TABLA DE CONTENIDO

1. OBJETIVO

Establecer las acciones para la gestión y tratamiento de los riesgos de seguridad y privacidad de la información identificados en la E.S.E. Hospital Departamental Tomás Uribe Uribe de Tuluá, articulando las actividades de prevención, mitigación, seguimiento y mejora con la Matriz de Riesgos institucional.

El Plan busca contribuir a la protección de la confidencialidad, integridad y disponibilidad de la información y de los servicios tecnológicos institucionales mediante la implementación y seguimiento de controles y acciones de tratamiento acordes con los riesgos identificados.

2. ALCANCE

El presente Plan aplica a los riesgos de seguridad y privacidad de la información asociados al proceso de Sistemas de Información, incluyendo los activos de información, sistemas de información, aplicaciones, bases de datos, infraestructura tecnológica, redes, equipos de cómputo, servicios tecnológicos y servicios suministrados por terceros.

Comprende la gestión de los riesgos registrados en la Matriz de Riesgos institucional y las situaciones que puedan ser identificadas mediante auditorías, reportes de proveedores, incidentes de seguridad, revisiones técnicas o actividades de seguimiento.

3. RESPONSABLE

Área de Sistemas de Información:

Es responsable de:

- Identificar y analizar riesgos y vulnerabilidades asociados con la seguridad de la información y la infraestructura tecnológica.
- Mantener actualizada la información correspondiente al proceso dentro de la Matriz de Riesgos institucional.
- Definir e implementar acciones de tratamiento de acuerdo con el nivel de riesgo identificado.

- Gestionar técnicamente los controles de seguridad, accesos, infraestructura, redes, sistemas de información y atención de incidentes.
- Realizar seguimiento a las acciones establecidas en el presente Plan.
- Conservar y organizar las evidencias que soporten la ejecución y efectividad de los tratamientos.
- Escalar las necesidades que requieran inversión, contratación o decisión institucional.

Líder del proceso de Sistemas de Información:

Es responsable de validar los riesgos identificados, priorizar las acciones de tratamiento, gestionar los recursos necesarios y realizar seguimiento al cumplimiento del Plan.

Líderes de procesos y terceros:

Los líderes de procesos, supervisores de contratos, proveedores y demás actores involucrados deberán ejecutar o apoyar las acciones que les sean asignadas y suministrar las evidencias necesarias para su seguimiento.

Alta Dirección o instancia institucional competente:

Intervendrá cuando el tratamiento de un riesgo requiera decisiones estratégicas, asignación significativa de recursos o cuando se proponga aceptar un riesgo residual que se encuentre por encima del nivel de aceptación definido institucionalmente.

4. DEFINICIONES

Activo de información: Información, recurso tecnológico, aplicación, infraestructura, servicio o elemento que posee valor para la entidad y requiere protección.

Amenaza: Causa potencial de un incidente que puede ocasionar daño a un activo, sistema o proceso institucional.

Confidencialidad: Propiedad de la información de no ser divulgada o puesta a disposición de personas, entidades o procesos no autorizados.

Control: Medida implementada para modificar la probabilidad y/o impacto de un riesgo.

Disponibilidad: Propiedad de la información y los servicios de encontrarse accesibles y utilizables cuando sean requeridos por usuarios autorizados.

Impacto: Consecuencia que puede generar la materialización de un riesgo sobre los objetivos, procesos, información o servicios institucionales.

Integridad: Propiedad relacionada con la exactitud, completitud y protección de la información frente a modificaciones no autorizadas.

Probabilidad: Posibilidad de ocurrencia de un evento de riesgo conforme a la metodología institucional de administración de riesgos.

Riesgo: Posibilidad de ocurrencia de un evento que pueda afectar el cumplimiento de los objetivos o comprometer la confidencialidad, integridad o disponibilidad de la información.

Riesgo inherente: Nivel de riesgo existente antes de considerar la aplicación de controles.

Riesgo residual: Nivel de riesgo resultante después de considerar la efectividad de los controles implementados.

Tratamiento del riesgo: Conjunto de acciones definidas para modificar un riesgo mediante estrategias como reducción, mitigación, corrección, prevención, transferencia, evitación o aceptación debidamente justificada.

Vulnerabilidad: Debilidad de un activo, control, sistema, infraestructura o proceso que puede ser aprovechada por una amenaza.

Incidente de seguridad de la información: Evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información o de los servicios tecnológicos institucionales.

5. DESCRIPCION

5.1 Gestión de riesgos de seguridad y privacidad de la información

La gestión de riesgos de seguridad y privacidad de la información se realizará de manera articulada con la Matriz de Riesgos institucional, en la cual se identifican los riesgos, sus causas, consecuencias, controles, valoración y nivel de riesgo residual.

El presente Plan toma como referencia dicha matriz para establecer y realizar seguimiento a las acciones de tratamiento que correspondan.

La identificación o detección de una vulnerabilidad no implicará necesariamente la creación de un nuevo riesgo institucional. El Área de Sistemas de Información evaluará su relación con los riesgos existentes y determinará, de acuerdo con su naturaleza e impacto, el tratamiento correspondiente.

5.2 Valoración de los riesgos

La valoración de probabilidad, impacto y nivel de riesgo será la establecida en la metodología institucional de administración de riesgos y registrada en la Matriz de Riesgos vigente.

El presente Plan no establece una metodología adicional o independiente de valoración.

Las decisiones de tratamiento deberán considerar, entre otros aspectos:

- El nivel de riesgo identificado.
- La afectación potencial sobre la confidencialidad, integridad y disponibilidad.
- La criticidad del activo o servicio afectado.
- Los controles existentes.
- La viabilidad técnica, administrativa y presupuestal de las acciones.

5.3 Tratamiento de riesgos

De acuerdo con la valoración realizada, podrán implementarse acciones orientadas a:

- Prevenir la materialización del riesgo.
- Reducir su probabilidad o impacto.
- Mitigar sus posibles consecuencias.
- Eliminar o aislar una condición vulnerable.
- Fortalecer los controles existentes.
- Transferir el riesgo cuando corresponda.
- Aceptar el riesgo cuando su nivel residual y contexto institucional lo permitan.

Las acciones de tratamiento serán registradas y gestionadas mediante la Matriz de Riesgos, planes institucionales, planes de acción, proyectos tecnológicos u otros instrumentos de gestión aplicables.

Cuando una acción requiera recursos económicos, su implementación estará sujeta a la planeación institucional, disponibilidad presupuestal y priorización de necesidades.

5.4 Gestión de vulnerabilidades

Las vulnerabilidades de seguridad de la información podrán ser identificadas mediante:

- Auditorías internas o externas.
- Informes de proveedores tecnológicos.
- Incidentes de seguridad.
- Actividades de monitoreo.
- Revisiones técnicas.
- Cambios en infraestructura o sistemas.
- Reportes de usuarios o terceros.

Una vez identificada una vulnerabilidad, el Área de Sistemas de Información realizará su análisis y determinará las acciones que sean aplicables, de acuerdo con el riesgo asociado y las condiciones institucionales.

El tratamiento podrá incluir corrección, mitigación, aislamiento, actualización, implementación de controles compensatorios o aceptación debidamente justificada.

Para efectos de trazabilidad, las vulnerabilidades identificadas que requieran tratamiento deberán contar con un registro o evidencia de seguimiento, el cual podrá conservarse mediante formato, matriz, plan de acción, informe técnico o repositorio definido por el Área de Sistemas de Información.

5.5 Seguimiento

El seguimiento a los riesgos se realizará conforme a los mecanismos establecidos en la Matriz de Riesgos institucional y en los instrumentos de seguimiento del proceso.

Las acciones de tratamiento que se encuentren en ejecución deberán contar con evidencia que permita verificar su avance o cumplimiento.

El seguimiento podrá apoyarse en:

- Matriz de Riesgos.
- Planes de acción.
- Informes de seguimiento.
- Tickets o registros de mesa de ayuda.
- Informes de proveedores.
- Actas.
- Inventarios.
- Registros técnicos.

- Evidencias de configuración, adquisición o intervención.

Cuando se identifiquen cambios relevantes en los riesgos, vulnerabilidades o controles existentes, se evaluará la necesidad de actualizar la Matriz de Riesgos o las acciones de tratamiento.

5.6 Verificación de las acciones de tratamiento

La verificación tendrá como propósito determinar si las acciones definidas fueron implementadas y si contribuyeron a controlar o reducir la condición de riesgo identificada.

La verificación podrá realizarse mediante revisión documental, validación técnica, revisión de evidencias, seguimiento a la Matriz de Riesgos o evaluación del estado de las acciones definidas.

Cuando una acción no haya logrado el resultado esperado o se identifique una nueva condición que incremente el riesgo, se podrán establecer acciones adicionales de mejora.

5.7 Aceptación de riesgos

La aceptación de un riesgo deberá estar sustentada en la valoración registrada en la Matriz de Riesgos y en los controles existentes.

Cuando se determine que un riesgo puede mantenerse bajo los controles existentes, deberá quedar documentada la justificación correspondiente dentro de la Matriz de Riesgos o instrumento de seguimiento aplicable.

Los riesgos que por su nivel, impacto o necesidad de recursos requieran una decisión institucional serán evaluados para determinar la necesidad de escalamiento a la instancia correspondiente

La aceptación de un riesgo no impide que este sea revisado posteriormente cuando cambien las condiciones que dieron origen a su valoración.

6. DOCUMENTOS RELACIONADOS

- MA-SI-MA-027 Manual de seguridad digital.
- MA-SI-MA-013 Manual de Gerencia de la Información.
- MD-DE-PO-035 Política de Privacidad y Tratamiento de Datos.
- MD-DE-PO-036 Política de Gerencia de la Información.
- MD-DE-PO-046 POLÍTICA DE GOBIERNO Y SEGURIDAD DIGITAL.
- Matriz de Riesgos vigente – Sistemas de Información.

7. REGISTROS RELACIONADOS

- MA-SI-RE-020 Aviso privacidad y tratamiento de datos.
- MA-SI-RE-039 Lista de chequeo ronda de seguridad - sistemas.
- MA-SI-RE-046 Compromiso de buen uso de tecnología informática y seguridad digital.

8. BIBLIOGRAFIA

- Resolución 02277 del 3 de junio de 2025.
- La Constitución política de 1991. Artículos 15 y 20.
- Ley 1581 de 2012.
- Decreto Reglamentario 1377 de 2013.
- Decreto 612 del 4 de abril de 2018.
- Decreto 1008 del 14 de junio de 2018.

9. CONTROL DE CAMBIOS

Cambios: Se actualiza el Plan Institucional de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, fortaleciendo su articulación con la Matriz de Riesgos institucional e incorporando lineamientos para la valoración, tratamiento, gestión de vulnerabilidades, seguimiento, verificación y aceptación de los riesgos de seguridad y privacidad de la información. Se actualizan responsables, definiciones, documentos relacionados, registros relacionados y referencias normativas aplicables.

Justificación: Fortalecer la gestión y trazabilidad de los riesgos de seguridad y privacidad de la información conforme a la matriz institucional y a los lineamientos vigentes de seguridad digital.

Elaboró:	Revisó:	Aprobó:

William Fernando Leyes Jimenez Profesional Administrativo	Andres Santacoloma Analista de Gestión de Procesos de Calidad Sandra Patricia Vargas Garcia Coordinador de Sistemas	Nini Yojana Renteria Angulo Coordinador de Calidad

Andres Santacoloma @ 2026-08-24, 9:46:22