y Privacidad de la Información del MinTIC – MSPI.

## **6. ACTIVIDADES:**

Oficina de recursos Informáticos proyecta las actividades en el marco del Plan de Acción – Modelo Integrado de planeación y Gestión y Plan de implementación del Sistema Integrado de Gestión, teniendo en cuenta esquema de procesos y tecnología de la E.S.E. Hospital CARISMA

En el esquema se identifican los procesos y arquitectura tecnológica de la E.S.E. Hospital CARISMA, en él se involucran las partes interesadas además de las aplicaciones que apoyan los procesos misionales de la Entidad, adicionalmente las actividades se proyectan teniendo en cuenta la normatividad relacionada, con los componentes del esquema:

Teniendo en cuenta la normatividad vigente del Estado Colombiano, que obliga el adecuado uso y tratamiento de la información gestionada por la Entidad en términos de confidencialidad, integridad y disponibilidad, se involucran el marco regulatorio teniendo en cuenta las partes interesadas.

### **6.1 Actualizar Inventario de activos de información.**

Un activo de información tiene valor para la organización y se requiere para la operación del proceso al cual pertenece, como por ejemplo sistemas de información, elementos de hardware, personas e instalaciones, en cumplimiento de la Ley 1712 de 2014 “Ley de transparencia” se hace necesario la actualización del inventario de activos de anualmente con el apoyo de cada uno de los procesos a nivel central.

### **6.2. Socializar boletines informativos de seguridad.**

Para que la información sobre Seguridad de la Información llegue a todos los procesos de la Entidad, se hace necesario contar con la ayuda de la oficina de comunicaciones, los boletines y buenas prácticas de seguridad de la información.

### **6.3. Proveedores críticos**

El objetivo de la actividad de identificación de proveedores críticos es tener el inventario de los terceros que proporcionan o soportan servicios necesarios para la operación de la E.S.E. Hospital CARISMA, para la identificación del inventario se hace requiere que todos los procesos a nivel central se involucren en esta actividad.

### **6.4. Riesgos de activos críticos:**

Los riesgos de seguridad de información son asociados a los activos críticos de información definidos y categorizados por cada proceso de la Entidad, con base al procedimiento de generación de inventario de activos de información establecido en el marco del Sistema Integrado de Gestión, conforme a la Metodología de Administración Gestión de Riesgos de la E.S.E. Hospital CARISMA.

Los activos críticos son aquellos que se encuentran en la escala del 4 al 5 en la valoración del activo; a aquellos activos que se localicen dentro de este rango se les realizará la correspondiente gestión de riesgos, a partir de la metodología de administración de riesgos definida por la E.S.E. Hospital CARISMA.

### **6.5. Respaldo de información**

Para proteger la información almacenada en los equipos de cómputo, los usuarios deberán realizar el respaldo de la información, en los servicios dispuestos por la Oficina de recursos Informáticos (Unidad de red ORION).

### **6.6. Etiquetado de documentos**

Por medio del inventario único documental cada uno de los procesos de la Entidad a nivel central, identificará, clasificará y/o etiquetará los documentos que se generen en el proceso. Por medio de este componente se adicionará propiedades de seguridad a la información sensible y/o confidencial que protegerán la información que transite vía electrónica, restringiendo permisos de copiado, transferencia, modificación y/o divulgación.