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

E.S.E HOSPITAL SANTA MARGARITA

La Cumbre - Valle

## VIGENCIA 2025

**40-42.16**

## TABLA DE CONTENIDO

**40-42.16**

## 1. INTRODUCCIÓN

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Es muy importante que las organizaciones cuenten con un plan de gestión do riesgos para garantizar la continuidad do las funciones misionales, por este motivo, se ha visto la necesidad de desarrollar un análisis de riesgo de seguridad de la información aplicado en la ESE HOSPITAL SANTA MARGARITA, antes de iniciar con este Plan de Gestión se ha revisado la situación actual de la entidad y la identificación de los activos con sus respectivas amenazas, para continuar con la medición de riesgos existentes y sugerir las protecciones necesarias que podrían formar parte del plan de gestión de riesgos en la seguridad de la información.

El aporte que arroja esto plan permite identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

## 2. CONTEXTO INSTITUCIONAL

### 2.1. ARTICULACIÓN CON EL PLAN DE DESARROLLO

Se articula el plan de tratamiento de riesgos de seguridad y privacidad de la información con el objetivo estratégico número 2. "*Mejorar la eficiencia operativa y la calidad en los procesos hospitalarios, impulsando la actualización de infraestructura, la adopción de tecnologías innovadoras, el fortalecimiento del posicionamiento institucional y la optimización de las finanzas, alcanzando estándares de excelencia."* del plan de desarrollo para la vigencia 2024-2028

### VISIÓN

Consolidarnos como un Hospital con énfasis en los servicios de prestador primario, referente en la prestación Integral de servicios de salud de baja complejidad, centrados en las personas de acuerdo con sus necesidades, integrado con los demás actores del sistema, implementando el Modelo de Acción Integral Territorial humanizado y seguro, con enfoque de gestión sostenible por su eficiencia, responsabilidad social y amigable con el medio ambiente. Generado bienestar en el municipio de La Cumbre Valle.

**40-42.16**

**MISIÓN**

Satisfacer las necesidades de salud de la baja complejidad de nuestros pacientes, integrando la atención primaria en salud (APS), práctica clínica y la educación, en una permanente búsqueda de la excelencia para beneficio de la comunidad.

**VALORES INSTITUCIONALES**

**Honestidad:** Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia, rectitud, y siempre favoreciendo el interés general.

**Respeto:** Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición.

**Compromiso:** Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar.

**Diligencia:** Cumplo con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud y eficiencia, para así optimizar el uso de los recursos del Estado.

**Justicia:** Actúo con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.

## 3. GLOSARIO DE TÉRMINOS

**Riesgo Estratégico:** Se define como la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la institución por parte de la alta gerencia.

**Riesgos de Imagen:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

**Riesgos Operativos:** Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

**40-42.16**

**Riesgos Financieros:** Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

**Riesgos de Cumplimiento:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.

**Riesgos de Tecnología:** Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.).

## 4. MARCO LEGAL

Como referente normativo se tienen principalmente las siguientes disposiciones:

**Ley 1581 de 2012 (Ley de Protección de Datos Personales):** Establece el régimen general de protección de datos personales en Colombia y regula el tratamiento de estos, garantizando los derechos de los titulares, como la confidencialidad, acceso, rectificación y eliminación de información.

**Decreto 1377 de 2013:** Reglamenta parcialmente la Ley 1581 de 2012 y establece disposiciones específicas para el manejo de datos personales, incluidos lineamientos sobre autorización de tratamiento, derechos de los titulares y medidas de seguridad.

**Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública):** Garantiza el acceso a la información pública, pero también resalta la importancia de proteger los datos sensibles y la información que pueda comprometer la privacidad o la seguridad.

**Ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso Administrativo):** Define principios relacionados con la protección de datos personales y el derecho a la reserva de información en los procesos administrativos.

**Ley 1273 de 2009:** Introduce el delito de "protección de la información y los datos" en el Código Penal, estableciendo sanciones para quienes accedan, usen, modifiquen o revelen información sin autorización.

**Resolución 1995 de 1999:** Regula el manejo de las historias clínicas en Colombia, destacando la confidencialidad como un principio fundamental en el tratamiento de la información médica.

**40-42.16**

**ISO/IEC 27001:** Estándar internacional para la gestión de la seguridad de la información, aplicable a la protección de datos en el ámbito hospitalario.

**ISO/IEC 27799:** Guía específica para implementar controles de seguridad en el manejo de información de salud.

## 5. OBJETIVOS

### 5.1. OBJETIVO GENERAL

Desarrollar un Plan de Gestión de seguridad y privacidad que permita minimizar los riesgos de pérdida de información de la BASES DE DATOS RFAST8 SISTEMA INTEGRADO de CLIENTES pacientes, HISTORIAL CLINICO, INFORMACION CONTABLE, CARTERA, FACTURACION del Hospital Santa Margarita de La Cumbre Valle.

### 5.2. OBJETIVOS ESPECÍFICOS

- Plantear modelos de reportes para su posterior uso en cada incidencia presentada en el Hospital Santa Margarita de La Cumbre.

- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.

- Determinar el alcance del plan de gestión de riesgos de la seguridad y Privacidad de la información.

- Definir los principales la información a proteger en el Hospital Santa Margarita de La Cumbre.

- Identificar las principales amenazas que afectan a los Sistemas de información.

- Proponer soluciones para minimizar los riesgos a los que está expuesto las BD de información de la ESE.

- Adquirir aplicaciones que controlen los accesos blindando y depurando correos electrónicos.

**40-42.16**

- Adquisición de consolas de antivirus y protección de copias de seguridad en la nube.

- Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el Plan de Gestión de Seguridad de la Información.

## 6. ALCANCE

El presente Plan Estratégico aplica para todos los procesos que contribuyen al desarrollo de los recursos de tecnologías de información y comunicación en la E.S.E. Hospital Santa Margarita de La Cumbre.

Al desarrollar e implementar este documento se logrará el compromiso del Hospital Santa Margarita de La Cumbre para emprender la Implementación del Plan de Gestión del Riesgo en la Seguridad de la Información y designar funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de Gestión. De igual forma capacitar al personal de la entidad en el proceso de Plan de Gestión del Riesgo de la Seguridad de la Información.

## 7. GESTIÓN DEL RIESGO

### 7.1. IMPORTANCIA DE GESTIÓN DEL RIESGO

El Hospital Santa Margarita de La Cumbre, siguiendo los lineamientos definidos por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al Decreto 1078 de 2015.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las instituciones. Una entidad sin Un plan de gestión de riesgos está expuesta a perder su información.

Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software, afectando la disponibilidad e integridad de la información almacenada o transportada a través de estos equipos de comunicación.

**40-42.16**

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad de la entidad tras sufrir alguna pérdida o daño en la información de la Institución.

Considerando la situación actual del Hospital Santa Margarita de La Cumbre, para reducir los niveles de riesgo, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

### 7.2. DEFINICIÓN DE GESTIÓN DE RIESGO

La gestión del riesgo se define como el proceso de identificar, analizar y cuantificar las posibilidades de pérdidas y efectos secundarios que se desprenden de los desastres, así como de las acciones preventivas, correctivas y reductivas correspondientes que deben emprenderse

### 7.3. IDENTIFICACIÓN DE SITUACIONES NO DESEADAS

- Todo Hurto de información o de equipos informáticos.
- Hurto de información durante el cumplimiento de las funciones laborales por intromisión.
- Incendio en las instalaciones de la ESE por desastre natural o de manera intencional.
- Alteración de claves y de información.
- Pérdida de información.
- Baja Cobertura de Internet.
- Daño de equipos y de BD Aplicativo institucional.
- Atrasos en la entrega de información.
- Atrasos en asistencia técnica.
- Fuga de información.
- Manipulación indebida de información.

## 8. ORIGEN DEL PLAN DE GESTIÓN DE RIESGO

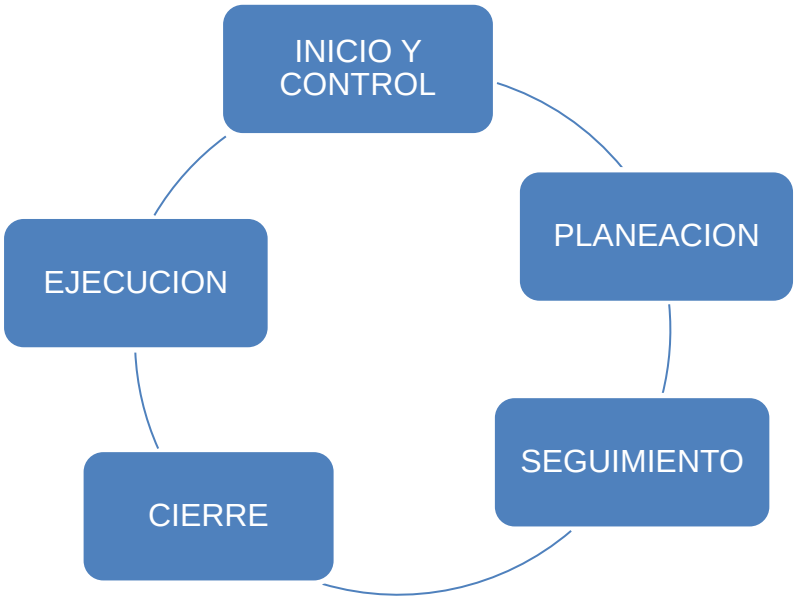
Debido al riesgo de pérdida de información es necesario crear un plan de gestión de riesgos de seguridad de la información que permita proteger el activo más valioso para la entidad; la información.

El gobierno nacional y el ministerio de las HC han abanderado los proyectos de Gobierno en Línea que permite conocer el funcionamiento de las diferentes entidades públicas en el País. Es por ello necesario que el Hospital Santa Margarita de La Cumbre cumpla con

**40-42.16**

los requisitos necesarios para entregar la información de manera oportuna y eficiente a estas entidades y a la población.

## 9. IDENTIFICACIÓN DEL RIESGO




## 10. ANÁLISIS DE VULNERABILIDADES

### 10.1. DESCRIPCIÓN DE VULNERABILIDADES

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios en el Hospital Santa Margarita de La Cumbre, se encontraron otras amenazas e impactos como los siguientes:

Las políticas y normas de seguridad de la información existentes no son controladas, por eso es muy común identificar el incumplimiento a las reglas básicas del cuidado tanto de los equipos informáticos, como de la información física y digital, algunas son:

- Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los activos de información y de informática.
- Reservada identificándose la falta de confidencialidad y privacidad
- Acceso sin restricciones a las Historias Clínicas del personal administrativo y podría ocasionar flujo de información confidencial de los clientes pacientes.
- No hay control para el uso dispositivos digitales USB y exponiendo a perder la información por virus no detectados o daños irreparables del hardware.

**40-42.16**

- Se identificó un completo desconocimiento del tema de seguridad y privacidad de la información en el l Hospital Santa Margarita de La Cumbre.
- No existe un antivirus licenciado administrado por consola
- No esta normaliza o regulada la red eléctrica.
- Cableado de red obsoleto.
- No existe un respaldo o backup en la nube.
- No se cuenta con respaldo de switch, routers, servidor en caso de fallo de algún equipo.
- No se cuenta con DATACENTER con seguridad física.
- No se cuenta con sistema cerrado de TV.
- No existe control de seguridad de ingreso y salida del personal y clientes.
- Falta de un Backup dedicado a la Nube

## 11. PROPUESTA DE SEGURIDAD

- Revisar las políticas existentes para identificar debilidades y fortalezas, si es necesario se hacen ajustes, teniendo en cuenta que seguridad informática no es igual a seguridad de la información

- Restringir el uso de dispositivos digitales, bloqueo de puertos, controlar el acceso a internet.

- Licenciamiento de software equipos y servidores.

- Adquisición de UPS CENTRALIZADA que proteja toda la red

- El personal de sistemas puede crear las cuentas y claves, socializando al Personal el Hospital Santa Margarita de La Cumbre la creación de claves en forma correcta.

- Adquisición de CONSOLA DE SEGURIDAD INFORMATICA. Que nos permita monitorear nuestros recursos de red, FIREWALL de nueva generación, DLP, Protección de virus hora cero, soluciones de seguridad informática, Diseño, Implementación, Soporte y Monito-reo. Firewall de nueva generación, DLP, Protección virus hora cero

## 12. PLAN SEGURO PARA LA CREACIÓN DE COPIAS DE SEGURIDAD

Es necesario capacitar de forma personal a los funcionarios de la ESE en el almacenamiento de copias de seguridad de la información que no sea administrado por

**40-42.16**

RFAST8 y que es l manejada en las diferentes dependencias. De igual forma contar con un plan alternativo que asegure la continuidad de la actividad en caso de que ocurran incidentes graves.

## 13. IMPLEMENTACIÓN DE POLÍTICA DE SEGURIDAD PARA LA INFORMACIÓN

El análisis permitió identificar que se desconocen y poco se cumplen las políticas de seguridad; por lo cual, debe quedar integrado con el documento actual. Se recomienda entre otros tener en cuenta: Los temas de seguridad informático y de la información, Ambiente con la seguridad física adecuada, y Sistemas de respaldo para mantener soporte de la información en caso de eventualidades catastróficas.

## 14. MATRIZ DE VULNERABILIDAD Y MITIGACIÓN DEL RIESGO

| VULNERABILIDAD | DESCRIPCION | CAUSA | EFECTO | CLASIFICACION | EVALAUCION | MITIGACION | VIGENCIA |
|---|---|---|---|---|---|---|---|
| Las políticas y normas de seguridad no se cumplen | Se desconocen las normas de seguridad en la ESE | Rotación del personal | Incumplimiento de la Confiabilidad | Riesgo del recurso humano | Alto | Implementar capación por cada uno de los procesos cuando ingrese personal a la ESE | 2025 |
| Uso de dispositivos digitales en los equipos | No hay control para el uso de dispositivos USB e internet | No se lleva control de ingreso a la institución | Incumplimiento de la Confiabilidad | Riesgo del recurso humano | Alto | Implementar registro y control del entrada y salida de equipos | 2025 |
| Servidor BD | No hay respaldo en caso de fallo | No se tienen respaldo de DISCOS, FUENTES, MEMORIA en caso de fallo | Atraso y perdida de la información para la ESE | Riesgo físico | Alto | Adquisición de respaldos para el servidor | 2025 |
| Switch y routers | No hay respaldo en caso de fallo | No se tiene respaldo en caso de fallo | Atraso y perdida de la información para la ESE | Riesgo físico | Alto | Adquisición de respaldos para la RED | 2025 |
| Sistema cerrado de TV | No hay cámaras de vigilancia en la ESE, en ninguna área. | presupuesto | En caso de alguna novedad o evento no hay como corroborar | Riesgo físico | Alto | Adquisición de circuito cerrado de TV | 2025 |
| Registro y control de acceso a la ESE | No hay control de ingreso, revisión de maletines, bolsas etc | No se ha implementado el procedimiento de portería | Riesgo de pérdida de elementos y objeto institucionales | Riesgo del recurso humano | Alto | Implementar procedimiento | 2025 |
| ADQUISICION DE FIREWALL Y PROTECCION DE VIRUS | NO poseemos software que nos brinde tranquilidad | presupuesto | Riesgo de pérdida o secuestro de la BASE DE DATOS de la | Riesgo OPERATIVO | Alto | ADQUISICION DE FIREWALL | 2025 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | información de la ESE | | | | |

## 15. CONTROL DE CAMBIOS

| LABORADO POR | REVISADO POR | APROBADO POR |
|---|---|---|
| Líder de Sistemas | Jefe de Oficina Administrativa y Financiera - Líder de Calidad | Gerente |

| REGISTRO DE CAMBIOS Y REVISIONES | | | | |
|---|---|---|---|---|
| **VERSIÓN** | **FECHA** | **PÁGINAS** | **SOLICITANTE** | **OBSERVACIONES** |
| 1 | 02/01/2025 | 12 | Gerencia | Creación del documento por Nixon Bravo – Líder de Sistemas<br>Revisado por Duvan Felipe Ochoa Toro – Líder de Calidad – Alix Arias – Asesora MIPG<br>Aprobado por Aicardo Solís - Gerente |