

|                                      |                                                                            |                            |               |  |
|--------------------------------------|----------------------------------------------------------------------------|----------------------------|---------------|--|
|                                      | PLANES INSTITUCIONALES                                                     |                            |               |  |
|                                      | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN |                            | PÁGINA 1 DE 4 |  |
|                                      | PROCESO                                                                    | GERENCIA DE LA INFORMACIÓN | 01GIN14-V3    |  |
| Elaboró: LUIS AUGUSTO OLAYA PALACIOS | Revisó: CARLOS FERNANDO GONZÁLEZ PRADA                                     | Aprobó: JORGE ANDRES LOPEZ |               |  |
| Cargo: SUBDIRECTOR SISTEMAS          | Cargo: DIRECTOR ADMINISTRATIVO                                             | Cargo: GERENTE             |               |  |

## 1. OBJETIVOS

**GENERAL:** Desarrollar un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información el cual sea una guía para el control y minimización de los de los riesgos y así proteger la privacidad de la información y los datos tanto de los procesos como de las personas vinculadas con la información de la institución.

### ESPECÍFICOS:

- Categorizar y valorar los activos de información
- Establecer los controles y políticas de la seguridad de la información que garantice la confidencialidad integridad y disponibilidad de la información.
- Ajustar el mapa de riesgos de los procesos donde se incluyan los riesgos definidos para los activos de información.

## 2. ALCANCE

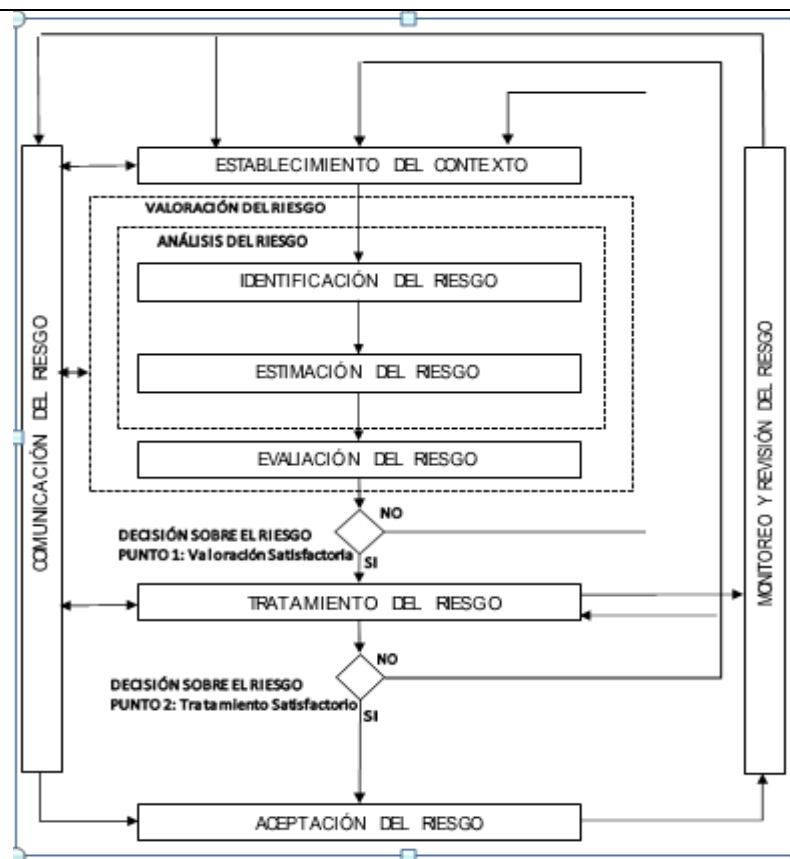
El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional.

Se definen las actividades a ser lideradas por el HUS durante el 2025, en cumplimiento de sus funciones y para el logro de sus objetivos.

## 3. METODOLOGÍA

La implementación del Sistema de gestión de seguridad y privacidad de la información, toma como base la metodología el modelo MSPI de MINTIC, el modelo integrado de planeación y gestión – MIPG y la norma ISO 27001:2013.

El HUS cuenta con un programa de Gestión y administración del riesgo 01GC04 que tiene como objetivo: *“Identificar los potenciales riesgos, adelantar las acciones para el adecuado tratamiento y reducción de los mismos, que eviten su materialización así como eventos no deseados, todo bajo un estrategia de priorización, cuyo manejo garantice el cumplimiento de los objetivos institucionales y de sus procesos, implementando acciones de monitoreo y retroalimentación pertinentes evitando así daños en los pacientes, usuarios y familiares, en los colaboradores del hospital, en el patrimonio e imagen de la entidad y en las partes interesadas”* y se tiene el procedimiento Administración del Riesgo 02GC05 que tiene como objetivo *“Mitigar el impacto y la frecuencia de ocurrencia del riesgo, a través de los controles establecidos, estos documentos se articulan con este plan ya cumplen con la Guía No 7 de MINTIC donde determina el Proceso para la administración del riesgo en seguridad de la información*



Adicionalmente MINTIC en su guía No. 7 define unas etapas sugeridas para la gestión del riesgo:

- La primera y más importante para lograr un adecuado avance en todo el proceso de administración del riesgo es el “Compromiso de las alta y media dirección”
- En segundo lugar, se encuentra la “Conformación de un Equipo MECI o de un grupo interdisciplinario”, la idea de una integralidad en el tratamiento de los riesgos para poder tener una visión completa de la Entidad.
- Finalmente se encuentra la “Capacitación en la metodología”, este punto es un poco más profundo, porque es claro que el equipo interdisciplinario debe capacitarse

|  | PLANES INSTITUCIONALES                                                     |                            |               |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------|----------------------------|---------------|
|                                                                                   | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN |                            | PÁGINA 3 DE 4 |
|                                                                                   | PROCESO                                                                    | GERENCIA DE LA INFORMACIÓN | 01GIN14-V3    |

05GIC28-V3

para poder analizar ahora los riesgos de seguridad.

Las etapas anteriores el HUS ya cuentan con un Equipo MECI y se articulará este plan con este equipo.

Etapas propuestas para la Generación del análisis de riesgos de las Entidades, basadas la norma ISO27005

**ETAPA 1: 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, las siguientes etapas deberían recolectar datos de entrada para esta actividad.

**ETAPA 2: 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. Para realizar esta identificación es necesario revisar la guía de gestión de activos adjunta al MSPI.

**ETAPA 3: 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.

**ETAPA 4: 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

**ETAPA 5: 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.

**ETAPA 6: MÉTODOS PARA LA VALORACIÓN DE LAS VULNERABILIDADES TÉCNICAS**

**ETAPA 7: 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 y Lista de las amenazas y vulnerabilidades con respecto a los activos y su pertinencia.

## ESTRATEGIAS

**Minimizar los riesgos asociados a los procesos tecnológicos existentes, con el fin de salvaguardar los activos de Información.**

- Componente GEL: TIC para la Gestión
- Dominios del Marco TI: Servicios tecnológicos, uso y apropiación

|  |                                                                            |                            |               |  |
|--|----------------------------------------------------------------------------|----------------------------|---------------|--|
|  | PLANES INSTITUCIONALES                                                     |                            |               |  |
|  | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN |                            | PÁGINA 4 DE 4 |  |
|  | PROCESO                                                                    | GERENCIA DE LA INFORMACIÓN | 01GIN14-V3    |  |

Objetivo estratégico Institucional: Garantizar un Sistema de Información integral, eficiente y eficaz

#### 4. ACTIVIDADES

| No | QUE (ACTIVIDADES)                                                     | RESPONSABLE DEL CUMPLIMIENTO | FECHA DE CUMPLIMIENTO | DONDE | COMO<br>Pautas para la realización de la actividad                    |
|----|-----------------------------------------------------------------------|------------------------------|-----------------------|-------|-----------------------------------------------------------------------|
| 1. | Documentación del proceso del levantamiento de activos de información | Subdirector Sistemas         | 30/11/2025            | HUS   | Documentación del proceso del levantamiento de activos de información |
| 2. | Actualización de los Activos información (Vigencia)                   | Subdirector Sistemas         | 30/11/2025            | HUS   | Actualización de los Activos información (Vigencia)                   |
| 3. | Publicación activos Información                                       | Subdirector Sistemas         | 30/11/2025            | HUS   | Publicación activos Información                                       |

#### 5. ANEXOS

#### 6. CONTROL DE CAMBIOS

| VERSIÓN | FECHA      | ÍTEM MODIFICADO | JUSTIFICACIÓN        |
|---------|------------|-----------------|----------------------|
| 1       | 01/02/2020 |                 | Se documenta plan    |
| 2       | 05/05/2023 |                 | se actualiza formato |
| 3       | 10/07/2025 |                 | se actualiza formato |

La última versión de cada documento será la única válida para su utilización y estará disponible en el Portal Interno de la E.S.E. Hospital Universitario de la Samaritana, evite mantener copias digitales o impresas de este documento porque corre el riesgo de tener una versión desactualizada.