Bogotá D.C, Marzo 28 de 2025

Ingeniero
LUIS AUGUSTO OLAYA PALACIOS
Subdirector de Sistemas
E.S.E. HOSPITAL UNIVERSITARIO DE LA SAMARITANA
E. S. D

Asunto: Informe Auditoria Verificación de cumplimiento y Normas en materia de Derechos de Autor sobre Software 2024

Cordial saludo,

Adjunto envío Informe de Auditoría del tema del asunto para su conocimiento y fines pertinentes a que haya lugar.

Se envía el Informe de Auditoría de la referencia para que dentro de los cinco (5) días hábiles siguientes se elabore Plan de Mejoramiento pertinente a las recomendaciones que lo requieran, el cual deberá ser elaborado según lo establecido en el Procedimiento identificado con Código 02CIN01-V2, Actividad 21 y al Instructivo "Lineamiento Oportunidades de Mejora", Código 06GIC03-V2.

Nota: Anexo veinticinco (25) Folios

Atentamente,

YETICA JHASVELLI HERNANDEZ ARIZA
Jefe de Control Interno

CC. JORGE ANDRES LOPEZ QUINTERO- Gerente
GUSTAVO AXEL VARGAS GALINDO- Directo Científico
YANET CRISTINA GIL ZAPATA- Directora Financiera
EDGAR HUMBERTO RODRIGUEZ B. - Jefe Oficina Asesora Jurídica (E),
CARLOS FERNANDO GONZALEZ PRADA -Director Administrativo
LEONARDO DUARTE DIAZ -Proceso Gestión Integrada de la Calidad
NUBIA DEL CARMEN GUERRERO PRECIADO - Directora Proceso Atención al Usuario, Familia y Comunidad

Aprobó: Yetica Jhasvelli Hernández Ariza
Elaboro: Claudia Yamile Rubiano
Reviso: Claudia Yamile Rubiano

EMPRESA SOCIAL DEL ESTADO HOSPITAL UNIVERSITARIO DE LA SAMARITANA

Nit.899999032-5

INFORME PRELIMINAR DE VERIFICACIÓN DE CUMPLIMIENTO DE LAS NORMAS EN MATERIA DE DERECHOS DE AUTOR RELACIONADA CON EL SOFTWARE VIGENCIA 2024

BOGOTÁ D.C, FEBRERO 2025

INDICE

1. Aspectos Generales

1.1. Objetivos de la auditoría

1.1.1. Objetivo General

Verificar el cumplimiento de la normatividad establecida en cuanto a la protección de Derechos de Autor sobre el uso del SOFTWARE en la Empresa Social del Estado Hospital Universitario de la Samaritana vigencia 2024.

1.1.2. Objetivos Específicos

Verificar el cumplimiento de la normatividad vigente en materia de derechos de autor sobre el uso de software en la Empresa Social del Estado Hospital Universitario de la Samaritana durante la vigencia 2024, a través del análisis de la información suministrada por la Subdirección de Sistemas y la información encontrada en el aplicativo ALMERA, con el fin de identificar posibles brechas, formular recomendaciones y garantizar el adecuado licenciamiento del software conforme a las disposiciones legales y directrices establecidas.

1.2. Alcance de la auditoría

Inventario de Propiedad Intelectual: Identificar y catalogar todas las obras protegidas por derechos de autor, como textos, imágenes, software, videos, música, entre otros.

Revisión de Licencias: Evaluar si todos los derechos de autor de terceros están cubiertos por licencias válidas y si las condiciones de uso se cumplen correctamente.

Cumplimiento Interno: Analizar los procedimientos internos para asegurar que la organización respeta las leyes de derechos de autor, incluyendo el uso de materiales protegidos.

Protección de Derechos Propios: Verificar si las obras propias de la organización están debidamente registradas, protegidas y monitoreadas para prevenir el uso no autorizado.

Evaluación de Riesgos Legales: Identificar posibles infracciones de derechos de autor, tanto realizadas por la organización como de las que podría ser víctima.

Políticas y Educación: Proponer políticas internas y programas de capacitación para asegurar el cumplimiento de las normativas y promover prácticas responsables.

1.3. Metodología de la auditoría

Con el memorando N.04 de 22 de enero de 2025 se da inicio a la Verificación de Cumplimiento y Normas en Materia de Derechos de Autor Sobre Software 2024. Mediante oficio radicado y enviado por medio de correo electrónico a la Subdirección de Sistemas se solicitó la información correspondiente a la verificación de cumplimiento de las normas en materia de derechos de autor, relacionada con software de la vigencia 2024.

1.4. Base legal de la auditoría

- Constitución Política
- Ley 87 de 1993
- Ley 603 de 2000
- Directiva Presidencial No.02 – Febrero de 2002
- Circular No.04 – Diciembre de 2006
- Circular Externa No.12 – Febrero de 2007
- Ley 1266 de 2008
- Ley 1273 de 2009
- Ley 1474 de 2011
- Circular Externa No. 017 – Junio de 2011
- Ley 1581 de 2012
- Ley 1712 de 2014
- Decreto 1078 de 2015
- Decreto 1499 de 2017
- Ley 1915 de 2018
- Decreto 1008 del 14 de junio de 2018
- Guía para la administración del riesgo y el diseño de controles en entidades publicas
- Norma ISO 27001

1.5. Objetivos estratégicos asociados a la auditoría

Es importante destacar que esta auditoría, al evaluar el año 2024, se alinea con los objetivos estratégicos establecidos en el Acuerdo No. 027 de 2022 de la E.S.E. Hospital Universitario de la Samaritana. Dicho acuerdo aprueba la Nueva Plataforma Estratégica 2021-2024, el Mapa de Procesos y el Modelo de Atención de la entidad, definiendo ocho (8) objetivos estratégicos.

En este contexto, los objetivos estratégicos que guardan relación con la auditoría son:

Objetivo Estratégico No. 5 "Alcanzar niveles de excelencia en los procesos organizacionales que redunden en la gestión clínica y administrativa a través de un sistema de gestión integral de calidad para mejorar la prestación de los servicios"

Objetivo Estratégico No. 7 "Consolidar las competencias del talento humano tendiente a fortalecer el crecimiento personal y laboral que propenda por el desarrollo y las satisfacción de los colaboradores en el cumplimiento de los propósitos organizacionales"

Objetivo Estratégico No. 8 "Modernizar la infraestructura física y tecnológica institucional para la adecuada prestación de los servicios humanizados y seguros"

La auditoría sobre derechos de autor en software se alinea con los objetivos estratégicos, fortaleciendo la excelencia organizacional (Objetivo Estratégico No. 5) mediante el cumplimiento normativo, apoyando la modernización tecnológica (Objetivo Estratégico No. 8) con software legal y seguro, y promoviendo la capacitación del talento humano (Objetivo Estratégico No. 7) para el uso adecuado de herramientas tecnológicas.

1.6. Políticas asociadas a la auditoría

En la E.S.E. Hospital Universitario de la Samaritana, se cuenta con una política asociada a la auditoría mencionada, la cual establece:

Política de Gestión de la Información y Comunicación (Código 01DE12-V1, aprobada en enero de 2018), establece el compromiso del hospital de desarrollar procesos confiables y adecuados para la generación,

análisis y archivo de la información. Esto permite una toma de decisiones oportuna y coherente con las metas institucionales, promoviendo una cultura de comunicación transparente y veraz hacia los diferentes grupos de interés a través de los medios disponibles. Esta política tiene tres (3) objetivos, de los cuales dos (2) se alinean directamente con la presente auditoría:

- ✓ Garantizar un sistema de información integral, eficiente y eficaz.
- ✓ Implementar, desarrollar y mantener una plataforma tecnológica de hardware y software que contribuya a la captura, confidencialidad y generación de datos confiables para la toma de decisiones.
- ✓ Establecer las directrices generales para el manejo efectivo de la comunicación interna y externa, asociado a todos los procesos.

Se recomienda actualizar la política mencionada, considerando que la revisión debió realizarse el 31 de enero de 2022, según lo establecido en su vigencia de cuatro años a partir de la fecha de elaboración.

1.7. Riesgos identificados por los procesos

Se procedió a revisar la Matriz de Riesgos 2024 V2 (con ruta de acceso en la Página Web: Transparencia y Acceso a la Información – Planeación Gestión y Control – Planes Programas y Proyectos – Plan Anticorrupción y Atención al Ciudadano 2024 – Matriz Riesgo 2024 V2), matriz vigente a la fecha del presente informe de auditoría en la cual se identificaron los siguientes riesgo asociados a la auditoria:

Código	Riesgo	Causas	Consecuencias	Zona de Riesgos (Absoluto / Residual)
GIS22034	Posibilidad de afectación reputacional y económica por pérdida de información de los sistemas críticos de la HUS y sus sedes, debido al inadecuado manejo de los sistemas de información, posibles ataques cibernéticos y falta de adherencia a los procesos y procedimientos.	Inadecuado manejo de los sistemas de información Posibles ataques cibernéticos Falta de adherencia a los procesos y procedimientos.	Pérdidas Económicas **Formas de materialización:** PQRSD de clientes internos o externos no satisfecha de solicitud de información y documentación demandas o sanciones no satisfecha de solicitud de información y documentación de usuarios o entes de control	Extremo / Extremo
GIS24075	Posibilidad de afectación Económica y Reputacional por alteración de la seguridad y confidencialidad de la información, debido a acceso no controlado a información confidencial.	Acceso no controlado a información confidencial.	Demandas, sanción, investigación, intervención **Formas de materialización:** PQRSD o demanda por publicación de información confidencial	Alto / Alto
GIS22018	Posibilidad de recibir o solicitar dadiva o beneficio a nombre propio o de terceros con el fin de facilitar el acceso indebido de la información contenida en los sistemas	Los funcionarios al retirarse no realizan la inactivación de usuarios Los líderes de proceso no informan oportunamente el retiro del personal Manejo inadecuado de contraseñas Uso inadecuado de dispositivos USB	Pérdida de imagen / credibilidad / Confianza / clientes, usuarios insatisfechos Perdidas económicas **Formas de materialización:** Violación a información institucional confidencial (difusión de información a terceros) Demanda o PQRS relacionada con vulnerabilidad de la información	Externo / Externo

Así como el Mapa de Riesgos SICOF CORRUPCIÓN OPACIDAD Y FRAUDE 2025 (con ruta de acceso desde la página web: Transparencia y Acceso a la Información – Planeación Gestión y Control – Planes Programas y Proyectos – Plan Anticorrupción y Atención al Ciudadano – Programa de Transparencia y Ética Pública 2025 - RIESGOS SICOF 2025 V1), matriz vigente a la fecha del presente informe de auditoría en la cual se identificó el siguiente riesgo asociado a la auditoria:

Número	Riesgo	Causas	Consecuencias	Zona de Riesgos (Absoluto / Residual)
10	Posibilidad de recibir o solicitar dadiva o beneficio a nombre propio o de terceros con el fin de facilitar el acceso indebido de la información contenida en los sistemas	Los funcionarios al retirarse no realizan la inactivación de usuarios Los líderes de proceso no informan oportunamente el retiro del personal Manejo inadecuado de contraseñas Uso inadecuado de dispositivos USB	Pérdida de imagen / credibilidad / confianza/ clientes, usuarios insatisfechos / Perdidas económicas /	Extremo / Extremo

1.8. Indicadores del proceso auditado

Los indicadores que se relacionan con el objetivo y alcance de la auditoría sobre la protección de Derechos de Autor en el uso del software en la ESE Hospital Universitario de la Samaritana son:

- ✓ **Indicador 971**: **Porcentaje de cumplimiento en la realización de Backups programados:** Relacionado con la seguridad de la información y la protección de datos, aspectos clave en la gestión del software.
- ✓ **Indicador 972**: **Porcentaje de ataques informáticos que afectan el sistema de información:** Vinculado a la seguridad del software y la integridad de los sistemas, lo cual es un factor clave en el cumplimiento normativo.
- ✓ **Indicador 973**: **Porcentaje de tiempo disponible del sistema de información:** Relacionado con la estabilidad y correcta gestión del software utilizado en la entidad.
- ✓ **Indicador 1020**: **Porcentaje de cumplimiento de mantenimiento preventivo de equipos de cómputo:** Aunque se enfoca en hardware, el mantenimiento adecuado puede incluir actualizaciones y licenciamiento de software.

Estos indicadores permiten evaluar aspectos de seguridad, cumplimiento normativo y gestión del software dentro de la entidad, alineándose con la auditoría enfocada en derechos de autor y licenciamiento. A continuación se detallan:

1.8.1. Porcentaje de cumplimiento en la realización de Backups programados

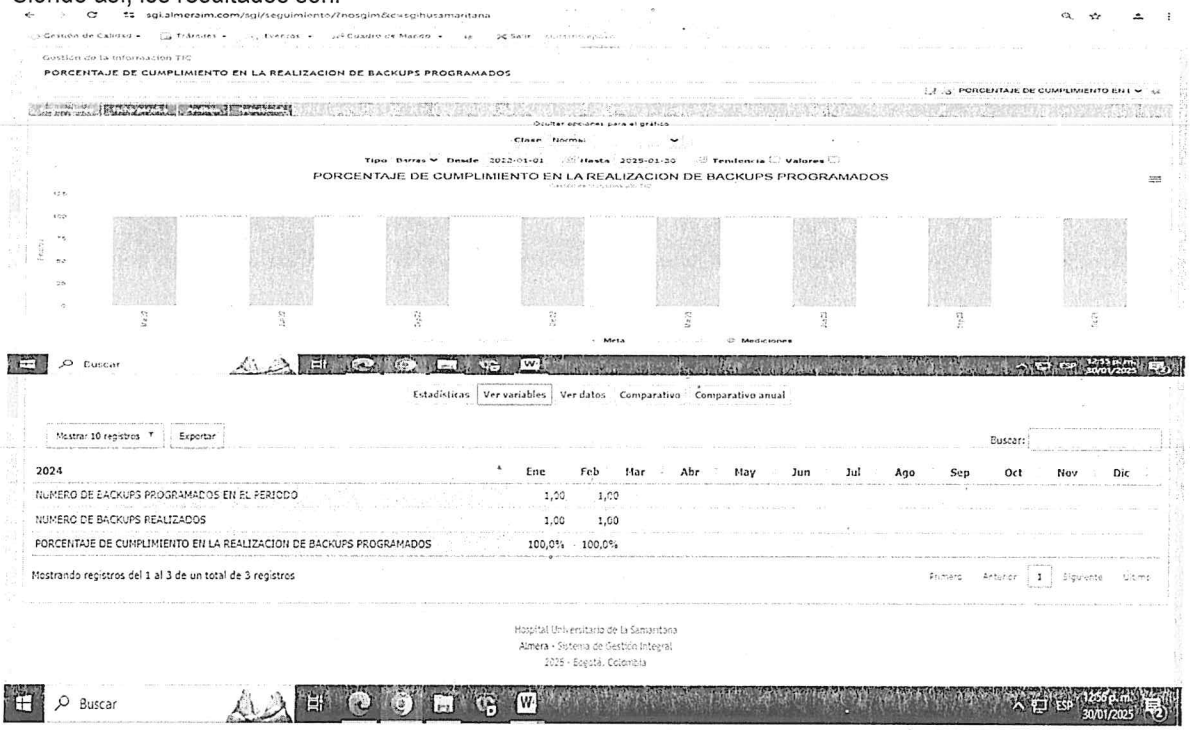
En el Sistema de Gestión Integral "ALMERA", se llevó a cabo una verificación de indicadores, encontrando en el proceso de Gestión de la Información TIC, el indicador identificado con el código 971, denominado "Porcentaje de Cumplimiento en la Realización de Backups Programados". A continuación, se detalla su composición, y las imágenes muestran la evolución del indicador en la tabla, junto con su correspondiente gráfica.

1.8.1.1. Composición del indicador

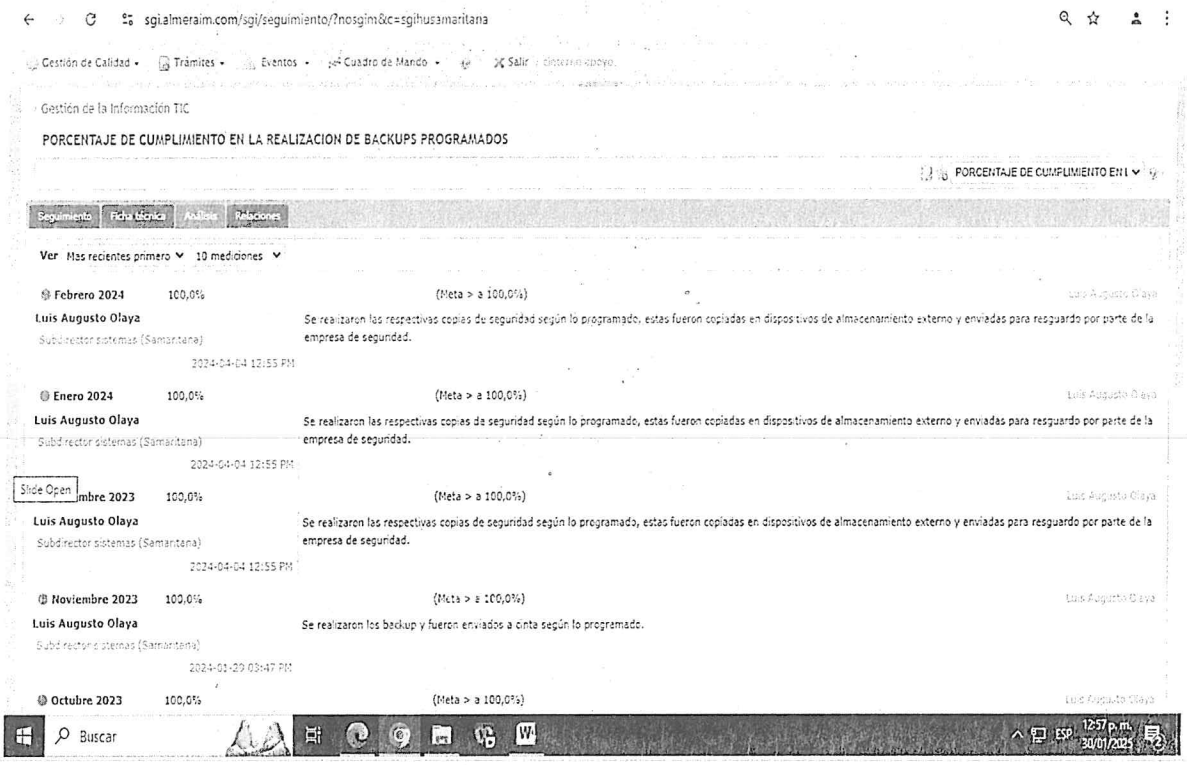
Frecuencia	Mensual
Objetivo Institucional	Sistema de información
Variables	1. Numero de Backups realizados
	2. Numero de Backups programados en el periodo
Fórmula	$\left(\frac{Numero\ de\ Backups\ realizados}{Numero\ de\ Backups\ programados\ en\ el\ periodo}\right) * 100$

1.8.1.2. Resultados del indicador

Siendo así, los resultados son:



Este indicador de gestión de la información TIC, medido mensualmente, no ha sido actualizado en el aplicativo "ALMERA" desde febrero de 2024. Del mismo modo, el análisis tampoco ha sido actualizado. Se recomienda registrar la información correspondiente, incluso si el valor del período es 0, para garantizar la trazabilidad y precisión de los datos.



1.8.2. Porcentaje de ataques informáticos que afectan el sistema de información

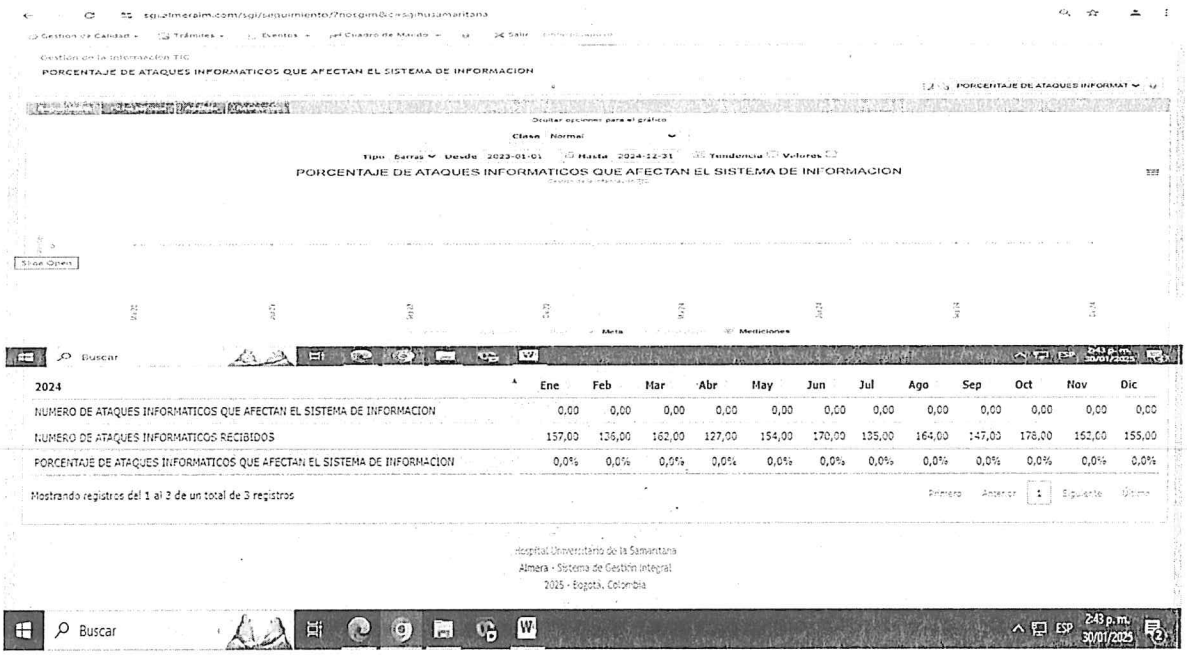
En el Sistema de Gestión Integral "ALMERA", se llevó a cabo una verificación de indicadores, encontrando en el proceso de Gestión de la Información TIC, el indicador identificado con el código 972, denominado "Porcentaje de ataques informáticos que afectan el sistema de información". A continuación, se detalla su composición, y las imágenes muestran la evolución del indicador en la tabla, junto con su correspondiente gráfica.

1.8.2.1. Composición del indicador

Frecuencia	Mensual
Objetivo Institucional	Sistema de información
Variables	1. Número de ataques informáticos que afectan el sistema de información
	2. Número de ataques informáticos recibidos
Formula	$\left(\frac{Numero\ de\ ataques\ informaticos\ que\ afectan\ el\ sistema\ de\ información}{Numero\ de\ ataques\ informaticos\ recibidos}\right) * 100$

1.8.2.2. Resultado del Indicador

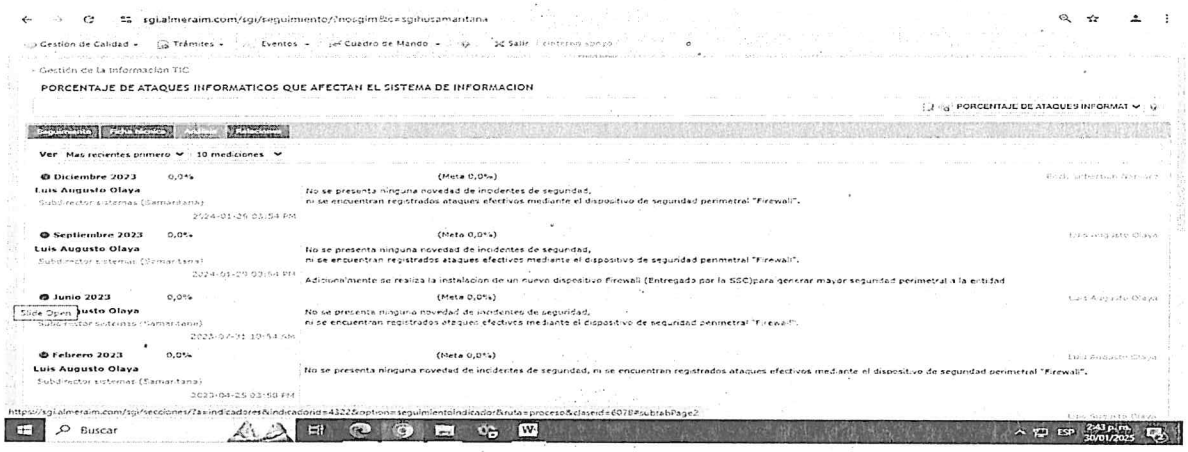
Siendo así, los resultados son:



2024	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
NUMERO DE ATAQUES INFORMATICOS QUE AFECTAN EL SISTEMA DE INFORMACION	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
NUMERO DE ATAQUES INFORMATICOS RECIBIDOS	157,00	136,00	162,00	127,00	154,00	170,00	135,00	164,00	147,00	178,00	162,00	155,00
PORCENTAJE DE ATAQUES INFORMATICOS QUE AFECTAN EL SISTEMA DE INFORMACION	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%

Mostrando registros del 1 al 3 de un total de 3 registros

Estê indicador de gestión de la información TIC, medido mensualmente, aunque aparece actualizado en la gráfica y los datos, no ha sido analizado desde diciembre de 2023. Se recomienda realizar el análisis correspondiente de manera mensual para garantizar un seguimiento adecuado y oportuno.



1.8.3. Porcentaje de tiempo disponible del sistema de información

En el Sistema de Gestión Integral "ALMERA", se llevó a cabo una verificación de indicadores, encontrando en el proceso de Gestión de la Información TIC, el indicador identificado con el código 973, denominado "Porcentaje de tiempo disponible del sistema de información". A continuación, se detalla su composición, y las imágenes muestran la evolución del indicador en la tabla, junto con su correspondiente gráfica.

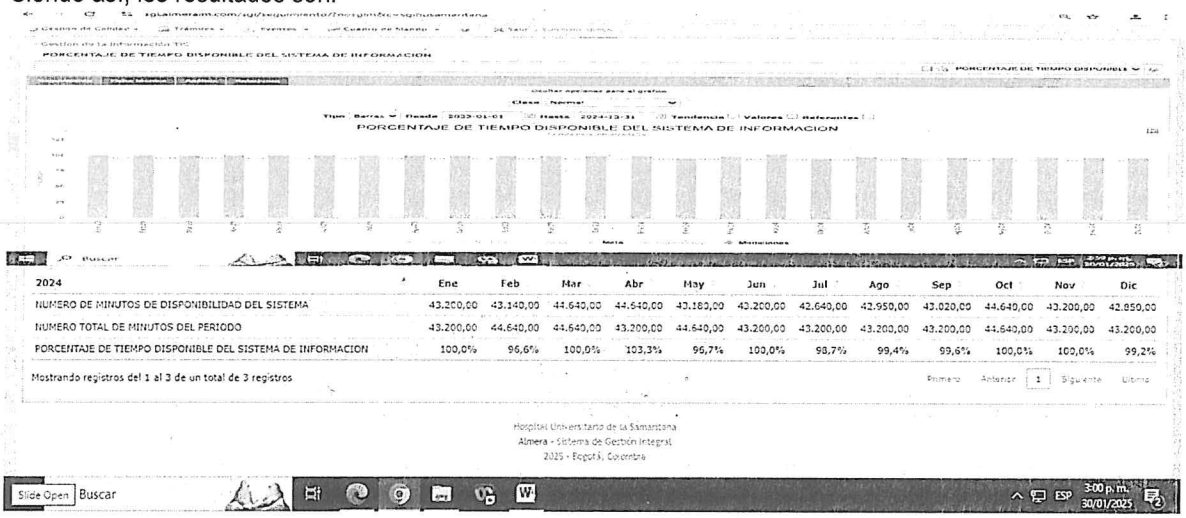
1.8.3.1. Composición del indicador

Frecuencia	Mensual
Objetivo Institucional	Sistema de información

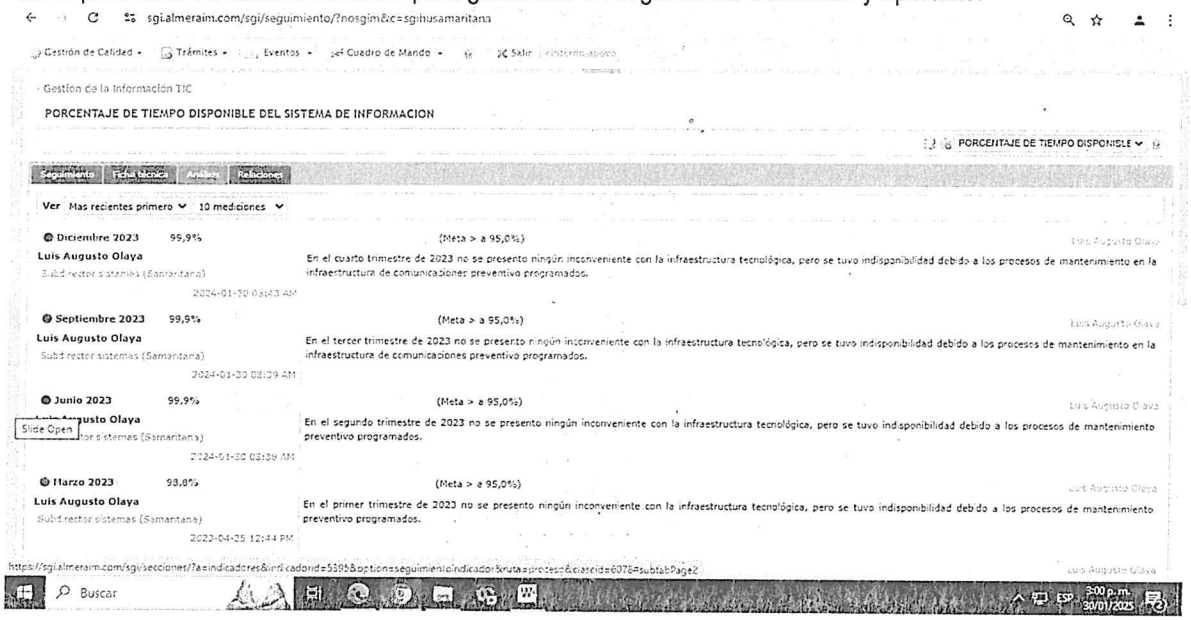
Variables	1. Numero de Backups realizados 2. Numero de Backups programados en el periodo
Formula	$(\frac{Numero\ de\ Backups\ realizados}{Numero\ de\ Backups\ programados\ en\ el\ periodo}) * 100$

1.8.3.2. Resultados del indicador

Siendo así, los resultados son:



Este indicador de gestión de la información TIC, medido mensualmente, aunque aparece actualizado en la gráfica y los datos, no ha sido analizado desde diciembre de 2023. Se recomienda realizar el análisis correspondiente de manera mensual para garantizar un seguimiento adecuado y oportuno.



1.8.4. Porcentaje de cumplimiento preventivo de equipos de cómputo

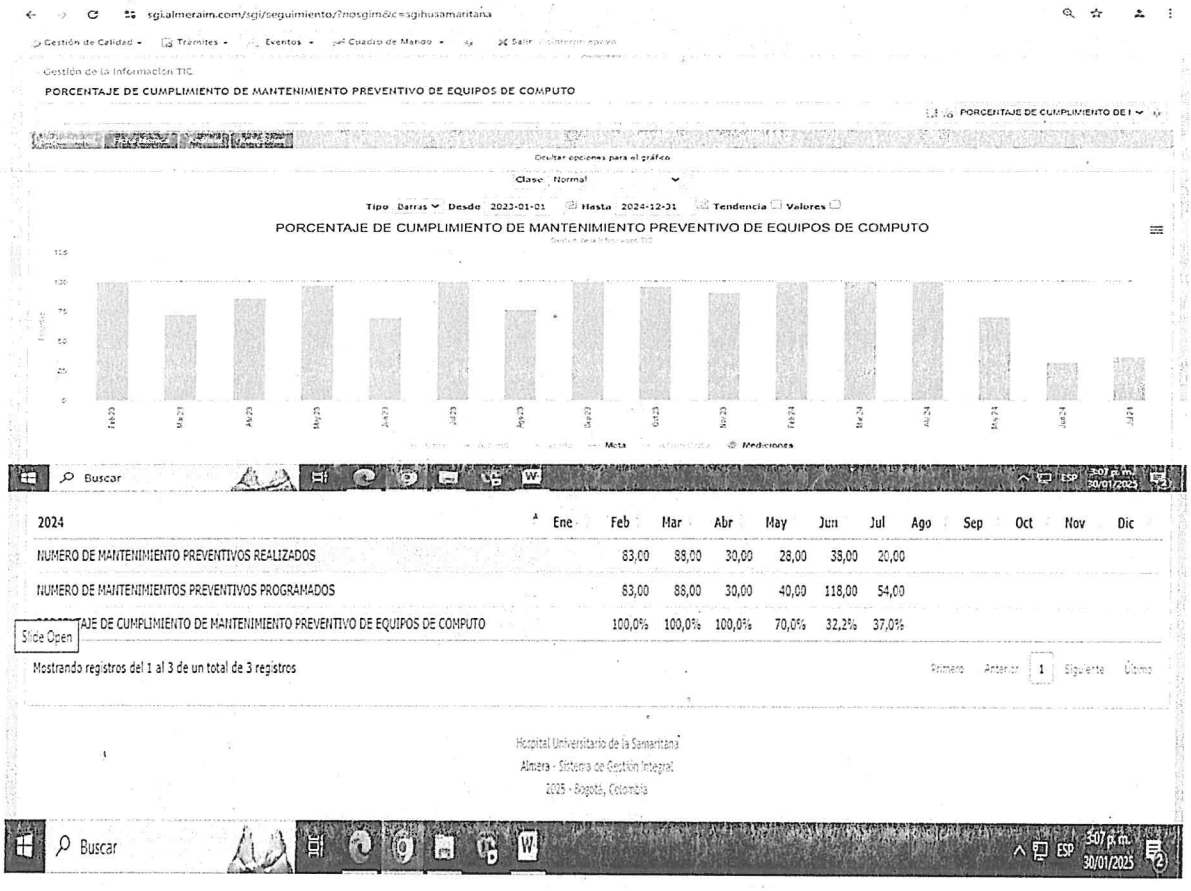
En el Sistema de Gestión Integral "ALMERA", se llevó a cabo una verificación de indicadores, encontrando en el proceso de Gestión de la Información TIC, el indicador identificado con el código 1020, denominado "Porcentaje de cumplimiento de mantenimiento preventivo de equipos de cómputo". A continuación, se detalla su composición, y las imágenes muestran la evolución del indicador en la tabla, junto con su correspondiente gráfica.

1.8.4.1. Composición del indicador

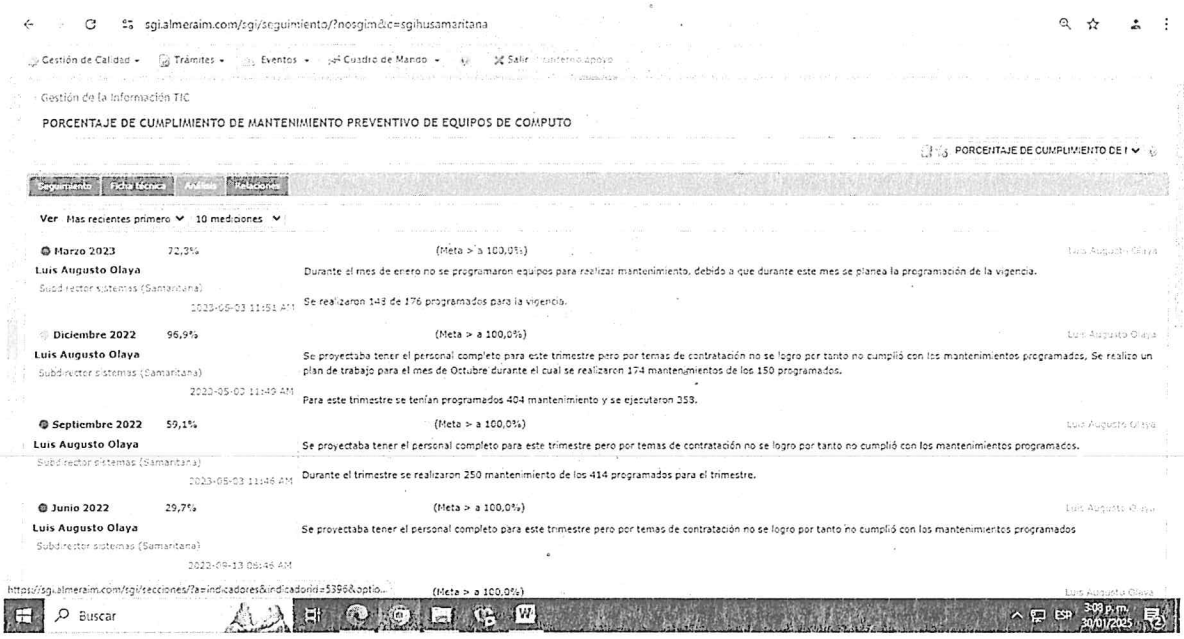
Frecuencia	Mensual
Objetivo Institucional	Sistema de información
Variables	1. Número de mantenimiento preventivos realizados
	2. Número de mantenimiento preventivos programados
Formula	$\left(\frac{Numero\ de\ mantenimiento\ preventivos\ realizados}{Numero\ de\ mantenimiento\ preventivos\ programados}\right) * 100$

1.8.4.2. Resultados del indicador

Siendo así, los resultados son:



Este indicador de gestión de la información TIC, medido mensualmente, no ha sido actualizado en el aplicativo "ALMERA" desde julio de 2024. Del mismo modo, el análisis tampoco ha sido actualizado desde marzo de 2023. Se recomienda registrar la información correspondiente.



1.9. Estándares de acreditación asociados a la auditoría

Según el Manual de Acreditación en Salud Ambulatorio y Hospitalario en Colombia Versión 3.1, los estándares de acreditación asociados con la auditoría de Verificación de Cumplimiento de las Normas en Materia de Derechos de Autor relacionada con el Software son:

1.9.1. Estándar 133. Código: (GT2)

La organización cuenta con una política organizacional definida, implementada y evaluada para adquisición, incorporación, monitorización, control y reposición de la tecnología. Incluye:

Criterios:

- ✓ La evidencia de seguridad.
- ✓ Evaluación de la confiabilidad, incluyendo el análisis de las fallas y eventos adversos reportados por otros compradores.
- ✓ La definición del tiempo de vida útil de la tecnología.
- ✓ La garantía ofrecida.
- ✓ Las condiciones de seguridad para su uso.
- ✓ Los manuales traducidos y la información necesaria para garantizar el uso óptimo de la tecnología.
- ✓ El soporte, incluidos el tipo de soporte y el tiempo que se garantiza (repuestos, software y actualizaciones, entre otros).
- ✓ Las necesidades e intervalos de mantenimiento.
- ✓ Las alternativas disponibles.
- ✓ Las proyecciones de nuevas necesidades.
- ✓ La validación por personal capacitado para comprobar que cumple con las especificaciones técnicas, está completa y funciona en forma correcta.
- ✓ Evaluación de costo beneficio, utilidad y costo efectividad de la tecnología.

1.10. Componentes y elementos del MECI

Es importante recordar que la articulación entre los dos sistemas se establece a partir del Modelo Integrado de Planeación y Gestión (MIPG), en el cual el Modelo Estándar de Control Interno (MECI) se integra como la séptima dimensión. Dentro de esta integración, se destacan objetivos clave de control interno que son indispensables para la realización de auditorías, como en el caso de la auditoría de Verificación de Cumplimiento de las Normas en Materia de Derechos de Autor relacionada con el Software. Estos objetivos incluyen:

- ✓ Obtener información correcta, segura y oportuna.
- ✓ Proteger los recursos de la entidad.
- ✓ Procurar eficiencia en las operaciones.
- ✓ Prevenir errores, irregularidades o detectar oportunamente los mismos.

La correcta articulación entre el MIPG y el MECI no solo fortalece la capacidad de la entidad para cumplir con sus objetivos, sino que también asegura que las auditorías, sino que también permite a la E.S.E. Hospital Universitario de la Samaritana cumplir con sus obligaciones normativas y operativas de manera eficiente y segura.

1.11. Encuesta Pre – Saberes

Mediante el comunicado con consecutivo Orfeo CI2025500000240, fechado el 17 de marzo de 2025, y a través de un correo electrónico enviado el mismo día, se compartió la encuesta titulada "DERECHOS DE AUTOR - Vigencia 2024". Dicha encuesta fue aplicada durante una reunión remota llevada a cabo el 18 de marzo de 2025, de 10:00 a.m. a 11:00 a.m., a través del enlace: *https://meet.google.com/vtm-aayr-xtn.* Se citaron a diecinueve (22) responsables de todos los procesos. De los cuales dieciocho (19) diligenciaron la encuesta, lo que resultó en que el 86,36% de los procesos socializados completaran la encuesta.

Los responsables del proceso, que representan el 13,63% de los participantes socializados y no respondió a las preguntas de la encuesta, fueron los siguientes:

	RESPONSABLE DE PROCESO NO PRESENTARON ENCUESTA
1	Néstor Andrés Rodríguez Ordoñez – Gestor asistencial HR
2	Adriana Vanessa Caballero Hernández – Coordinadora de apoyo HR
3	Gabriel Ángel Ramírez – Proceso de bienes y servicios

Realizando el análisis respectivo a cada una de las respuestas obtenidas de los responsables de proceso a las nueve (9) preguntas planteadas, de las cuales tres (3) son de selección múltiple con única respuesta y seis (6) son de respuesta abierta. Una vez tabulada y calificada se obtuvieron los siguientes resultados:

1.11.1. Tabulación de las respuestas

A continuación se relacionan las diecinueve (19) respuestas entregadas por cada uno de los procesos a las preguntas de selección múltiple con única respuesta:

No.	Pregunta	% Asertividad en general
1	¿Cuál es el principal objetivo de la auditoría sobre el uso de software en la entidad?	84,21
2	¿A qué se refieren el software en la entidad?	100%
6	¿Los usuarios pueden solicitar un nuevo software?	73,68

Las calificaciones por proceso se distribuyen de la siguiente manera:

No	PROCESO	CALIFICACIÓN	CALIFICACIÓN PREGUNTA 1 CUAL ES EL OBJETIVO DE LA AUDITORÍA	CALIFICACIÓN PREGUNTA 2 A QUE SE REFIEREN LOS SOFWARE DE LA ENTIDAD	PREGUNTA 3 SABE MANEJAR EL SOFWARE DE LA ENTIDAD	PREGUNTA 4 MANTENIMIENTO A LOS EQUIPOS	PREGUNTA 5 EL SOFWARE CUMPLE CON LAS NECESIDADES	PREGUNTA 6 FACILIDAD PARA SOLICITAR NUEVO SOFWARE
1	DIRECCIÓN ADMINISTRATIVA	66,66	0	100	100	100	100	0
2	CALIDAD	66,66	0	100	100	100	100	0
3	UNIDAD FUNCIONAL DE ZIPAQUIRÁ	83,33	0	100	100	100	100	100
4	PROCESO DE GESTIÓN DE SERVICIOS QUIRURGICOS	83,33	100	100	100	100	100	0
5	DIRECCIÓN DE ATENCIÓN AL USUARIO	83,33	100	100	100	100	100	0
6	PROCESO DE GESTIÓN JURÍDICA	83,33	100	100	100	100	100	0
7	PROCESO DE GESTIÓN DE SERVICIOS AMBULATORIOS	83,33	100	100	100	0	100	100
8	DIRECCION CIENTÍFICA	100	100	100	100	100	100	100
9	APOYO DIAGNOSTICO	100	100	100	100	100	100	100
10	PROCESO DE GESTIÓN DE LA INFORMACIÓN TIC	100	100	100	100	100	100	100
11	PROCESO DE GESTIÓN DE SALUD PÚBLICA	100	100	100	100	100	100	100
12	PROCESO DE GESTIÓN DE SERVICIOS HOSPITALARIOS	100	100	100	100	100	100	100
13	DIRECCIÓN FINANCIERA	100	100	100	100	100	100	100

No	PROCESO	CALIFICACIÓN	CALIFICACIÓN PREGUNTA 1 CUAL ES EL OBJETIVO DE LA AUDITORÍA	CALIFICACIÓN PREGUNTA 2 A QUE SE REFIEREN LOS SOFWARE DE LA ENTIDAD	PREGUNTA 3 SABE MANEJAR EL SOFWARE DE LA ENTIDAD	PREGUNTA 4 MANTENIMIENTO A LOS EQUIPOS	PREGUNTA 5 EL SOFWARE CUMPLE CON LAS NECESIDADES	PREGUNTA 6 FACILIDAD PARA SOLICITAR NUEVO SOFWARE
14	PROCESO DE URGENCIAS	100	100	100	100	100	100	100
15	PROCESO DE GESTIÓN DE SERVICIOS COMPLEMENTARIOS	100	100	100	100	100	100	100
16	PROCESO DE INGENIERIA HOSPITALARIA	100	100	100	100	100	100	100
17	PROCESO DE INTELIGENCIA DE MERCADOS	100	100	100	100	100	100	100
18	PROCESO DE TECNOLOGÍA BIOMEDICA	100	100	100	100	100	100	100
19	PROCESO DE GESTIÓN DE TALENTO HUMANO Y HOTELERIA HOSPITALARIA	100	100	100	100	100	100	100

1.11.2. Respuestas a preguntas formuladas en la encuesta

Las respuestas correctas de la encuesta mencionada son:

Pregunta 1. ¿Cuál es el principal objetivo de la auditoría sobre el uso de software en la entidad?
Respuesta correcta: Verificar el cumplimiento de la normatividad vigente en materia de derechos de autor sobre software.

Pregunta 2. ¿A qué se refieren el software en la entidad?
Respuesta correcta: A los programas y aplicaciones instalados en los equipos de la entidad, que deben contar con licenciamiento adecuado y cumplir con las normativas de derechos de autor.

Pregunta 3. ¿Usted sabe manejar correctamente el software de la entidad? Si no es así, ¿ha recibido alguna capacitación?
Respuesta Abierta, No hay una única respuesta correcta, ya que esta pregunta busca conocer la capacitación y el manejo del software por parte de los funcionarios.

Pregunta 4. ¿Cuantos mantenimientos preventivos de los equipos le han realizado en su proceso?
Respuesta Abierta, (busca conocer la cantidad de mantenimientos preventivos realizados).

Pregunta 5. ¿Considera que el software utilizado actualmente en la entidad cumple con sus necesidades operativas?
Respuesta Abierta, (busca evaluar si el software actual satisface las necesidades operativas)

Pregunta 6. ¿Los usuarios pueden solicitar nuevo software? Si es así, ¿cómo es el proceso de solicitud y aprobación?
Respuesta Abierta, (busca entender si los usuarios pueden solicitar nuevo software y cómo se lleva a cabo el proceso de solicitud y aprobación)

Pregunta 7. ¿Qué mejoras propondría en la gestión del software en la entidad?
Respuesta Abierta, (busca obtener sugerencias sobre posibles mejoras en la gestión del software, basadas en la experiencia y necesidades de los usuarios).

Pregunta 8. ¿Cuáles son las fortalezas en el ejercicio de la actividad de derechos de autor relacionados con el software?
Respuesta Abierta, busca identificar las fortalezas en la gestión de los derechos de autor relacionados con el software, según la percepción de quienes participan en el proceso.

Pregunta 9. ¿Cuáles son las debilidades en el ejercicio de la actividad de derechos de autor relacionados con el software?
Respuesta Abierta, busca identificar las debilidades en la gestión de los derechos de autor relacionados con el software, según la percepción de quienes participan en el proceso.

1.11.3. Debilidades y fortalezas detectadas

Como se mencionó anteriormente, se les preguntó a los líderes de procesos sobre las debilidades y fortalezas relacionadas con el ejercicio y/o actividad de derechos de autor relacionada con el software, a lo cual respondieron:

No	PROCESO	PREGUNTA 8. FORTALEZAS DEL SOFWARE	PREGUNTA 9. DEL SOFWARE
1	DIRECCIÓN ADMINISTRATIVA	Licenciamientos	Ninguno que este licenciado el software de la organización sea la que sea
2	CALIDAD	Controles definidos por sistemas para la instalación de software de manera personal	No se tiene implementado la NTC ISO 27001
3	UNIDAD FUNCIONAL DE ZIPAQUIRÁ	Protección de la propiedad intelectual creación de nuevas y mejores aplicaciones	Periodicidad en controles para evitar copia o piratería no se cuenta con licenciamiento 100% de los equipos de cómputo.
4	PROCESO DE GESTIÓN DE SERVICIOS QUIRURGICOS	Los derechos de autor impiden que terceros reproduzcan, distribuyan o modifiquen el código sin permiso, protegiendo así la inversión en desarrollo	Dificultad en la Protección de Funcionalidades: Los derechos de autor protegen la expresión del código, pero no las funcionalidades o ideas detrás del software. Aunque los derechos de autor protegen el código fuente, la ingeniería inversa permite reconstruir funcionalidades sin acceder directamente al código original. Además, la piratería de software sigue siendo un problema global difícil de controlar.
5	DIRECCIÓN DE ATENCIÓN AL USUARIO	Se protege la autoría del Hospital en investigaciones, aplicativos, lo cual fortalece la imagen institucional Evitar plagios, se evita los copias fraudulentas Ingresos económicos al Hospital como Empresa Social del Estado, Hospital Universitario	Que el Hospital posiblemente no estén tramitando los derechos de autores en su totalidad de las investigaciones, software o aplicativos
6	PROCESO DE GESTIÓN JURÍDICA	Control a páginas ociosas de internet No se puede instalar un software sin la respectiva licencia Manipulación de la configuración de los computadores solo por personal autorizado, es decir técnicos o ingenieros de sistemas	Falta de presupuesto asignado al área de sistemas Obsolescencia tecnológica
7	PROCESO DE GESTIÓN DE SERVICIOS AMBULATORIOS	Bloqueos controlados a varias páginas. No se pueden instalar software sin licencias avaladas por Sistemas. La configuración de los equipos es únicamente por el área de Sistemas.	Falta de presupuesto asignado a Sistemas Obsolescencia tecnológica.
8	DIRECCIÓN CIENTÍFICA	Se evita el uso de software no licenciados	Existen demasiados puestos de trabajo lo que hace difícil el control
9	APOYO DIAGNOSTICO	Todo el software, aplicaciones o herramientas informáticas utilizados en la entidad cuentan con licencia.	La obsolescencia tecnológica.
10	PROCESO DE GESTIÓN DE LA INFORMACIÓN TIC	Que solo se permite la instalación de software licenciado y este debe realizarse por parte del equipo de informática en caso de los equipos de cómputo.	Presupuesto para la renovación debido al costo de los licenciamientos.

No	PROCESO	PREGUNTA 8. FORTALEZAS DEL SOFWARE	PREGUNTA 9. DEL SOFWARE
11	PROCESO DE GESTIÓN DE SALUD PÚBLICA	Dentro de las fortalezas tenemos que se protege la auditoria, se incentiva la creación de nuevas ideas, favorecen la competencia de leal, se promueve el intercambio de conocimiento, se protege contra el uso indebido de nuevos conocimientos.	Las debilidades en el ejercicio de la actividad de derechos de autor relacionados con el software, puede ser que no se protegen las ideas, conceptos, se puede contar con mecanismos redundante para facilitar encontrar infractores, mantener actualizado la administración de licencias para que el manejo de estas sea seguro y flexible, contra con el registro del software ante la dirección nacional de derecho de autor,
12	PROCESO DE GESTIÓN DE SERVICIOS HOSPITALARIOS	Los empleados reciben formación sobre el uso adecuado del software y las normativas de derechos de autor. Se fomenta el uso de alternativas legales y accesibles para optimizar costos sin infringir derechos de autor.	Algunos empleados pueden desconocer las leyes de derechos de autor y las políticas internas sobre software. Algunas aplicaciones pueden estar fuera de soporte, lo que puede generar vulnerabilidades de seguridad y problemas operativos.
13	DIRECCIÓN FINANCIERA	La ESE cuenta con las licencias respectivas, las cuales se encuentran centralizadas en el área de sistemas para su seguimiento y control de las mismas, con respecto a vencimientos	El costo que puede generar para generar nuevos desarrollos que permita facilitar agilizar algunas actividades
14	PROCESO DE URGENCIAS	No, se realiza instalación del software sin licencia por parte del área de sistemas	Obsolescencia de Tecnología
15	PROCESO DE GESTIÓN DE SERVICIOS COMPLEMENTARIOS	Que todos los software o sistemas de información, aplicaciones y demás herramientas informáticas cuentan con el respectivo licenciamiento	la obsolescencia tecnológica
16	PROCESO DE INGENIERIA HOSPITALARIA	No se instala software sin licencia por parte de la subdirección de sistemas ni tampoco por parte de los usuarios	Falta de presupuesto asignado ocasionando obsolescencia tecnológica
17	PROCESO DE INTELIGENCIA DE MERCADOS	Control de Páginas Distractoras Manipulación de los Equipos por los encargados del área	Falta de Presupuesto Obsolescencia de la Tecnología
18	PROCESO DE TECNOLOGÍA BIOMEDICA	Agilidad en soporte técnico. Versiones completas del software.	Costos elevados.
19	PROCESO DE GESTIÓN DE TALENTO HUMANO Y HOTELERÍA HOSPITALARIA	La confiabilidad de la información y soporte del mismo	Compatibilidad con otros sistemas y posibles actualizaciones

1.11.3.1. Análisis General

Resumen de las debilidades encontradas por los líderes de los procesos, las cuales deben atenderse mediante plan de mejoramiento.

Categoría	Debilidades Identificadas
Licenciamiento	- Falta de licenciamiento completo en equipos. - Uso de software sin registro oficial. - Dificultad para proteger funcionalidades e ideas detrás del software.
Normatividad y Cumplimiento	- No se implementa la NTC ISO 27001. - Insuficiencia en controles contra piratería. - Falta de socialización de leyes y políticas sobre derechos de autor.
Recursos Económicos	- Presupuesto limitado para licencias y desarrollos. - Costos elevados para renovación tecnológica y nuevos desarrollos.
Tecnología	- Obsolescencia tecnológica recurrente. - Aplicaciones fuera de soporte, generando vulnerabilidades de seguridad.
Gestión y Control	- Dificultades en el control del licenciamiento debido a muchos puestos de trabajo. - Falta de administración actualizada de licencias.

Categoría	Debilidades Identificadas
Compatibilidad	- Problemas de compatibilidad con otros sistemas y posibles actualizaciones.

2. Seguimiento para rendir el informe anual en al aplicativo de la Dirección Nacional de Derechos de Autor

El 22 de enero de 2025, mediante correo electrónico, se remitió un oficio a la Subdirección de Sistemas con una serie de preguntas relacionadas con la auditoría. A continuación, se presenta un resumen de las respuestas recibidas:

2.1. Gestión de Inventarios de Equipos y Software

Pregunta 1. **¿Con cuántos equipos cuenta la entidad?**

La entidad cuenta con Total Equipos 1416, discriminados de la siguiente manera:

Equipos Bogotá:

- 136 portátiles
- 24 portátiles nuevos (Bodega)
- 677 equipos escritorio
- 50 equipos escritorio nuevo (Bodega)

Total 887

Equipos Sede HRegional:

- 23 portátiles
- 241 equipos escritorio
- 15 equipos escritorio nuevo (Bodega)

Total 279

Equipos Sede UFuncional

- 23 portátiles
- 202 equipos escritorio
- 25 equipos escritorio nuevo (Bodega)

Total 250

Pregunta 2. **¿Existe un inventario actualizado de los equipos y el software instalado en la entidad?**

Actualmente cada una de las sedes cuentan con un sistema de información llamado GLPI, el cual es una herramienta de gestión de servicios y seguimientos de incidencias, que adicionalmente cuenta con un sistema de inventario el cual toma la información de todos los equipos que se encuentren dentro del dominio (Red Privada del Hospital), esto incluye seriales de CPU, monitores, periféricos conectados y software instalado.

Pregunta 3. **¿Con qué frecuencia se realiza el mantenimiento preventivo de los equipos?**

Se tiene un cronograma anual establecido para realizar a los equipos de cómputo mantenimiento preventivo, este está dividido por áreas y pisos donde se establecen unas metas diarias. Por la cantidad de equipos la estimación de mantenimiento a cada equipo es 1 vez al año.

Pregunta 4. **¿Qué porcentaje de los equipos está operativo en relación con el total?**

El total de equipos de cómputo de todas las sedes son 1416 operativamente, con corte a 31/12/2024 solo se encuentras los equipos adquiridos en Diciembre en bodega en espera de reasignación.

2.2. Políticas de Licenciamiento y Uso de Software

Pregunta 1. **¿El software instalado en estos equipos se encuentran debidamente licenciados?**

En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y de acorde a la propiedad intelectual. Si los equipos son externos (Equipos en tránsito rápido) deben cumplir con las políticas de licenciamiento y uso de software establecidos por la subdirección de sistemas.

Pregunta 2. **¿La entidad cuenta con políticas documentadas sobre la adquisición y el uso de software?**

La subdirección de Sistemas cuenta con un documento donde se encuentran establecidas las políticas de seguridad y manejo de la información, en ellas se incluye Políticas de Licenciamiento y uso de Software. Corresponde a la Subdirección de Sistemas emitir las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia así como el verificar que el software provenga de fuentes conocidas y seguras.

2.3. Seguridad y Control de Software

Pregunta 1. **¿Qué mecanismos de control se han implementado para evitar que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva?**

Acorde con la política de la institución, la Subdirección de Sistemas es el organismo oficial del Hospital para establecer los mecanismos de procuración de sistemas informáticos, corresponde a la Subdirección de Sistemas emitir las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo además de esto la instalación de software que desde el punto de vista de la Subdirección de Sistema pueda poner en riesgo los recursos de la institución no está permitida.

Actualmente se cuentan con las siguientes políticas implementadas para restringir la instalación de aplicativos por parte de los usuarios en los equipos de cómputo:

- ✓ Directorio Activo:

Restricción desde el directorio activo (Aplica para usuarios y equipos conectado al dominio HUS.CO) la restricción a los usuarios para la instalación de software, este solo puede realizarse desde los usuarios administradores.

- ✓ Filtrado de Contenido (Firewall):

- Se tiene configurado la restricción de la descarga e instalación por Internet de software e licenciados y software malicioso.
- Se cuenta con una consola de administración de antivirus para el bloqueo de ejecutables para la instalación de software y análisis de virus informáticos.

Pregunta 2. **¿Se han reportado incidentes relacionados con el uso de software sin licencia?**

Actualmente no se tienen reportes del uso o incidentes relacionados con el uso de un aplicativo sin licencia que se encuentre instalado en la infraestructura tecnológica del hospital y sus sedes.

2.4. Gestión de Software Dado de Baja

Pregunta 1. **¿Cuál es el destino final que se le da al software dado de baja en la entidad?**

Debido a que las licencias corresponden a un intangible, para esto se genera el documento de la salida (baja), este es validado por parte del Comité de Inventarios como está definido en el procedimiento "02GBS11 - BAJA DE ACTIVOS FIJOS" y estas son desinstaladas de los equipos de cómputo por parte del personal de sistemas y algunas licencias debido a que tienen un tiempo fijo automática mente se desactivan en el caso

que no se procede a realizar desinstalación en su totalidad en los equipos informáticos que cuenten con el software salvaguardando la data que este software pudiesen generar con información institucional y se procede a retirar de los activos fijos.

Pregunta 2. ¿Se realiza un análisis previo para determinar si el software dado de baja puede ser reutilizado o transferido?
Si el software va ser remplazado por versión actualizada pero aún cuenta con licencia vigente y el nuevo software ingresa con licenciamiento independiente, se realiza un análisis previo de las funciones y la vida útil del respectivo licenciamiento teniendo en cuenta que varios casos el licenciamiento va ligado a la versión del hardware.

2.5. Adquisición y Actualización de Software

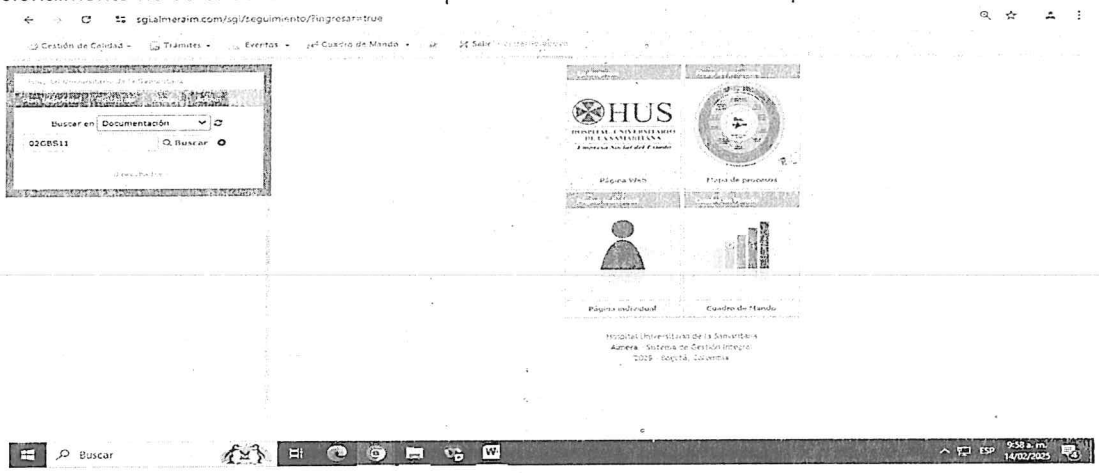
Pregunta 1. **¿Qué criterios se consideran para adquirir software nuevo en la entidad?**
La mayoría de compras de licenciamiento se realizan a la necesidad y con el objetivo de salvaguardar la seguridad informática de la entidad, posteriormente dar la continuidad en los procesos asistenciales y administrativos de la entidad y por ultimo necesidades específicas de los servicios, Todo esto con previa inclusión dentro del PAA para la vigencia y el presupuesto de los proyectos que se otorga a las diferentes unidades funcionales del HUS dependiendo la necesidad.

Pregunta 2. **¿Qué planes de actualización o renovación de licencias están en marcha?**
Los procesos de actualización se van realizando dependiendo el periodo y tipo de licencia, de los cuales se tienen proyectado los siguientes aplicativos:
Almera (licencia de uso – anualidad).
PACS – RIS (licencia de uso – anualidad).
AMSI (Mesa Ayuda Mantenimiento).
Antivirus (Anualidad).
Firewall (Anualidad).
Licenciamiento Correo Electrónico (Anualidad).
Plataforma Diagnósticos Relacionados GRD (Anualidad).
Aplicativo Trazabilidad (Anualidad).

De acuerdo a la respuesta en la cual dice: *"Se tiene un cronograma anual establecido para realizar a los equipos de cómputo mantenimiento preventivo, este está dividido por áreas y pisos donde se establecen unas metas diarias. Por la cantidad de equipos, la estimación de mantenimiento a cada equipo es 1 vez al año"*.
Se recomienda analizar la posibilidad de aumentar la frecuencia del mantenimiento preventivo para aquellos equipos que presenten un mayor uso o criticidad en los procesos institucionales, con el fin de reducir el riesgo de fallas técnicas y garantizar su óptimo funcionamiento.

De acuerdo a la respuesta en la cual dice: *"Debido a que las licencias corresponden a un intangible, para esto se genera el documento de la salida (baja), este es validado por parte del Comité de Inventarios como está definido en el procedimiento '02GBS11 - BAJA DE ACTIVOS FIJOS"*.
Se recomienda evaluar la posibilidad de reutilización del software dado de baja en aquellos casos en los que las licencias aún sean vigentes y puedan ser aprovechadas en otros equipos o áreas de la entidad. Para ello, se puede establecer un proceso de análisis previo que determine la viabilidad de su transferencia antes de proceder con la baja definitiva.

Adicionalmente no se encontró en Almera el procedimiento indicado en la respuesta:

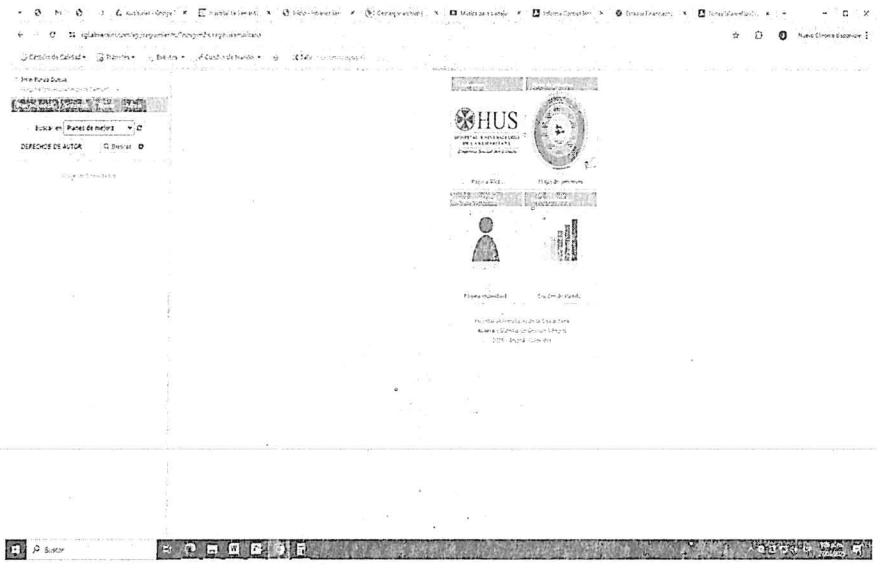


De acuerdo a la respuesta en la cual dice: *"Los procesos de actualización se van realizando dependiendo el periodo y tipo de licencia, de los cuales se tienen proyectado los siguientes aplicativos: Almera, PACS – RIS, AMSI, Antivirus, Firewall, Licenciamiento de Correo Electrónico, Plataforma Diagnósticos Relacionados GRD y Aplicativo de Trazabilidad"*.

Se recomienda realizar una planificación detallada de la renovación de licencias con suficiente antelación para evitar interrupciones en los servicios y optimizar el uso del presupuesto asignado. Asimismo, se sugiere explorar alternativas de licenciamiento que permitan reducir costos sin comprometer la funcionalidad y seguridad del software utilizado en la entidad.

3. Seguimiento a Planes de Mejoramiento.

Tras revisar el Aplicativo Institucional Almera, destinado a centralizar todos los planes de mejoramiento de la institución, se evidenció que no existen planes de mejoramiento vinculados al presente informe de auditoría.



4. Recomendaciones

4.1. Recomendaciones Vigencia 2025

No.	Descripción de la recomendación
1	**Condición:** Se identificó que la **Política de Gestión de la Información y Comunicación** (Código 01DE12-V1), aprobada en enero de 2018, no ha sido actualizada conforme a su periodo de revisión de cuatro años, el cual venció el 31 de enero de 2022. **Criterio:** Según el Modelo Integrado de Planeación y Gestión (MIPG) y los principios de administración pública, la actualización periódica de las políticas es fundamental para garantizar su eficacia, alineación con los objetivos estratégicos de la entidad y cumplimiento de las normativas vigentes**. Procedimientos internos.** **Causa:** Falta de un mecanismo de seguimiento y actualización periódica de las políticas institucionales. **Efecto:** Puede generar desalineación con la normatividad vigente, afectando la gestión efectiva de la información y la comunicación institucional.
2	**Condición:** Se evidenció que los indicadores de Gestión de la Información TIC con códigos 971, 972, 973 y 1020 no han sido actualizados en el aplicativo "ALMERA", y su respectivo análisis tampoco ha sido registrado. **Criterio**: Decreto 612 de 2018, que regula la preparación, presentación y publicación de informes de gestión, estableciendo la obligación de realizar seguimiento oportuno a los indicadores financieros. **Causa:** Falta de seguimiento y control en la actualización de los indicadores en la plataforma institucional. **Efecto:** Impide una evaluación precisa del desempeño en la gestión de TIC, afectando la toma de decisiones estratégicas y la planeación de mejoras en los procesos tecnológicos de la entidad.
3	**Condición:** Se evidenció que el procedimiento "02GBS11 - Baja de Activos Fijos" no está disponible en el sistema ALMERA. Además, no se ha evaluado la posibilidad de reutilización de software dado de baja, a pesar de que algunas licencias aún podrían estar vigentes y ser aprovechadas en otras áreas de la entidad. **Criterio:** De acuerdo con la Ley 1712 de 2014 sobre la transparencia y el derecho de acceso a la información pública, y la normatividad interna de la entidad sobre la gestión de activos tecnológicos. **Causa:** Falta de un proceso estructurado para la revisión y reutilización de licencias antes de su baja definitiva, así como la ausencia de registros actualizados en ALMERA sobre los procedimientos aplicables. **Efecto:** Posible desaprovechamiento de recursos tecnológicos, generando costos innecesarios por la compra de nuevas licencias cuando algunas aún podrían ser utilizadas. Además, la ausencia del procedimiento en ALMERA dificulta su consulta y aplicación adecuada.

4	**Condición:** Se ha identificado que la entidad no cuenta con una planificación detallada de la renovación de licencias de software, lo que podría generar interrupciones en los servicios si no se gestionan adecuadamente. A pesar de que se tiene proyectada la actualización de algunos aplicativos clave, como Almera, PACS – RIS, AMSI, Antivirus, Firewall, Licenciamiento de Correo Electrónico, Plataforma Diagnósticos Relacionados GRD y Aplicativo de Trazabilidad, no se ha establecido una estrategia clara y anticipada para la renovación de estas licencias. **Criterio:** De acuerdo con el Decreto 1078 de 2015, que establece el régimen de contratación y administración de recursos en el sector público, es fundamental garantizar la continuidad operativa mediante una gestión proactiva en la renovación de licencias de software. **Causa:** Ausencia de un proceso formalizado o la falta de visibilidad sobre los plazos y tipos de licencias a renovar. **Efecto:** Sin una planificación adecuada, la entidad podría enfrentar interrupciones en los servicios operativos debido a la caducidad de las licencias. Esto afectaría la continuidad de los servicios y la eficiencia de las funciones institucionales. Además, podría implicar un mal uso del presupuesto, al no contar con tiempo suficiente para evaluar alternativas más costo-efectivas.
5	**Condición**: Los procesos "Dirección Administrativa" y "Calidad" han mostrado un nivel de conocimiento del 66.66% respecto al tema auditado, lo que evidencia áreas de mejora en su comprensión y aplicación práctica. De acuerdo con los estándares organizacionales, los responsables de estos procesos deben alcanzar un nivel óptimo de conocimiento y liderazgo sobre el tema auditado, para asegurar un direccionamiento adecuado y efectivo del personal a cargo. **Criterio:** Ley 87 de 1993, Ley 1915 de 2018, Norma ISO 27001 **Causa:** La insuficiencia de formación o actualización en temas específicos relacionados con el asunto auditado ha limitado la capacidad de estos procesos para ejercer un liderazgo completo. **Efecto:** Esta deficiencia puede ocasionar dificultades en la orientación y supervisión del personal, afectando la efectividad y los resultados de las actividades institucionales.
6	**Condición:** Los líderes de los procesos han identificado debilidades significativas a través de las encuestas de pre saberes, las cuales afectan el desempeño y conocimiento técnico de sus equipos. Según los estándares organizacionales, los líderes deben contar con información clara y precisa sobre las competencias de sus equipos, para implementar estrategias de mejora que fortalezcan los procesos internos y alineen los resultados con los objetivos institucionales. **Criterio:** Ley 87 de 1993, Ley 1915 de 2018, Norma ISO 27001 **Causa:** Las debilidades reportadas son producto de un conocimiento insuficiente en áreas clave y de la falta de implementación de programas de capacitación específicos para abordar las brechas detectadas. **Efecto:** No atender estas debilidades puede generar deficiencias en la ejecución de los procesos, disminuir la calidad del trabajo y limitar el alcance de los objetivos organizacionales, impactando negativamente la eficacia y eficiencia de la institución.
7	**Condición:** Los equipos institucionales con alto uso o criticidad requieren especial atención debido a su impacto en los procesos operativos esenciales. Se recomienda analizar la frecuencia actual del mantenimiento preventivo y evaluar si esta es adecuada para garantizar el funcionamiento continuo y eficiente de dichos equipos. **Criterio:** Ley 87 de 1993, Ley 1915 de 2018, Norma ISO 27001 **Causa:** La falta de mantenimiento preventivo adecuado o frecuente aumenta el riesgo de fallas técnicas en equipos críticos, afectando su desempeño y la continuidad operativa. **Efecto:** Incrementar la frecuencia del mantenimiento preventivo reducirá el riesgo de fallas técnicas, mejorará la confiabilidad de los equipos y garantizará su óptimo desempeño en los procesos institucionales.

4.2. Recomendaciones Vigencias Anteriores

No.	Descripción de la recomendación

No.	Descripción de la recomendación
1	**Condición:** En la identificación de este riesgo de proceso institucional III trimestre 2022, una de las causas de posible de ocurrencia, la primera de este riesgo está encaminado a la dirección del ciclo vital de los archivos físicos, ley 594 de 2000, la tercera causa encauzada a el hardware utilizado y solo la segunda causa está orientada a los posibles ataques cibernéticos; en la identificación del riesgo, lo mismo que en las causas, se advierte en su primera parte la perdida de información por el inadecuado manejo de sistemas y en su segunda parte la inconsistencia en el manejo de la gestión documental; los controles están encaminados a la gestión documental; ninguno está dirigido a mitigar y/o minimizar las posibles materializaciones. El riesgo de corrupción vigencia 2022, aunque se ajusta a la definición de los que es el riesgo de corrupción, tiene como causa "que los controles existentes son insuficientes", y aplicados los controles (cuatro) la zona de riesgo residual continua siendo ALTA, por lo que puede afirmarse que los controles establecidos para este riesgo de corrupción no conducen a mitigar, minimizar la materialización de este riesgo,. En ninguna de sus partes se identifican riesgos de fraude, clientelismo, deficiente calidad de información pública, entre otros. **Criterio:** Decreto No. 1499 de 2014, Decreto 1083 de 2015 **Causa:** Debilidad en el tratamiento de los riesgos de seguridad de la información y sus controles asociados **Efecto:** Ataques cibernéticos, secuestro de la información Incumplimiento del Tratamiento de Riesgos de seguridad de la Información Riesgos sin controles asociados correctamente y/o riesgos con controles inadecuadamente identificados Incumplimiento de la normatividad vigente
2	**Condición:** Se evidencia que no existe documentación asociada a la gestión que se adelanta frente al inventario, a la administración de las firmas digitales de los funcionarios de dirección de la E.S.E. relacionados con el proveedor CERTICAMARA y controles en lo referente a los procedimientos de creación, renovación, recuperación, eliminación de llave y controles criptográficos **Criterio:** Circular Externa No.12 de febrero de 2007 DNDA, Circular Externa No. 017 de junio de 2011 DNDA **Causa:** Debilidad en los controles de firmas digitales **Efecto:** Desconocimiento de los inventarios de software con que cuenta la E.S.E
3	**Condición:** En el manual de seguridad informática se observa: **En su alcance,** con la respuesta se observa el resultado de una medición a través de un indicador (PORCENTAJE DE ATAQUES INFORMATICOS QUE AFECTAN EL SISTEMA DE INFORMACIÓN), mas no se evidencia un ciclo en donde haya diseños e implementación de unas medidas y patrones técnicos de administración a equipos de cómputo, pagina WEB, INTRANET, y que posterior al seguimiento y evaluación al cumplimiento de la seguridad de la información arrojen como resultado un indicador , que permitan **prevenir detectar** y/o mitigar los posibles actos que vulneren la seguridad informática; WUE GARANTICEN LA INTEGRIDAD DE LA INFORMACIÓN. ***Del numeral 7.7*** **Del contenido página web e intranet del HUS**: No se da aplicabilidad a lo establecido en el Manual de seguridad informática de la E.S.E. ***Del numeral 7.11*** **Auditoria software instalado**: La oficina de control interno no es la responsable de realizar revisiones para asegurar que solo el software con licencia este instalado en los computadores del hospital y menos el corresponderá dictar las normas procedimientos. Ya que la oficina de Control Interno no es competente, la Ley 87 de 1993 establece **que en ningún caso, podrá el asesor, coordinador, auditoria interno o quien haga sus veces participar en los procedimientos administrativos de la entidad a través de autorizaciones y refrendaciones**. El desarrollo del Sistema de Control Interno se orientara, a la protección de los recursos de la organización y a la adecuada administración ante posibles riesgos que los afecten y a la aplicación de medidas pata prevenir detectar y corregís las desviaciones que se presenten al interior y que pueden afectar el logro de los sus objetivos. Y como mecanismos de verificación y evaluación dl control interno se utilizaran las auditorias generalmente aceptadas por la normatividad Ahora bien con lo anterior Control Interno no es responsable de realizar revisiones y menos dictar normal ni procedimientos. Por lo tanto el responsable de asegurar que solo el software con licencia este instalado en los computadores del hospital, está en cabeza de la Subdirección de Sistemas. **En la afirmación "...son los responsables de realizar revisiones periódicas para asegurar que solo el software con licencia este instalado en los computadores del hospital**; ajustado con lo anterior se ha evidenciado que en varios de los equipos de cómputo se encuentran software libres y en ninguna de las partes del manual de seguridad informática hace referencia a este tipos software. ***Numeral 7.12*** **Software propiedad de la institución** se adjunta inventario del software de propiedad de la E.S.E., no incluidos el inventario de software solicitado para la realización de la presente auditoria ***Numera 7.13*** **Uso del Software Académico Software: Dentro del inventario de software académico se establece** el Saberes y el Biteca, no incluido en el inventario de software de la E.S.E **Criterio:** Ley 1273 de 2009 **Causa:** Debilidad en la construcción y aplicabilidad del Manual de seguridad informática, generando debilidad de seguridad informática, con referencia al SOFTWARE **Efecto:** -Posibles ataques cibernéticos producidos por la debilidad de la protección del software -Vulnerabilidad de los sistemas informáticos, es decir, fallas o deficiencias que ponen en riesgo los activos al no estar protegidos de manera efectiva
4	**Condición:** Coherente con lo establecido en el Manual de seguridad informática – numeral 7 y acorde con los lineamientos de la institución, el proceso de gestión de la información es el proceso oficial encargado de establecer los mecanismos de administración de los sistemas informáticos. -Una vez observada la información allegada y realizada la verificación del SOFTWARE instalado en los equipos de la E.S.E., según la muestra establecida, el SOFTWARE está comprendido por: – Software debidamente licenciado

No.	Descripción de la recomendación
	– De propiedad de la E.S.E. Hospital Universitario de la Samaritana – El SOFTWARE académico – El SOFTWARE libre uso en la E.S.E. – Otro SOFTWARE de uso en la E.S.E. Cada uno de estos SOFTWARE es de uso de la E.S.E. Hospital Universitario de la Samaritana, por lo tanto debe estar contenido en un inventario general de SOFTWARE institucional. El módulo de Inventarios de DGH tiene identificadas todas las licencias por número de plaza individual, las LICENCIAS ANTIVIRUS EST ENDPOINT SECURITY adquiridas anualmente e identificadas en el módulo continúan como un activo intangible, no han sido dadas de baja según el procedimiento establecido para los activos intangibles inventario. - Con lo informado la sede Unidad Funcional Zipaquirá, no registra dentro de sus inventarios de software el antivirus ESET ENDPOINT SECURITY. - Con la información aportada, las demás registradas son: cuatro mil quinientos veinte y uno (4.521) licencias, cada una de ellas identificadas con número de placa, se observa que la sede Unidad Funcional Zipaquirá reconoce 15 software debidamente licenciados y dentro del inventario de hardware reconoce 205 computadores de escritorio+ 25 computadores portátiles. - En coherencia con lo establecido en el Manual de seguridad informática – numeral 7 y acorde con los lineamientos de la institución, el proceso de gestión de la información es el proceso oficial encargado de establecer los mecanismos de administración de los sistemas informáticos; por lo tanto la administración absoluta, dentro de la cual están incluidos los inventarios y la seguridad del SOFTWARE es competencia proceso de gestión de la información. **Criterio:** LEY 1273 de 2009, Circular Externa No. 12 de febrero de 2007 DNDA, Circular Externa No. 017 de junio de 2011 DNDA **Causa:** Debilidad en el establecimiento de los inventarios de software y/o Fallá en las conciliaciones de los inventarios de activos fijos intangibles, Los activos fijos Intangibles, al igual que todos los activos fijos son de importancia fundamental en las entidades. Corta frecuencia en la revisión y verificación del SOFTWARE. Todo software adquirido por la E.S.E. sea por compra, donación o sesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera. No aplicabilidad del Manual de seguridad informática generando debilidad de seguridad informática, con referencia al SOFTWARE. **Efecto:** Posibles riesgos, dada la Vulnerabilidad de los sistemas informáticos, en cuanto hace referencia la identificación compilaciones de software de uso de la E.S.E. (numeral 7.12).

SOLICITUD: Las recomendaciones registradas anteriormente en este informe de Auditoría, que se requieren Plan de Mejoramiento, deben quedar plasmadas conforme se enuncian, no deben ser modificadas de manera total ni parcialmente.

El Código Único Disciplinario, Ley 737 de 2002 el cual se encuentra vigente a la fecha del presente informe de auditoría, Ley 1952 de 2019 – Código General Disciplinario, Ley 2094 de 2021 – "Por medio de la cual se reforme la Ley 1952 de 2019 y se dictan otras disposiciones", establece que se debe dar aplicabilidad a lo que se registra en las solicitudes realizadas y a las cuales se les debe dar respuesta por cada uno de los Responsables de Proceso y cuyo texto es el siguiente: "No dar respuesta a los requerimientos que se realicen constituye una falta disciplinaria".

El presente informe de auditoría es de carácter institucional, la verificación fue realizada con base a la información mínima publicada en el sitio WEB, Sistema de Gestión Integral "ALMERA" de propiedad de la E.S.E. Hospital Universitario de la Samaritana, si bien es cierto que la información es plasmada y de responsabilidad de cada uno de los servidores públicos responsables de procesos, estas NO son de carácter individual ni personal, por lo tanto las conclusiones y recomendaciones aquí registrados, como los Planes Únicos de Mejoramiento por Procesos a que dé lugar, son netamente de carácter institucional.

YETICA JHASVELLI HERNANDEZ ARIZA
Jefe Oficina Asesora de Control Interno

YINETH DANIELA RUGELES BASTOS
Técnico II Oficina Asesora de Control Interno

Bogotá, D.C. Marzo 27 de 2025