
| Documentado. | | Revisado | Aprobado |
|---|---|---|---|
| **Nombre:** | | | |
| **Cargo:** | | | |
| **Firma:** | | | |



Calle 16 Avenida La Popa No. 17-141 teléfono: 5748452 Fax: 5748451
E-mail: meci@hrplopez.gov.co

## 1. INTRODUCCIÓN

La información que genera constantemente La **ESE Hospital Rosario Pumarejo de López**, es crucial para su correcto desempeño y cumplimiento de los objetivos organizacionales, es por ello que la seguridad y privacidad de la información se convierten en atributos indispensables para evitar cualquier posibilidad de alteración, mal uso, pérdida, entre otros eventos, que puedan significar una alteración para el normal desarrollo en la prestación de servicios de salud.

De acuerdo a lo mencionado anteriormente, dentro de Marco de Seguridad del Modelo de Seguridad y Privacidad de la información –MSPI-, un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones. Es por esto que La **ESE Hospital Rosario Pumarejo de López**, adopta la metodología “Guía de Riesgos” del Departamento Administrativo de la Función Púbica y como herramienta metodológica la utilizada por la Unidad Nacional para la Gestión del Riesgo de Desastres de la Presidencia de la República, además ha incorporado como referente la Norma ISO 31000 con el objetivo de generar buenas prácticas de gobierno corporativo y del mejoramiento continuo en la gestión de riesgos.

La **ESE Hospital Rosario Pumarejo de López**, acoge la gestión de riesgos como un proceso sistemático de identificación, análisis, evaluación, valoración, y tratamiento de los riesgos; aplicando los controles necesarios para evitar, reducir, compartir, transferir o asumir el riesgo con medidas preventivas o correctivas que deberá generar como resultado minimizar pérdidas, maximizar rendimientos y cuidar la seguridad del paciente.

## 2. GENERALIDADES:

### RESPONSABLES


La estructura organizacional de los procesos responsables de la realización del plan es la siguiente:

- Subgerente Financiero
- Profesional Universitarios de Planeación
- Profesional Universitarios de Calidad
- Ingeniero de Sistemas
- Técnico en gestión documental
- Profesional Especializada Estadística
- SIAU

**PLATAFORMA ESTRATEGICA:**

**MISIÓN.**

"SOMOS UNA EMPRESA SOCIAL DEL ESTADO PRESTADORA DE SERVICIOS DE SALUD DE MEDIANA Y ALTA COMPLEJIDAD EN EL DEPARTAMENTO DEL CESAR Y SU ÁREA DE INFLUENCIA, INCLUYENTE, PARTICIPATIVA PARA SATISFACCIÓN DE LAS NECESIDADES DEL USUARIO Y SU FAMILIA, COMPROMETIDA CON LA SEGURIDAD PACIENTE, HUMANIZACIÓN, PROTECCIÓN DEL MEDIO AMBIENTE Y LA FORMACIÓN DEL CAPITAL HUMANO FUNDAMENTADO EN LA RELACIÓN DOCENCIA SERVICIO".

**VISIÓN.**

"SER EN EL 2025 UN HOSPITAL RECONOCIDO EN EL CESAR Y ÁREA DE INFLUENCIA POR CRECER EN SERVICIOS DE SALUD INTEGRALES DE MEDIANA Y ALTA COMPLEJIDAD ENFOCADOS EN EL MEJORAMIENTO CONTINUO CON CALIDAD, PROMOVIENDO SEGURIDAD PACIENTE, HUMANIZACIÓN Y REDUCCIÓN DE LA HUELLA ECOLÓGICA; FORTALECIENDO AVANCES ACADÉMICOS Y CIENTÍFICOS".

**PRINCIPIOS Y VALORES:**

En el Hospital, se ha fundamentado los siguientes principios, que fueron identificados y concertados soporte de una cultura organizacional comprometida con la atención humanizada y segura, el respeto a los Derechos del Usuario, a la formación del talento humano, al medio ambiente, como un compromiso ético adoptado por los servidores públicos de la entidad hospitalaria, así:

- **HUMANIZACION:** Trato con calidez y dignidad.
- **PERTINENCIA:** Atención científica con el mínimo riesgo de acuerdo a la necesidad.
- **OPORTUNIDAD:** Garantizar los servicios requeridos sin retraso.
- **INTEGRALIDAD:** Cobertura de las necesidades de salud y satisfacción del Usuario.

- **TRABAJO EN EQUIPO:** Cooperación y armonía para el logro de objetivos.

**VALORES:**

"Los servidores públicos somos personas que con vocación y orgullo trabajamos duro todos los días para servir y ayudar a los colombianos, en el Hospital el cumplimiento de los Valores rigen de manera implícita la conducta de los servidores públicos de la entidad, soportando el cumplimiento de la visión, misión, estrategias y objetivos institucionales, los valores se manifiestan y hacen realidad en nuestra forma de ser, pensar y conducirnos, a partir de la implementación de los lineamientos del Modelo Integrado de Planeación y Gestión Versión II, el Hospital Rosario Pumarejo de López, apropia los Valores contemplados en el Código de Integridad, que se encuentran incorporados al Código de Ética y Buen Gobierno de la ESE, los cuales favorecen el cumplimiento de los objetivos misionales de la ESE, y son:

**HONESTIDAD:** Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia y rectitud, y siempre favoreciendo el interés general en especial si es el paciente.

**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, destreza 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.

**Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

**Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

**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.

**Ley de Transparencia y Acceso a la Información Pública**: Se refiere a la Ley Estatutaria 1712 de 2014.

**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 Rosario Pumarejo de Lopez.

**Comité de Seguridad de la Información (CSI):** Instancia del nivel superior, que deben validar la Política de Información, así como los procesos, procedimientos y metodologías específicas de seguridad de la información para el adecuado uso y administración de los recursos informáticos y físicos, asignados a los servidores públicos de cada ente público.

**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 de Hospital Rosario Pumarejo de Lopez 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.
**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.
**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.

## 4. DESARROLLO DEL PLAN.

### 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, dónde, y por qué podría ocurrir está perdida, las siguientes etapas recolectan datos de entrada para esta actividad.

### Categorías de riesgos:

**ET: Estratégicos:** Relacionados a lineamientos, políticas, estrategias o directrices no adecuadas o no convenientes para la Entidad.

**OP: Operativo:** Relacionado a procesos, conductas o actividades inapropiadas, contrarias al deber ser o que presente una posible brecha frente a la calidad esperada.

**FA: Financiero:** Relacionado con la asignación, suficiencia o recaudo de recursos económicos que puedan afectar a corto, mediano o largo plazo financieramente.

**TE: Tecnológico:** Relacionado al uso, manejo o disposición de equipos biomédicos, industriales o de cómputo y periféricos.

**CL: Clínico:** Relacionados a condiciones patológicas de pacientes atendidos en La ESE Hospital Rosario Pumarejo de López.

**Identificación de riesgos:**

Normalmente se identifican los riesgos como eventos o situaciones no deseadas que se pretenden evitar, por tal razón la identificación de riesgos inicia con términos como: Ausencia, No adherencia, Inadecuada, No suficiencia, entre otros.

Una vez se identifique el riesgo, debe complementarse para obtener el contexto del riesgo, ya que éste puede presentarse en un área, en un horario, por parte de un grupo de colaboradores, o en unas circunstancias específicas que ayudarán más adelante a determinar las acciones a tomar. Estos son algunos ejemplos de preposiciones a utilizar: al, durante, en, sobre, con, hacia, de, mediante, entre otros.

**Descripción de Causas:**

Se describen las causas asociadas al riesgo identificado, pueden ser intrínsecas: atribuidas a personas, métodos, materiales, equipos, instalaciones, directamente involucradas en el proceso o externas: cuando provienen del entorno en el que se desarrolla el proceso.

**Consecuencias:**

Se describen los efectos asociados a la materialización del riesgo, que incidan sobre el objetivo del proceso o la Entidad. Pueden agruparse en: Daños a pacientes o trabajadores, Perdidas económicas, Perjuicio de la imagen, Sanciones legales, reproceso, Demoras, Insatisfacción, entre otras.

**Barreras de Seguridad Existentes:**

Se describen los controles implementados o barreras que existen actualmente para evitar la materialización del riesgo, se pueden encontrar en los protocolos o

procedimientos documentados, en las guías de reacción inmediata o en los correctos de buenas prácticas de seguridad del paciente.

| PROBABILIDAD | | |
|---|---|---|
| Remota | 1 | La probabilidad de ocurrencia es muy baja, casi nula |
| Poco Probable | 2 | Puede ocurrir bajo circunstancias excepcionales |
| Probable | 3 | Puede ocurrir con cierta frecuencia |
| Ocasional | 4 | Ocurre algunas veces |
| Frecuente | 5 | La ocurrencia se da de manera común en circunstancias actuales |

| IMPACTO | | |
|---|---|---|
| Muy bajo | 1 | Los efectos de materialización del riesgo no son significativos |
| Bajo | 2 | Los efectos de materialización del riesgo son poco significativos |
| Moderado | 3 | Los efectos de materialización del riesgo pueden significar aspectos |
| Alto | 4 | Los efectos de materialización del riesgo son significativos e importantes |
| Muy Alto | 5 | Los efectos son catastróficos, como muerte, lesiones incapacitantes o liquidación de la empresa |

| PROBABILIDAD | | | | | | |
|---|---|---|---|---|---|---|
| | 5 | 5 | 10 | 15 | 20 | 25 |
| | 4 | 4 | 8 | 12 | 16 | 20 |
| | 3 | 3 | 6 | 9 | 12 | 15 |
| | 2 | 2 | 4 | 6 | 8 | 10 |
| | 1 | 1 | 2 | 3 | 4 | 5 |
| | | 1 | 2 | 3 | 4 | 5 |
| | | IMPACT | | | | |

| NIVEL DE RIESGO | MEDIDAS DE |
|---|---|
| BAJA | ASUMIR EL RIESGO Y CONTINUAR MONITORIZANDOLO |
| ACEPTABLE | REDUCIR EL RIESGO PARA LLEVARLO A ZONA BAJA |
| ALTA | EVITAR-COMPARTIR-TRANSFERIR POR MEDIO DE UN PLAN |
| INACEPTABLE | EVITAR-COMPARTIR-TRANSFERIR POR MEDIO DE UN PLAN |

**Tratamiento y seguimiento del Riesgo**:

Se describen los controles o barreras a ser implementadas que fortalezcan las existentes, con lo cual aportar y evitar la materialización del riesgo desde la reducción de la probabilidad y/o del impacto. Las acciones propuestas pueden en algunos casos significar actualización de protocolos o procedimientos documentados, adopción de mejores prácticas a través de referenciaciones realizadas, fortalecimiento de buenas prácticas de seguridad del paciente, asesorías con expertos, entre otras.

Un aspecto de gran importancia es la definición de indicadores para determinar el impacto de las acciones realizadas, ya que no es suficiente cumplir las actividades propuestas sino también valorar como estas acciones permiten disminuir la probabilidad de ocurrencia o nivel de impacto del riesgo; es decir, el indicador mide la efectividad de las acciones frente a la mitigación del riesgo.

| CATEGORIA | Nº | IDENTIFICACION DE RIESGOS | FECHA DE IDENTIFICACION DE RIESGO | ANALISIS DEL RIESGO | | | VALORACION INICIAL DEL RIESGO | | | TRATAMIENTO Y SEGUIMIENTO DEL RIESGO | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | CAUS | CONSECUENCIAS | BARRERAS DE SEGURIDAD | VALOR DE PROBABILIDAD | VALOR DE IMPACTO | NIVEL DEL RIESGO | BARRERAS DE SEGURIDAD A IMPLEMENTAR | RESPONSABLE DEL SEGUIMIENTO | INDICADOR | LINEA BASE | META | RESULTADOS DE EFECTIVIDAD DE LAS ACCIONES (Planeación) | VALORACION DEL RIESGO DESPUES DE CONTROLES (Control |
| | | | | | | | | | | | | | | | | |

## 5. MARCO LEGAL.

Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública

Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública

Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública

Ley 57 de 1985 -Publicidad de los actos y documentos oficiales

Ley 594 de 2000 - Ley General de Archivos

Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática

Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad

Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo

Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos

Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública

Decreto 2364 de 2012 - Firma electrónica

Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos

Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales

Ley 527 de 1999 - Ley de Comercio Electrónico

Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública

Ley Estatutaria 1581 de 2012 - Protección de datos personales

Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información