EMPRESA SOCIAL DEL ESTADO HOSPITAL UNIVERSITARIO SAN RAFAEL DE TUNJA

INFORME
SEGUIMIENTO MAPA DE RIESGOS POR PROCESO CON CORTE A JUNIO DE 2023

Elaborado
OFICINA ASESORA DE CONTROL INTERNO

Tunja, agosto de 2023

INTRODUCCIÓN

Teniendo en cuenta que con la expedición del Decreto 1499 de 2017 "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015", se crea un solo Sistema de Gestión y se alinea con el Sistema de Control Interno, hoy todas las entidades públicas requieren actualizar y/o implementar el Modelo Integrado de Planeación y Gestión MIPG, modelo que incorpora el Modelo Estándar de Control Interno MECI a través de la séptima dimensión del mismo.

Esta estructura requiere de un análisis articulado frente al desarrollo de las políticas de gestión y desempeño contenidas en el modelo y su efectividad en relación con la estructura de control, este último, aspecto especial para garantizar el buen manejo de los recursos, que las metas y objetivos se cumplan y se mejore la prestación del servicio a los usuarios, ejes fundamentales para la generación de valor público. Dentro de dicho Modelo se encuentra el componente denominado Evaluación de Riesgos.

Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las unidades de control interno o quien haga sus veces, evaluando aspectos, tanto internos como externos, que pueden llegar a representar amenaza para la consecución de los objetivos organizacionales, con miras a establecer acciones efectivas, representadas en actividades de control.

Artículo 17 del Decreto N° 648 de 2017 que modifica el Artículo 2.2.21.5.3 del Decreto N° 1083 de 2015, donde se define los roles que debe cumplir las oficinas de Control interno de Gestión
Los cuales juegan un papel fundamental, a través de la asesoría, acompañamiento técnico y de evaluación y seguimiento a los diferentes pasos de la gestión del riesgo, que van desde la fijación de la política de administración de riesgo hasta la evaluación de la efectividad de los controles

Que según el establecido Acuerdo 015 de 30 de junio de 2023 La junta directiva de la E.S.E Hospital Universitario san Rafael de Tunja aprueba la política de gestión de riesgo integral de la Empresa social de Estado Hospital Universitario san Rafael de Tunja

En el marco de lo expuesto y el Rol de evaluación de la gestión del riesgo, se presenta el siguiente informe, teniendo en cuenta el mapa de riesgos institucional consolidado, y la política de administración del riesgo integral de la E.S.E hospital universitario san Rafael de Tunja

OBJETIVO

Evaluar la Gestión del riesgo de la E.S.E Hospital universitaria san Rafael de Tunja, validando que la línea estratégica, la primera línea y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos estratégicos, de acuerdo a lo establecido en Acuerdo 015 de 30 de junio de 2023

OBJETIVOS ESPECÍFICIOS

- Revisar el adecuado diseño de los riesgos identificados, de acuerdo a los lineamientos de la **Guía para la administración del riesgo y el diseño de controles en entidades públicas" Versión 6**

- Revisar el adecuado diseño y estructura de los controles para la mitigación de los riesgos establecidos por parte de la Primer Línea de Defensa, de acuerdo a los lineamientos de la **Guía para la administración del riesgo y el diseño de controles en entidades públicas" Versión 6**

- Hacer seguimiento a las actividades de control establecidas para la mitigación de los riesgos de los subprocesos que se encuentren documentadas y actualizadas.

- Realizar la correlación de los hallazgos de la Auditoría realizada por la Contraloría General de Boyacá/Riesgos identificados mapa de riesgos 2023

ALCANCE DEL SEGUIMIENTO

La evaluación aplica para todos los Procesos y Subprocesos de la E.S.E Hospital Universitario San Rafael de Tunja que tiene identificados riesgos de proceso, en lo que corresponde al primer semestre de la vigencia 2023.

CRITERIOS DE EVALUACION

- Ley 87 de 1993, por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.
- Artículo 17 del Decreto N° 648 de 2017 que modifica el Artículo 2.2.21.5.3 del Decreto N° 1083 de 2015, donde se define los roles que debe cumplir las oficinas de Control interno de Gestión.

- Ley 1474 de 2011, por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión
- Guía para la administración del riesgo y el diseño de controles en entidades públicas" Versión 6
- Dimensión 7 Control Interno – Modelo Integrado de Planeación y Gestión - MIPG
- Manual de Gestión del riesgo OADS-M-02
- Guía Rol de las Oficinas de Control Interno o quien hace sus veces Versión 3
- Acuerdo 015 de 30 de junio de 2023 "Por medio del cual se adopta la política de gestión de riesgo integral de la Empresa social de Estado Hospital Universitario san Rafael de Tunja"
- Circular externa de la Superintendencia nacional de salud 20211700000004-5 de 2021

METODOLOGÍA:

La metodología utilizada para la revisión, análisis y evaluación de la Gestión de los riesgos se realizó teniendo en cuenta los siguientes criterios:

1. Mapa de riesgos publicado en página web institucional
2. Responsabilidades de la Gestión del riesgo de la primera y segunda línea de defensa de acuerdo a lo establecido en el Acuerdo 015 de 30 de junio de 2023 política de gestión de riesgo integral
3. Procedimiento de Gestión y Administración de riesgos OADS-PR-11
4. Manual de Gestión del Riesgos OADS-M-02
5. Verificación de las evidencias que soportan los avances en cada uno de procesos, cargadas en link dispuesto por Gestión de riesgos, las cuales son insumo necesario para generar valor agregado al seguimiento.

En la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" Versión 6, se encuentran las definiciones claves que fueron tenidas en cuenta para aplicación de la metodología y por ende la elaboración del presente informe, por tanto, se recomienda su lectura y apropiación.

Se aclara que para la evaluación correspondiente al primer semestre de 2023 no se realiza la efectividad de los controles, teniendo en cuenta que de acuerdo al cronograma dispuesto por la segunda línea de defensa (Gestión del riesgo), mediante mesas de trabajo con los procesos realizadas del 17 al 29 de julio de 2023, fueron identificados nuevos riesgos y actualizados los existentes, siendo este mapa de riesgos el insumo para realizar la evaluación. La efectividad de los controles se medirá para el segundo semestre del 2023

Hace parte de este informe archivo denominado: "Evaluación del Mapa de riesgos – primer semestre de 2023", el cual contiene la matriz Excel donde se registraron las observaciones para

cada uno de los 104 controles correspondientes a los 80 riesgos institucionales de los diferentes procesos del HUSRT

DESARROLLO DEL SEGUIMIENTO

1. SEGUIMIENTO A LA POLÍTICA DE GESTION DEL RIESGO INTEGRAL

Teniendo en cuenta lo establecido en la Circular externa de la Superintendencia Nacional de Salud 20211700000004-5 de 2021 POR LA CUAL SE IMPARTEN INSTRUCCIONES GENERALES RELATIVAS AL CÓDIGO DE CONDUCTA Y DE BUEN GOBIERNO ORGANIZACIONAL, EL SISTEMA INTEGRADO DE GESTIÓN DE RIESGOS Y A SUS SUBSISTEMAS DE ADMINISTRACIÓN DE RIESGOS, la Empresa Social de Estado Hospital Universitario san Rafael de Tunja , adopta la política de gestión de riesgo integral mediante el Acuerdo 015 de 2023, documento por medio de la cual se deroga la resolución 141 del 2023 y se adopta la política de gestión de riesgos integral, la E.S.E Hospital Universitario San Rafael de Tunja se compromete a gestionar los riesgos de manera integral por medio de estrategias que permitan evitar, reducir, mitigar, compartir, aceptar, controlar, minimizar y/o evitar la ocurrencia de eventos no deseados que puedan afectar positiva o negativamente el logro de los objetivos institucionales.

Documento que se puede consultar en la página web institucional en la siguiente ruta: Inicio - Transparencia y acceso a la información pública - 2. Normatividad - 2.1 Políticas institucionales - 5. Política de gestión del riesgo integral o ingresando al siguiente link: https://www.hospitalsanrafaeltunja.gov.co/contenido.php?id=229&seccion=transparencia-y-acceso-a-la-informacion-publica&slug=acuerdos ,

Fuente: Pantallazo página web institucional

La Política de Gestión de Riesgos Integral tiene definido dentro de su estructura, Compromiso, el objetivo, el alcance, metodología, los responsables y sus roles, niveles de aceptación del riesgo y comunicación y socialización.

La Guía para la administración del riesgo y el diseño de controles en entidades públicas" Versión 6 establece los aspectos mininos que debe cumplir la Política de administración de riesgos los cuales describo a continuación:

LINEAMIENTOS MINIMOS SEGÚN GUIA ADMINISTRACION RIESGOS
La metodología a utilizar.
Niveles de Responsabilidad y autoridad frente a la Administración del riesgo en la entidad (acorde con el esquema de líneas de defensa).
Acorde con el punto anterior, incluir la periodicidad para el monitoreo y revisión de los riesgos, donde se determine el seguimiento a los controles establecidos.
En caso de que la entidad haya dispuesto un software o herramienta para su desarrollo, deberá explicarse su manejo.
Incluir los aspectos relevantes sobre los factores de riesgo estratégicos para la entidad, a partir de los cuales todos los procesos podrán iniciar con los análisis para el establecimiento del contexto.
Incluir todos aquellos lineamientos que en cada paso de la metodología sean necesarios para que todos los procesos puedan iniciar con los análisis correspondientes.
Incluir los niveles de riesgo aceptado para la entidad y su forma de manejo.
Incluir las tablas de probabilidad e impacto institucional.
Incorporar los lineamientos para el manejo de riesgo fiscal, aquellos relacionados con posibles actos de corrupción y el anexo metodológico para la gestión de riesgos de seguridad de la información, temas articulados en la presente guía.

Se recomienda a la segunda línea de defensa incluir en el Manual de riesgos los lineamientos para el manejo de riesgo fiscal y el anexo metodológico para la gestión de riesgos de seguridad de la información, de acuerdo a lo establecido en el capítulo 4 de la **Guía para la administración del riesgo y el diseño de controles en entidades públicas" Versión 6**.

2. SEGUIMIENTO A LAS HERRAMIENTAS PARA LA ADMINISTRACIÓN DE RIESGOS

2.1 PROCEDIMIENTO DE GESTIÓN Y ADMINISTRACIÓN DE RIESGOS OADS-PR-11

En el listado maestro de documentos de DARUMA se encuentra publicado el Procedimiento de Gestión y Administración de riesgos OADS-PR-11, dentro de sus actividades se encuentran descritas las etapas de identificación, análisis, evaluación, monitoreo y seguimiento de los controles establecidos, con el fin de prevenir o mitigar los eventos que puedan afectar el cumplimiento de los objetivos estratégicos y de procesos, Procedimiento con última actualización del 01 de julio de 2022.

Al verificar el procedimiento en mención se evidencia que no está actualizado de acuerdo a los lineamientos de la política de Gestión de riesgo integral Acuerdo 015 de 2023, toda vez que el

responsable de este procedimiento ya no es la oficina de planeación, sino la Coordinación de riesgos integral, adicionalmente la metodología fue ajustada por la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6

A su vez se observa incumplimiento a la actividad 12 "Una vez consolidados Mapas de Riesgo Se presenta en Comité de Gestión y desempeño los Mapas de Riesgo de los procesos aplicables, para su conocimiento y aprobación", esto teniendo en cuenta que el mapa de riesgos de gestión fue publicado sin la debida aprobación.

2.1.1 SEGUIMIENTO PRIMERA LINEA

La actividad 15 del procedimiento indica que: Para riesgos de proceso y riesgos de los sistemas de Gestión se realiza un primer seguimiento por primera línea de defensa desde el rol del Responsable del proceso (Autocontrol) presentando reporte de seguimiento a la oficina de planeación en formato OADS-F-36.

En el sistema de gestión documental DARUMA se encuentra publicado el formato OADS-F-36. FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSA, con última fecha de actualización 17 de julio de 2023.

Es importante recordar lo establecido en la Guía para la administración del riesgo del departamento administrativo de la función pública. Versión 6 ***"Desde la 1ª línea de defensa todos los servidores tienen una responsabilidad frente a la aplicación efectiva de los controles, por lo que se trata de un seguimiento permanente, esto incluye la aplicación de controles de gerencia operativa que corresponde a aquellos que son aplicados por servidores con personal a cargo (jefes, coordinadores u otro cargo)."***

Para verificar esta actividad la Oficina asesora de control interno verifico, que los sub procesos adjunten el formato debidamente diligenciado y firmado en el link establecido para subir las respectivas evidencias de la ejecución de los controles, resultado que se presenta a continuación:

PROCESOS ESTRATÉGICOS

	PROCESO	RIESGOS	CONTROLES	SEGUIMIENTO 1a LINEA DE DEFENSA
PROCESOS ESTRATEGICOS	Direccionamiento Estratégico y humanización	2	2	Adjuntan OADS-F-36 FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, en PDF, DEBIDAMENTE FIRMADO POR QUIEN ELABORO Y APROBO
	Gestión QHSE	6	9	Adjuntan FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin firmas de quien elaboró y revisó.
	Gestión de investigación e innovación	2	2	Adjuntan FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin firmas de quien elaboró y revisó
	Gestión de talento humano	3	4	Adjuntan FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin firmas de quien elaboró y revisó
	TOTAL	13	17	

Fuente: Propia – Revisión OACI seguimiento líneas de defensa

El seguimiento por parte de la primera línea de defensa de los procesos estratégicos, lo realizan los 4 procesos que tiene identificados riesgos de proceso, sin embargo, es de resaltar que el único proceso que adjunto el formato OADS-F-36 FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, en pdf debidamente firmado por quien elaboró y aprobó, fue el proceso Direccionamiento Estratégico y humanización, los demás procesos adjuntan soportes sin las debidas firmas.

Se recomienda a los líderes de proceso diligenciar en el formato correspondiente, el nombre de quien elaboró y revisó, adjuntando sus respectivas firmas, lo cual se convierte en la prueba del conocimiento y de la verificación de la integridad y aprobación de la información contenida en un documento

PROCESOS MISIONALES

	PROCESO	RIESGOS	CONTROLES	SEGUIMIENTO 1a LINEA DE DEFENSA
PROCESOS MISIONALES	Gestión Clínica	2	3	Adjuntan OADS-F-36 FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin firmas de quien elaboró y revisó
	Unidad de Cuidado Intensivo	2	3	Adjuntan OADS-F-36 FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, formato sin firmas de quien elaboró y revisó
	Gestión Quirúrgica	2	3	Adjuntan OADS-F-36 FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin firmas de quien elaboró y revisó
	Atención de Urgencias	2	3	Adjuntan OADS-F-36 FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin firmas de quien elaboró y revisó
	Enfermería	2	2	Adjuntan OADS-F-36 FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin firmas de quien elaboró y revisó
	Epidemiología y Salud Pública	1	1	Adjuntan OADS-F-36 FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin firmas de quien elaboró y revisó
	Gestión farmacéutica	6	7	Adjuntan OADS-F-36 FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin firmas de quien elaboró y revisó
	Sistema de información y atención al usuario	2	2	Adjuntan OADS-F-36 FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin firmas de quien elaboró y revisó
	Apoyo servicios de salud	1	1	Adjuntan OADS-F-36 FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin firmas de quien elaboró y revisó
	TOTAL	20	25	

Fuente: Propia – Revisión OACI seguimiento líneas de defensa

El seguimiento por parte de la primera línea de defensa de los procesos misionales, lo realizan 9 procesos que tiene identificados riesgos de proceso, los cuales adjuntan el formato OADS-F-36 FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin embargo, se evidencia que los formato no cuenta con las respectivas firmas

Se recomienda a los líderes de proceso diligenciar en el formato correspondiente, el nombre de quien elaboro y reviso, adjuntando sus respectivas firmas, lo cual se convierte en la prueba del conocimiento y de la verificación de la integridad y aprobación de la información contenida en un documento

PROCESOS DE APOYO

	PROCESO	RIESGOS	CONTROLES	SEGUIMIENTO 1a LINEA DE DEFENSA
PROCESOS APOYO	Gestión Financiera	11	15	Adjuntan FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, por subprocesos (contabilidad, presupuesto y tesorería) sin firmas de quien elaboró y revisó., se recomienda describir en el formato únicamente los riesgos asociados a cada subproceso.
	Gestión Administrativa	15	17	Adjuntan FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, por subprocesos (auditoría de cuentas médicas, autorizaciones, cartera y facturación) sin firmas de quien elaboró y revisó.
	Gestión Documental	2	2	Adjuntan FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin firmas de quien elaboró y revisó.
	Gestión de la Tecnología	2	3	Adjuntan FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, formato versión 1 desactualizado, sin firmas de quien elaboró y revisó. El líder del proceso indica que de los dos riegos asociados al proceso se materializo uno.
	Gestión Mantenimiento	2	2	Adjuntan FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, formato versión 1 desactualizado, sin firmas de quien elaboró y revisó.
	Gestión de Suministros y Activos Fijos	3	4	Adjuntan FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin firmas de quien elaboró y revisó.
	Gestión Jurídica	2	2	Adjuntan FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin firmas de quien elaboró y revisó.
	Gestión Servicios de apoyo-TERCERIZADOS	1	2	Adjuntan FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin firmas de quien elaboró y revisó.
	Gestión de sistemas de información y comunicación	3	6	Adjuntan FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, formato versión 1 desactualizado, sin firmas de quien elaboró y revisó.
	Gestión contratación	4	4	Adjuntan FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, en PDF, DEBIDAMENTE FIRMADO POR QUIEN ELABORO Y APROBO
	TOTAL	**45**	**57**	

Fuente: Propia – Revisión OACI seguimiento líneas de defensa

El seguimiento por parte de la primera línea de defensa de los procesos de apoyo, lo realizan 10 procesos que tiene identificados riesgos, los cuales adjuntan el formato OADS-F-36 FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, sin embargo es de resaltar que el único proceso que adjunto el formato OADS-F-36, en pdf debidamente firmado por quien elaboró y aprobó, fue el proceso Gestión contractual, para el caso de Gestión tecnológica y Gestión de mantenimiento aportaron evidencias en formatos desactualizados

Se recomienda a los líderes de proceso diligenciar en el formato correspondiente, el nombre de quien elaboro y reviso, adjuntando sus respectivas firmas, lo cual se convierte en la prueba del conocimiento y de la verificación de la integridad y aprobación de la información contenida en un documento.

PROCESO DE EVALUACIÓN

	PROCESO	RIESGOS	CONTROLES	SEGUIMIENTO 1a LINEA DE DEFENSA
PROCESOS EVALUACION	CONTROL INTERNO	2	5	Adjuntan OADS-F-36 FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS, en PDF, DEBIDAMENTE FIRMADO POR QUIEN ELABORO Y APROBO
	TOTAL	2	5	

Fuente: Propia – Revisión OACI seguimiento líneas de defensa

El proceso de evaluación adjunta formato OADS-F-36 FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS,

La oficina asesora de control interno, evidencia que los 59 sub procesos de la E.S.E realizaron el primer seguimiento por primera línea de defensa desde el rol del responsable del proceso (Autocontrol) adjuntando reporte de seguimiento en formato establecido OADS-F-36, con corte a junio de 2023.

Es importante tener en cuenta que tanto la Política de Gestión de riesgo integral como el Procedimiento de Gestión y Administración de riesgos OADS-PR-11, tiene establecido que el seguimiento por parte de la primera línea (autocontrol), se debe realizar trimestralmente presentando el reporte a la oficina de planeación y según evidencias aportadas por los subprocesos esta actividad se realizó únicamente para el segundo trimestre de 2023.

Se recomienda a los líderes de los procesos verificar, validar y firmar todos los documentos que se convierten en soporte de evidencia para garantizar de forma razonable la entrega de información, lo cual se convierte en la prueba del conocimiento y de la verificación de la integridad y aprobación de la información contenida en un documento, lo anterior teniendo en cuenta que de los 24 procesos, solo 3 procesos (Direccionamiento estratégico, Gestión contractual y evaluación) entregaron los soportes del formato debidamente firmado, tres procesos utilizaron formato OADS-F-36, de la versión anterior, desactualizado (Gestión de mantenimiento, gestión tecnológica y Gestión de sistemas de información y comunicación)

2.1.2. SEGUIMIENTO SEGUNDA LINEA

La actividad 16 del Procedimiento de Gestión y Administración de riesgos OADS-PR-11 **indica**: la Oficina de Planeación, (actualmente coordinación gestión de riesgo) generar informe a nivel institucional de seguimiento a la gestión del Riesgo desde el rol de la Segunda Línea de Defensa semestralmente.

En cumplimiento de esta actividad y de lo establecido en la Política integral de gestión del riesgo la segunda línea de defensa realizo mesas de trabajo con el objeto identificar y actualizar los riesgos y controles existentes, y posteriormente actualizar el mapa de riesgos, Mesas de trabajo realizadas entre del 17 al 26 de julio de 2023.

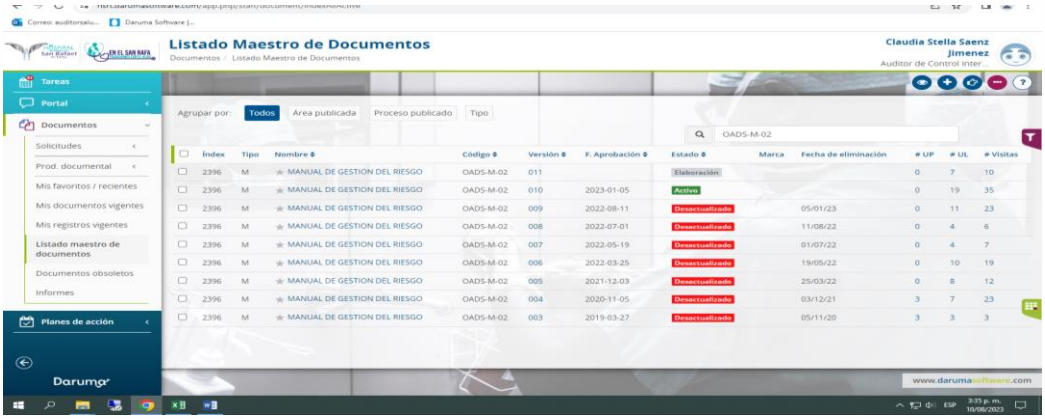
Producto de las mesas de trabajo se Actualizaron el mapa de riesgos institucional el cual fue publicado en la página web institucional el 26 de julio de 2023.

La Coordinación de Gestión del riesgo, elabora informe de Seguimiento segunda línea de defensa Mapa de Riesgos de Gestión, informe que fue dado a conocer mediante correo electrónico a la Oficina asesora de control interno el día 18 de agosto de 2023 y socializado en Comité institucional de coordinación de control interno el 22 de agosto del 2023

2.2 MANUAL DE GESTIÓN DEL RIESGO CÓDIGO: OADS-M-02

En el sistema de gestión documental DARUMA se encuentra publicado el Manual de gestión del riesgo con última fecha de actualización el 07 de julio de 2022 y cuyo objeto general es: Establecer los parámetros para la gestión del riesgo en la E.S.E Hospital Universitario San Rafael de Tunja, asegurando la trazabilidad y seguimiento a los riesgos que puedan afectar el cumplimiento de la misión y objetivos institucionales.

A la fecha se evidencia que el Manual de gestión del riesgo se encuentra en estado de elaboración, por tal razón se estaría incumpliendo lo normado en el artículo cuarto del Acuerdo 015 de 2023, METODOLOGÍA, toda vez que es el documento Establecer los parámetros para la gestión del riesgo en la E.S.E Hospital Universitario San Rafael, lo cual se puede observar en la siguiente imagen.



Fuente: Pantallazo listado maestro de documentos, DARUMA

2.3 MAPA DE RIESGOS INSTITUCIONAL

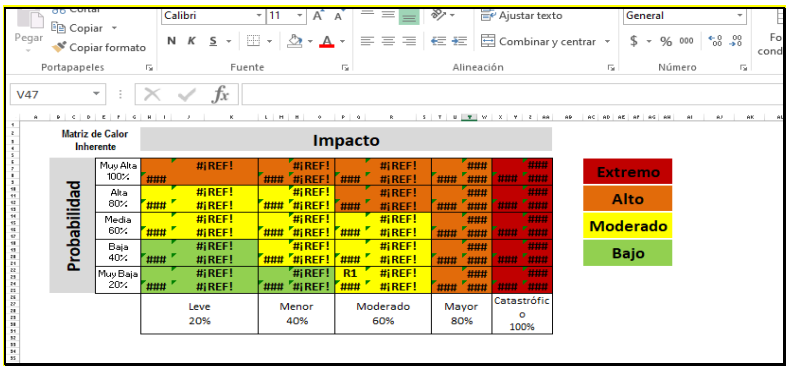
Consultando la página web de la ESE Hospital Universitario San Rafael de Tunja, dentro de la ruta Nuestra entidad, se encontró publicada la matriz OADS-F-13, Mapa de riesgos de Gestión como se observa en la siguiente imagen

Fuente: Pantallazo página web institucional

Adicionalmente el mapa de riesgos de gestión se puede consultar en el siguiente enlace: https://www.hospitalsanrafaeltunja.gov.co/contenido.php?id=388&seccion=nuestra--entidad&slug=mapa-de-riesgos-de-gestion

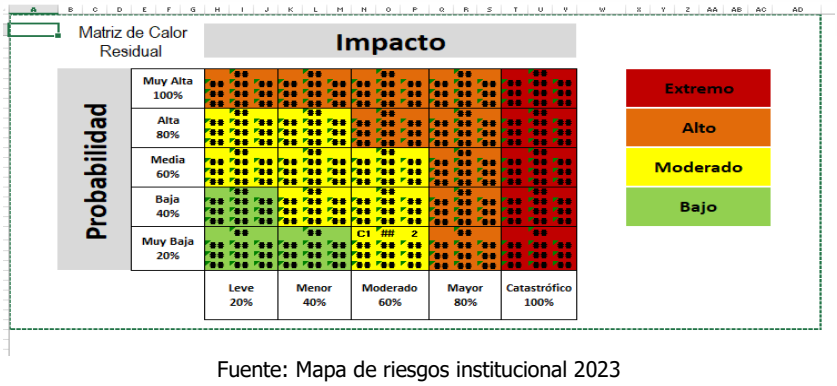
Es importante tener en cuenta lo establecido en la actividad No 12 del procedimiento GESTIÓN Y ADMINISTRACIÓN DE RIESGOS OADS-PR-11, la cual indica lo siguiente: "Una vez consolidados Mapas de Riesgo, Se presenta en Comité de Gestión y desempeño los Mapas de Riesgo de los procesos aplicables, para su conocimiento y aprobación", teniendo en cuenta lo anterior se evidencia incumplimiento a este procedimiento ya que el mapa fue publicado sin la debida aprobación.

Al verificar la matriz de riesgos se observa en la Hoja 3 Matriz de Calor Inherente, no se encuentra parametrizada o formulada, teniendo en cuenta que, en esta hoja, en la medida en que esa diligencia el Mapa Final, se verán reflejados los riesgos en su zona correspondiente. Esta hoja no se diligencia se genera de manera automática.



Fuente: Mapa de riesgos institucional 2023

Lo mismo se evidencia en la Hoja 4 Matriz de Calor Residual: En esta hoja, en la medida en que ese diligencia el Mapa Final, se verán reflejados los riesgos en su zona correspondiente. Esta hoja no se diligencia se genera de manera automática.



Fuente: Mapa de riesgos institucional 2023

3. IDENTIFICACIÓN DE RIESGOS Y CONTROLES

Conforme a la Guía para la administración del riesgo y el diseño de controles en entidades públicas – versión 6; esta etapa tiene como objeto identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Del 17 de julio al 26 de julio de 2023, Gestión del riesgo, realizo mesas de trabajo con el objetivo de, identificar nuevos riesgos y controles y actualizar los mapas de riesgos institucionales.

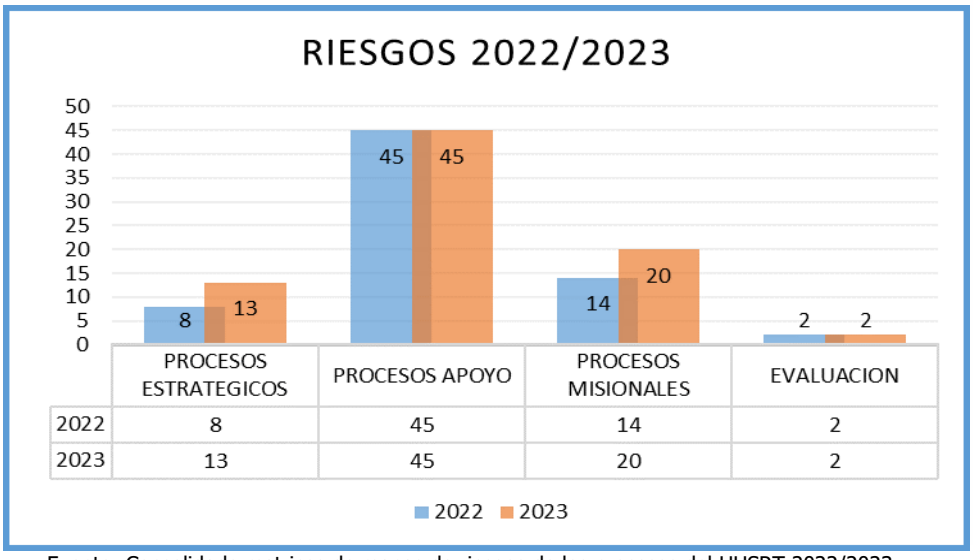
Como resultado de estas mesas de trabajo se identifican nuevos riesgos y controles, actualizando el mapa de riesgos institucional de la vigencia 2023, los cuales se distribuyen en los diferentes procesos de la siguiente manera:

	PROCESO	RIESGOS 2022	RIESGOS 2023	CONTROLES 2022	CONTROLES 2023	ACCIONES 2022	ACCIONES 2023
PROCESOS ESTRATEGICOS	Direccionamiento Estratégico y humanización	1	2	1	2	1	1
	Gestión QHSE	2	6	4	9	2	3
	Gestión de investigación e innovación	2	2	2	2	0	0
	Gestión de talento humano	3	3	4	4	0	0
PROCESOS APOYO	Gestión Financiera	11	11	15	15	1	4
	Gestión Administrativa	15	15	17	17	6	10
	Gestión Documental	2	2	2	2	0	0
	Gestión de la Tecnología	2	2	3	3	2	0
	Gestión Mantenimiento	2	2	2	2	1	1
	Gestión de Suministros y Activos Fijos	3	3	4	4	1	1
	Gestión Jurídica	2	2	2	2	1	0
	Gestión Servicios de apoyo-TERCERIZADOS	1	1	2	2	1	1
	Gestión de sistemas de información y comunicación	3	3	6	6	1	2
	Gestión contratación	4	4	4	4	0	3
PROCESOS MISIONALES	Gestión Clínica	2	2	3	3	1	2
	Unidad de Cuidado Intensivo	2	2	3	3	1	0
	Gestión Quirúrgica	2	2	3	3	1	0
	Atención de Urgencias	2	2	3	3	1	0

	Enfermería	2	2	3	2	1	0
	Epidemiología y Salud Pública	1	1	1	1	0	0
	Gestión farmacéutica	0	6	0	7	0	0
	Sistema de información y atención al usuario	2	2	2	2	1	2
	Apoyo servicios de salud	1	1	1	1	0	0
EVALUACION	Control Interno	2	2	5	5	0	0
	TOTAL	69	80	92	104	23	30

Fuente: Consolidado matrices de mapas de riesgos de los procesos del HUSRT

El mapa de riesgos de la ESE Hospital Universitario San Rafael de Tunja, vigencia 2023, identificaron 11 riegos nuevos para un total de 80 riesgos de proceso y 12 nuevos controles para un total de 104 controles asociados respectivamente, dando cumplimiento a los lineamientos establecido en la Guía para la administración del riesgo del departamento administrativo de la función pública. Versión 6, los cuales se encuentran distribuidos en los 24 procesos de la entidad de la siguiente manera:



	PROCESOS ESTRATEGICOS	PROCESOS APOYO	PROCESOS MISIONALES	EVALUACION
2022	8	45	14	2
2023	13	45	20	2

Fuente: Consolidado matrices de mapas de riesgos de los procesos del HUSRT 2022/2023

4. SEGUIMIENTO RIESGOS POR PROCESO TERCERA LINEA DEFENSA – CONTROL INTERNO

Para la evaluación del estado de la Gestión del Riesgo la Oficina Asesora de Control Interno del HUSRT, utilizó el archivo denominado: "Evaluación del Mapa de riesgos – segundo semestre de 2023", el cual contiene la matriz Excel agregándole una columna que contiene las observaciones realizadas por la Oficina de control interno segundo semestre 2023. En este aparte se

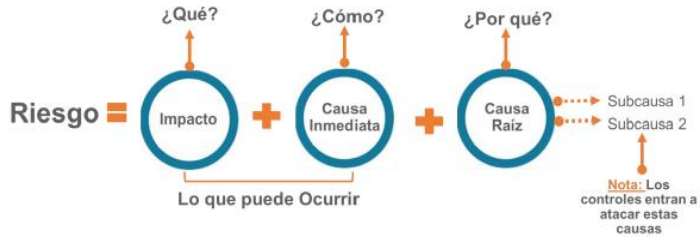
registraron las conclusiones del análisis metodológico del diseño del riesgo y del control, y el aporte de evidencias, se realizan comentarios acerca de la materialización u ocurrencia del riesgo y recomendaciones con el fin de mejorar el proceso de administración del riesgo y la aplicación de la metodología dispuesta por el DAFP.

Esta verificación se realizó en base a las evidencias que soportan los avances en la gestión del riesgo en cada una de procesos de la ESE, las cuales fueron cargadas en el Link que dispuso Gestión de riesgo, en algunas ocasiones fueron tomadas otras evidencias que se encuentran publicadas en la página web del HUSRT, plataforma Daruma y evaluaciones o Auditorías realizadas por control interno

Se anexa matriz Excel donde se dejaron registradas las observaciones para cada uno de los 104 controles correspondientes a los 80 riesgos institucionales de los diferentes procesos del HUSRT, en la cual se analizaron los siguientes criterios:

4.1 DESCRIPCIÓN DE LOS RIESGOS: Para realizar el análisis del diseño de los riesgos de los procesos se aplicaron los criterios establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6, respectivamente

Figura 10 Estructura propuesta para la redacción del riesgo



Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

4.2 DESCRIPCION DE LOS CONTROLES. Para que un control este adecuadamente diseñado y que su implementación sea efectiva a la hora de mitigar un riesgo debe cumplir con la siguiente estructura definida en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6

- **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.

■ **Complemento**: corresponde a los detalles que permiten identificar claramente el objeto del control.

4.3 ESCALA DE SEVERIDAD DEL RIESGO

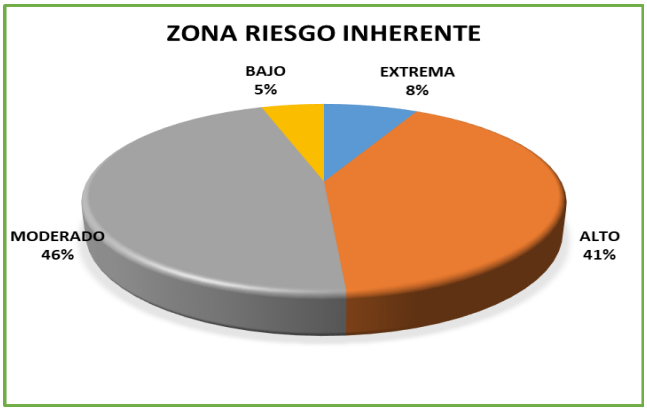
Conforme a las directrices metodológicas de la *Guía para la administración del riesgo del departamento administrativo de la función pública. Versión 6,* ante la identificación de riesgos inherentes, corresponde el diseño y la aplicación de controles orientados a una debida orientación de los componentes de probabilidad e impacto asociados al riesgo y de esta manera disminuirlos a límites razonables según sea el caso, llegando a un nivel de riesgo residual.

Resultado de la aplicación del diseño e implementación de los controles, el panorama de los riesgos residuales reportados por el HUSRT, se presenta de la siguiente manera:

RIESGO INHERENTE

ZONA DE RIESGO	ZONA RIESGO INHERENTE	PORCENTAJE
EXTREMA	6	7,50%
ALTO	33	41%
MODERADO	37	46,25%
BAJO	4	5%

En la Tabla observamos la dinámica en el riesgo inherente de acuerdo a la severidad de la zona donde se evidencia que la mayoría de riesgos de ubican en zona moderada (46%) y Alta con un (41%). (Ver gráfica 2).



Grafica 2

RIESGO RESIDUAL

ZONA DE RIESGO	ZONA DE RIESGO FINAL	PORCENTAJE
EXTREMA	6	7,50%
ALTO	18	22,50%
MODERADO	43	54%
BAJO	13	16,25%

Por otra parte, observamos la dinámica en el riesgo Residual de acuerdo a la severidad de la zona donde se evidencia que la mayoría de riesgos de ubican en zona Moderada (54%) y alta (22.5%).

Grafica 3

Lo que se puede observar es que los riesgos de zonas altas, los cuales eran 33, bajaron a 18 en zona residual, lo que indica que los controles son efectivos.

Para el caso de riesgos ubicados en zona extrema se mantienen en la misma zona, no obstante, se evidenció que, del total de riesgos identificados, 43 se encuentran en zona de riesgos moderada, es decir que el 54% moderado y 13 se encuentran en zona bajo, es decir el 16,25% bajo.

De acuerdo con la tabla anterior, se observa que después de realizar la respectiva valoración de controles, seis (6) riesgos quedaron ubicados en zona extrema, no presentaron variación después de controles y de los treinta y cinco (35) riesgos inherentes que se encontraban en zona alta, después de controles solo 11 pasaron a zona moderada.

4.4. SEGUIMIENTOS PLANES DE ACCION ASOCIADOS A LOS RIESGOS DE PROCESO

La Oficina de Control Interno procedió a realizar el seguimiento al avance y/o cumplimiento de 104 controles y 30 acciones asociadas a los 80 riesgos de proceso con corte al 30 de junio de

2023. Asimismo, realizó la verificación a través de la información suministrada por los procesos responsables de su ejecución, como resultado de este seguimiento se evidenció lo siguiente:

- Sub Proceso Comunicaciones y medios: No se dio cumplimiento a las siguientes acciones "Actualizar procedimiento CO-PR-06 divulgación de información a través de comunicado de prensa" y "Actualizar manual C0-M-01 MANUAL DE USO DE MEDIOS DE COMUNICACIÓN (NUMERALES DEL 8 AL 9)" teniendo en cuenta que la fecha de cumplimiento establecida era junio de 2023.

Como resultado entonces, del seguimiento y verificación realizada a las 30 acciones que se han implementado para el manejo y control del riesgo, en cada sub procesos de la entidad, se estableció que 29 acciones continúan en curso, por tal razón esta oficina realizara seguimiento en el próximo semestre.

4.4 MATERIALIZACION DE RIESGOS

Producto del seguimiento hecho por la OACI se evidencia que se materializaron 3 riesgos, lo cual se describe a continuación:

- ✓ Al verificar el Indicador 549 Proporción de fallas asociadas a la inadecuada manipulación del equipo a través del software Daruma, se observa incumplimiento a las metas en los meses de marzo, abril, mayo y junio de 2023, este control se encuentra asociado al riesgo "Posibilidad de presentarse Falla en los equipos biomédicos asociados a operación indebida", Con lo anterior se evidencia que el riesgo deja de ser una probabilidad y se convierte en un hecho real. (materialización de este riesgo).

- ✓ La OACI en cumplimiento del Plan anual de auditoria vigencia 2023, realizo seguimiento al tratamiento realizado por la Oficina de Jurídica y por el Sistema de Información y Atención al Usuario (SIAU) de las peticiones, quejas, reclamos, sugerencias, felicitaciones y denuncias (PQRSD) correspondientes al primer semestre de 2023, que se interponen ante la E.S.E Hospital Universitario San Rafael de Tunja, teniendo en cuenta lo anterior se realizó verificación a los archivos físicos y se observó que a 20 derechos de petición se les dio respuesta fuera de lo términos legales establecidos en la ley 1755 de 2015 y la resolución interna 194 de 2018. Con lo anterior se evidencia que el riesgo "Posibilidad de inicio de acciones constitucionales por extemporaneidad en la emisión de respuestas a los derechos de petición conforme a la normatividad vigente" deja de ser una probabilidad y se convierte en un hecho real. (materialización de este riesgo)

- ✓ El proceso GESTIÓN QHSE identifico el riesgo "Posibilidad de no conformidades por la utilización de formatos desactualizados por falta de adherencia a la norma fundamental", con las siguientes causas asociadas (No aplicación de las mecanismos de control establecidos para asegurar la aplicación de formatos actualizados en los procesos

institucionales, Falta de adherencia a la norma fundamental), riesgo y controles identificados sin la intervención y concertación con el líder de procesos y procedimientos.

En la descripción del riesgo, se observa que la causa raíz fue por (Falta de adherencia a la norma fundamental), razón por la cual se puede presentar el riesgo, constituyéndose este como la base para la definición de controles en la etapa de valoración del riesgo, según los establecido en la Guía de administración de riesgos del DAFP V6, se recomienda a la segunda línea de defensa realizar mesas de trabajo con los responsables de este proceso para realizar un adecuado análisis de causas y sus respectivos controles, teniendo en cuenta que como resultado de la Auditoria interna de calidad este riesgo se materializo.

Se recomienda tener en cuenta lo establecido en el Manual de Gestión del riesgo OADS-M-02 ***Si dentro del seguimiento realizado, bien sea por parte de la Oficina de Control Interno o por los líderes de los procesos, se establece que se ha materializado uno o más riesgos, las acciones requeridas son las siguientes:***

DETECTADO POR	ACCIÓN
OFICINA DE CONTROL INTERNO	1. Convocar al Comité de Coordinacion de Control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. 2. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo. 3. Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados. 4. 4. Verificar que se tomaron las acciones y se actualizo el mapa de riesgos.
LÍDER DEL PROCESO U OTRO(S) FUNCIONARIO(S) QUE PARTICIPA(N) O INTERACTÚA(N) CON EL PROCESO	1. Informar a la Alta Direccion sobre el hecho encontrado. 2. De considerarlo necesario, realizar la denuncia ante el ente de control respectivo. 3. Iniciar con las acciones correctivas necesarias. 4. Realizar el analisis de causas y determinar acciones preventivas y de mejora. 5. Analisis y actualizacion del mapa de riesgos.

Una vez materializado un riesgo, el líder del proceso procederá de manera inmediata a aplicar las actividades que permitan dar continuidad del servicio o el restablecimiento del mismo (si es el caso), se debe reportar en el seguimiento trimestral que realiza cada líder de proceso a través del formato OADS-F-36, para lo cual se documenta un plan de Mejora y se ajustaran y/o replantearán los riesgos y/o controles del proceso, para lo cual se debe establecer un plan de acción que permita generar acciones correctivas, preventivas y oportunidades de mejora.

4.6 CORRELACION HALLAZGOS AUDITORIA CONTRALORIA DEPARTAMENTAL / MAPA DE RIESGOS INSTITUCIONAL 2023

Teniendo en cuenta el informe definitivo de la auditoría financiera y de gestión realizada por la contraloría General de Boyacá para la vigencia 2022, se elaboró plan de mejoramiento, en el cual se identificaron 56 hallazgos.

La OACI, confronto lo hallazgos con los riesgos identificados en el mapa de riesgos de la vigencia 2023, producto de esta verificación se observa que es necesario crear nuevos riesgos y fortalecer los controles

Se adjunta Anexo 2 con la correlación de los hallazgos/ mapa de riesgos

4.7 RESULTADO SEGUIMIENTO RIESGOS POR PROCESO

La evaluación específica para cada riesgo y controles se encuentra en la **Matriz de seguimiento "Evaluación del Mapa de riesgos – primer semestre de 2023", archivo que se anexa a este informe.** Por lo cual se invita a los procesos y sub procesos a que realicen la consulta de dichos resultados, a fin que se tomen decisiones sobre el particular y se implementen las mejoras del caso.

Como resultado del seguimiento realizado por la tercera línea a los Riesgos de proceso se evidenció lo siguiente:

- ✓ Los (59) subprocesos realizaron el seguimiento por parte de la primera línea de defensa, de autocontrol con corte al segundo trimestre del 2023, sin embargo, se recuerda a los líderes de proceso que de acuerdo a los lineamientos Acuerdo 015 de 2023 y al Procedimiento de Gestión y Administración de riesgos OADS-PR-11, actividad 15, el autocontrol se debe realizar trimestralmente, ya que no aportan evidencias del monitoreo del primer trimestre.

- ✓ Se evidenció que 3 de los 59 subprocesos reportaron información en formatos desactualizados. (FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS) versión 1

- ✓ Se evidenció que de los 59 sub procesos, solo 3 sub procesos (Direccionamiento estratégico, Gestión contractual y evaluación) entregaron los soportes del FORMATO SEGUIMIENTO Y AUTOCONTROL GESTION DE RIESGOS / PRIMERA LINEA DE DEFENSAS debidamente firmado, evidencias que se convierte en la prueba del conocimiento y la verificación de la integridad y aprobación de la información contenida en un documento por parte de los líderes de proceso.

- ✓ Se evidenció que, de los 80 riesgos identificados, 34 cumplen con la descripción del riesgo de acuerdo a los lineamientos establecidos en numeral 2.5 DESCRIPCION DEL RIESGO de la Guía para la administración del riesgo y el diseño de controles en entidades públicas" Versión 6.

- ✓ Se evidenció que de los 104 controles asociados a los riesgos, 45 cumplen con la descripción del riesgo de acuerdo a los lineamientos establecidos en numeral **3.2.2.1**

Estructura para la descripción del control de la Guía para la administración del riesgo y el diseño de controles en entidades públicas" Versión 6.

- ✓ Incumplimiento actividad 12 del Procedimiento de Gestión y Administración de riesgos OADS-PR-11 "Una vez consolidados Mapas de Riesgo Se presenta en Comité de Gestión y desempeño los Mapas de Riesgo de los procesos aplicables, para su conocimiento y aprobación", esto teniendo en cuenta que el mapa de riesgos de gestión fue publicado sin la debida aprobación.

- ✓ Incumplimiento a lo normado en el artículo cuarto del Acuerdo 015 de 2023, METODOLOGÍA, toda vez que es el documento Manual de gestión del riesgo OADS-M-02, Establece los parámetros para la gestión del riesgo en la E.S.E Hospital Universitario San Rafael de Tunja, asegurando la trazabilidad y seguimiento a los riesgos que puedan afectar el cumplimiento de la misión y objetivos institucionales y a la fecha de la realización de las mesas de trabajo para la identificación y construcción del nuevo mapa de riesgos se encontraba en estado de elaboración.

- ✓ No se evidencio la identificacion de riesgos fiscales, a pesar que se encuentran relacionados en la Política de Gestión de riesgos integral actualizada recientemente mediante Acuerdo 015 de 30 de junio de 2023

- ✓ Se evidenció que los soportes adjuntados por algunos procesos no son suficientes para verificar la aplicación del control, por tal razón se recomienda a la primera y segunda línea de defensa realizar un monitoreo adecuado y dar cumplimiento a las responsabilidades establecidas en la Política de Gestión de riesgos Integral. (Observaciones Anexo 1)

- ✓ Los siguientes procesos: Enfermería, Gestión Quirúrgica, Unidad de cuidados intensivos, Gestión clínica, urgencias, tienen asociados los siguientes riesgos y controles.

RIESGOS	CONTROLES
Posibilidad de incumplimiento de los objetivos misionales y metas debido a la falta de identificación, análisis y seguimiento de indicadores	El líder de la unidad estadística valida el reporte mensualmente y trimestralmente el análisis y los planes de mejora de los indicadores de los procesos
Posibilidad de desviación en la prestación del servicio por la no actualización o ausencia de protocolos, guías, procedimientos, formatos	El profesional de procesos y procedimientos de la oficina de calidad validad mensualmente el estado de los documentos del proceso
	El referente de procesos prioritarios valida la actualización de las guiase de practica clínica de los procesos

Al verificar los responsables de la ejecución de los controles se observa que están asignados a profesionales que pertenecen a la segunda líneas de defensa, lo que permite evidenciar que la primera línea y/o el líder del proceso no cuenta con ninguna

responsabilidad frente a la gestión del riesgos asociado, toda vez que el responsable de una posible materialización seria el líder del proceso y afectaría el cumplimiento de los objetivos y metas del proceso, por tal razón se recomienda identificar controles que permitan verificar la gestión de la primera línea de defensa

SEGUIMIENTOS RIESGOS SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta lo establecido en el Acuerdo 015 de 30 de junio de 2023 "Por medio del cual se adopta la política de gestión de riesgo integral de la Empresa social de Estado Hospital Universitario san Rafael de Tunja" Articulo 5 Responsabilidades… "Monitorear y revisar los riesgo identificados", "Hacer seguimiento a los resultados de las acciones emprendidas para mitigar los riesgos", Realizar informe de seguimiento y monitoreo de la gestión del riesgos acorde a la fechas definidas en el manual".

Adicionalmente el Capítulo 10 EVALUACION. M**ANUAL METODOLÓGICO PARA LA GESTIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN** establece **"**El Hospital universitario San Rafael de Tunja y su equipo "Evaluará el desempeño de la implementación de la metodología para el levantamiento y gestión de riesgos de, los activos de información", por medio de un monitoreo que permite hacer seguimiento de la gestiones que están llevando a cabo y evaluar la eficiencia en su puesta en marcha, adelantando comprobaciones al menos una vez al semestre o cuando la entidad lo considere necesario, comunicando a la alta dirección aquellas situaciones o causas que pueden estar influyendo en la aplicación de las acciones de tratamiento

Teniendo en cuenta lo anterior, la oficina Asesora de Control interno solicitó el 24 de agosto de 2023, por correo electrónico al líder del proceso de Sistemas y Comunicaciones el resultado de monitoreo realizado de riesgos de los activos de información corte primer semestre 2023, información que fue suministrada el día 25 de agosto de 2023.

Al verificar los soportes aportadas por el proceso se evidenció lo siguiente:

- MATRIZ DE RIESGO SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN - MSPI - GOBIERNO DIGITAL E.S.E. HOSPITAL UNIVERSITARIO SAN RAFAEL TUNJA, en formato desactualizado
- Informe ejecutivo presentado a la oficina de control interno, sin las respectivas firmas de quien elaboró y revisó.
- Se logra evidenciar que el informe ejecutivo presentado no contiene el membrete correspondiente a la vigencia 2023, lo cual podría materializar el riesgo "Posibilidad de no conformidades por la utilización de formatos no autorizados por falta de adherencia a la norma fundamental". Lo que afecta la imagen de la entidad lo que se puede observar en la siguiente imagen.

7. CAÍDA TECNOLÓGICA TOTAL O PARCIAL DE SERVICIOS: (CORREO ELECTRONICO, SERVICIOS OUTLOOK, SERVIDORES EN LA NUBE, SISTEMAS DE INFORMACION CLOUD)

En este resigo pueden ocurrir ataques de Malware, de ciberseguridad, daño del sistema operativo y aplicativos, saturación en la red, errores de conectividad, daños físicos y lógicos en la red, licencias obsoletas y perturbaciones en la red eléctrica y alta temperatura en el Datacenter, golpes, movimientos bruscos e inapropiados.

Acciones: Contratos firmados que tiene la institución; proveer los servicios de: 1) canal dedicado mediante modelo MPLS por fibra óptica, con canal simétrico dedicado redundante en anillo con reúso 1:1, incluye administración centralizada, servicio de UTM, filtrado de contenido y administración a los dispositivos y las conexiones de internet a través de equipo firewall de seguridad, proveer los servicios de: 1) hosting 2) correo electrónico corporativo para 320 usuarios con administración.

Evidencias: Carpeta Evidencias Riesgo 2

8. MODIFICACIÓN, ALTERACIÓN, PÉRDIDA TOTAL O PARCIAL DE LA INFORMACIÓN ALMACENADA EN MEDIOS CLOUD

Los riesgos presentes son los Malwares, ataques de ciberseguridad, daños en sistema operativos y aplicativos, accesos no autorizados, roles ni permisos definidos, contraseñas débiles, equipos desatendidos, borrados accidental, saturación de medios de almacenamiento y no contra con copias de seguridad o Backup.

Acciones: Contratos firmados que tiene la institución; IMPLEMENTACIÓN Y DESPLIEGUE DE LA TRANSICIÓN DE IPV4 A IPV6, y contrato de mantenimiento de redes

Fuente. Informe seguridad de la información-primer semestre 2023

La oficina de control interno realizo seguimiento a la aplicación de los controles establecidos en el mapa de riesgos de seguridad de la información, verificando las evidencias aportadas para cada uno de los controles dejando las respectivas recomendaciones las cuales se adjuntan en el anexo 3.

CONCLUSIONES Y RECOMENDACIONES

- Se genera una alerta a la Alta Dirección, con respecto a la materialización en la actualidad de 3 riesgos, e igual manera se recomienda para que desde la segunda línea, se apoye a los líderes de proceso en la elaboración del respectivo plan de Mejora y se ajusten y/o replanteen los riesgos y/o controles del proceso, para lo cual se debe establecer un plan de acción que permita generar acciones correctivas, preventivas y oportunidades de mejora dando cumplimiento a lo establecido en el Manual de Gestión del riesgo OADS-M-02

- Reitera esta oficina de control interno, que es necesario fortalecer la cultura del reporte de cambio o materialización de los riesgos, con el fin de tomar correctivos oportunos e iniciar acciones frente a las desviaciones producto de la aplicación de los controles. Para esto se requiere que los líderes y grupos de trabajo conozcan el proceder frente a la materialización de los riesgos. Por lo tanto, se recomienda que la segunda línea en los monitoreos o en la estructuración de los mapas de riesgos, capaciten sobre la ocurrencia de estos hechos y brinde la asesoría necesaria. En la medida que se reporten la materialización de los riesgos, se pueden tomar decisiones oportunas y efectivas frente a los controles.

- De acuerdo al significativo número de riesgos y controles que no cumplen con el diseño y estructura de acuerdo a lo establecido en **Guía para la administración del riesgo y el diseño de controles en entidades públicas" Versión 6**, es necesario que los subprocesos soliciten acompañamiento de la segunda línea de defensa para mejorar en la implementación de la metodología adoptada por la entidad. Una vez sea culminada esta etapa se solicita a esta oficina actualizar y publicar el mapa de riesgos nuevamente.

- Se reitera la observación, realizada en el informe SEGUIMIENTO DE MAPAS DE RIESGOS DE CORRUPCION, OPACIDAD Y FRAUDE PRIMER CUATRIMESTRE 2023, al proceso Gestión contractual, respecto a "Se recomienda al líder del proceso de contratación actualizar los formatos C-F-27 Y C-F-28 Estudios de conveniencia de prestación de servicios y ECO Requerimientos, subasta inversa o convocatoria pública, respectivamente ya que al consultarlos en DARUMA ,se observa que en la parte de la firma de gerente aparece el nombre del anterior ordenador del gasto.

- Los responsables de los controles de los riesgos deben entender su compromiso con el proceso, la tarea no es solo cargar archivos, sino garantizar que la información sea la que corresponda.

- Se recomienda a los líderes de proceso recordar que la utilización de documentos y formatos no vigentes ocasionado una no conformidad dentro del sistema de Gestión de Calidad, y un reproceso en el desarrollo de las diferentes actividades de los servicios.

- Conforme al seguimiento realizado, se concluye un incumplimiento la Política de Gestión de riesgos integral de la entidad, la cual no está siendo implementada como ha sido definida, específicamente en lo establecido en el artículo 4 METODOLOGÍA el cual se articula con los parámetros de MIPG – la guía de administración del riesgo y el diseño de controles, lo que genera incumplimiento de la normatividad interna, poniendo en riesgos los objetivos del HUSRT.

- Se recomienda a la segunda línea de defensa (Gestión del riesgo), actualizar las herramientas para la administración del riesgo como son el procedimiento y el manual, alineándolas con lo establecido en la Política de Gestión de riesgos integral de la entidad actualizada recientemente, documentos que establecen los parámetros que permiten administrar los riesgos de forma integral

- Se recomienda realizar el respectivo monitoreo en donde se verifique la aplicación de los controles, adelantando comprobaciones al menos una vez al semestre, evidenciando y comunicando constantemente a la alta gerencia aquellas situaciones o causas que pueden estar influyendo en la aplicación de las acciones del tratamiento, según lo establecido en el manual de gestión del riesgo código OADS-M-02en su numeral 8.4.4

- Se recomienda a la segunda línea de defensa tener en cuenta, las observaciones descritas en el Anexo 2 CORRELACION HALLAZGOS AUDITORIA CONTRALORIA/MAPA DE RIESGOS, con el fin de apoyar y dar cumplimiento al plan de mejoramiento suscrito con este ente de control.

- Se recomienda a la segunda línea de defensa «Gestión del riesgo», establecer fecha de entrega del monitoreo por parte de esta línea, teniendo en cuenta que, para el caso del seguimiento de este semestre, la demora de la entrega del monitoreo afecto la planeación y ejecución de las actividades de la oficina de control interno.

- Teniendo en cuenta la medición de índice de desempeño institucional vigencia 2022, la cual fue reportada en julio del 2023, en el componente Política de control interno se encuentra la siguiente pregunta:

«Acorde con lo establecido en la política de administración del riesgo en el marco del esquema de líneas de defensa, se tienen identificadas las instancias responsables del seguimiento y monitoreo a la gestión del riesgo institucional así:

•La alta dirección o el comité institucional de coordinación de control interno como línea estratégica, encargados de monitorear y analizar eventos y riesgos críticos
•Los líderes de los planes, programas o proyectos, como primera línea de defensa, encargados de implementar los controles identificados para mitigar los riesgos a los mismos

•Oficina de planeación o quien haga sus veces como instancia de 2a línea de defensa, encargada de consolidar la gestión del riesgo y llevar ante la Línea Estratégica alertas sobre eventos y cambios en el entorno

- Oficial de seguridad de la información o quien haga sus veces, como instancia de 2a línea de defensa, encargado de evaluar en cumplimiento de los controles asociados a las Políticas de Seguridad de la Información
- El jefe administrativo o secretario general o quien haga sus veces, como instancia de 2a línea de defensa encargado de monitorear la gestión contractual y generar alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas
- El jefe de talento humano o quien haga sus veces encargado, como instancia de 2a línea de defensa encargado de monitorear temas clave del ciclo del servidor (capacitación, bienestar, incentivos, convivencia laboral, código integridad), generando alertas sobre incumplimientos, situaciones críticas que afectan en clima laboral y posibles afectaciones al código de integridad
- El jefe de tecnología o quien haga sus veces, como instancia de 2a línea de defensa encargado de monitorear en Plan Estratégico de Tecnologías de la Información - PETI, generando sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas en materia de tecnología
- El jefe de jurídica, asesor, coordinador o quien haga sus veces, como instancia de 2a línea de defensa encargado de monitorear la gestión jurídica, generando alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas en esta materia
- Otras instancias de 2a línea identificadas de alta o media gerencia como secretarios de despacho, subdirectores, directores técnicos, coordinadores, gerentes de proyectos u otros que lideran temas misionales (programas y proyectos de alto impacto presupuestas y reputacional), encargados de monitorear aspectos estructurales de los temas bajo su gestión, generando alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas acorde con las materias a su cargo
- El jefe de control interno o quien hace sus veces, como como instancia de 3a línea de defensa, encargada de suministrar alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas, a partir de sus seguimientos y procesos de auditoría interna».

De acuerdo a lo anterior es importante que se revise este tema por la segunda línea de defensa (Gestión del Riesgo) y se estudie la posibilidad de incluir los responsables que no se encuentran en la actual política y se establezcan las responsabilidades según su rol.

Hace parte integral de este informe, Anexo 1: Matriz de seguimiento Evaluación del Mapa de riesgos – primer semestre de 2023, Anexo 2 Excel Correlación hallazgos contraloría/ mapa de riesgos institucional y Anexo 3 Seguimiento aplicación controles riesgos seguridad de la información HUSRT, **documento** en donde se registran las observaciones y recomendaciones para cada uno de los riesgos y sus controles. Algunas de las observaciones se encuentran en el presente informe porque se consideraron relevantes, pero la mayoría se deben consultar en la respectiva matriz.

Dado lo anterior, y basados en el rol de enfoque a la prevención, la Oficina de Control Interno de Gestión debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva, por lo que se sugiere a la segunda línea, realizar mesas de trabajo con los procesos que a la fecha presentan debilidades en la gestión de riesgos, buscando mecanismos que faciliten el cumplimiento, y de esta forma evitar la materialización de riesgos por falta de gestión en sus controles.

Anexo 1: Matriz de seguimiento "Evaluación del Mapa de riesgos – primer semestre de 2023"

Anexo 2: Excel Correlación hallazgos contraloría/ mapa de riesgos institucional

Anexo 3 Seguimiento aplicación controles riesgos seguridad de la información HUSRT

ORIGINAL FIRMADO

DIANA LIZBETH VARGAS GONZÁLEZ
Asesora de Control Interno
ESE Hospital Universitario San Rafael de Tunja

Proyectó: Claudia S. Sáenz Jiménez
Profesional especializado OACI