



E.S.E. HOSPITAL UNIVERSITARIO DE LA SAMARITANA

CONTROL INTERNO

INFORME DE AUDITORÍA INTERNA INDEPENDIENTE

05CIN01-V2



05GIC92-V1

EMPRESA SOCIAL DEL ESTADO HOSPITAL UNIVERSITARIO DE LA SAMARITANA

NIT. 899.999.032-5

INFORME FINAL AUDITORÍA DE PROCESO GESTIÓN DE LA INFORMACIÓN TIC-SISTEMAS.

Bogotá D.C, septiembre 28 de 2026

Tabla De Contenido

1. ASPECTOS GENERALES.....	3
1.1 Introducción	3
1.2. Objetivo general.....	3
1.3 Alcance	3
1.4 Marco normativo	4
1.5 Metodología	5
2. RECONOCIMIENTO DE BUEN DESEMPEÑO (PROCESOS EN CUMPLIMIENTO)	5
3. ANÁLISIS DE LAS EVIDENCIAS	7
4. OBSERVACIONES.....	9
5. RECOMENDACIONES Y OPORTUNIDADES DE MEJORA.....	10
6. TABLA CONSOLIDADA OBSERVACIONES Y RECOMENDACIONES ACEPTADAS	11
7. CONCLUSIÓN	13
8. ANEXOS	15
Anexo 1. Lista de Chequeo.....	15

1. ASPECTOS GENERALES

1.1 Introducción

La presente auditoría se realiza con el propósito de evaluar la gestión de Sistemas y Tecnologías de la Información de la E.S.E. Hospital Universitario de la Samaritana y su Red, verificando las condiciones de la infraestructura tecnológica, los controles de ciberseguridad, el licenciamiento de software, la redundancia de red y conectividad, los mecanismos de respaldo de la información (backups), así como la aplicación de las políticas de Gobierno Digital y del Modelo de Seguridad y Privacidad de la Información (MSPI).

La revisión busca contribuir al fortalecimiento de la disponibilidad, continuidad y seguridad de los servicios tecnológicos que soportan los procesos misionales y administrativos de la entidad, mediante la identificación de fortalezas y aspectos susceptibles de mejora que permitan fortalecer los controles y la gestión de los riesgos asociados a la tecnología y la seguridad de la información.

1.2. Objetivo general

Evaluar la gestión de la información y los servicios tecnológicos asociados al proceso de Gestión de la Información TIC – Área de Sistemas de la E.S.E. Hospital Universitario de La Samaritana, mediante la verificación de los controles, procedimientos y mecanismos implementados para la administración, protección, disponibilidad, continuidad y seguridad de la información y de la infraestructura tecnológica, de conformidad con el PETIC, el MSPI y demás lineamientos institucionales aplicables.

1.3 Alcance

La auditoría comprende la evaluación de las actividades, procedimientos, registros, controles y servicios tecnológicos asociados al proceso de Gestión de la Información TIC – Área de Sistemas de la Red Samaritana, incluyendo la Sede Bogotá, la Unidad Funcional de Zipaquirá (UFZ) y el Hospital Regional de Zipaquirá (HRZ).

La revisión contempla los siguientes aspectos:

- Gestión de los riesgos asociados a la información y a los activos de información.
- Administración, operación y disponibilidad de los sistemas de información institucionales y sus controles.
- Producción, organización, almacenamiento, transferencia, conservación y disposición final de la información y documentación electrónica.
- Gestión de usuarios, perfiles de acceso, mecanismos de autenticación y controles de seguridad de la información.
- Administración de copias de seguridad (backups), recuperación de la información y continuidad de los servicios tecnológicos.
- Verificación del cumplimiento de políticas, procedimientos, lineamientos institucionales y normatividad vigente relacionada con la gestión documental electrónica, seguridad de la información y Tecnologías de la Información y las Comunicaciones (TIC).
- Seguimiento a indicadores, gestión de riesgos, acciones de mejora y controles implementados en el proceso.

1.4 Marco normativo

El proceso de auditoría de sistemas se fundamenta jurídicamente en las siguientes disposiciones del orden constitucional, legal e institucional:

- **Constitución Política de Colombia (Artículos 209 y 269):** Principios rectores de la función pública administrativa y la obligación legal de diseñar y aplicar controles internos institucionales
- **Ley 1712 de 2014 y Decreto Reglamentario 0103 de 2015:** Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, aplicable a la estandarización del menú web institucional
- **Resolución 1519 de 2020 del Ministerio de las TIC:** Directrices de accesibilidad web, uso de lenguaje inclusivo y estandarización del portal de transparencia gubernamental
- **Decreto 780 de 2016 (Compilatorio del Sector Salud):** Reconoce expresamente los sistemas de información, redes de datos y telecomunicaciones como parte fundamental de la infraestructura hospitalaria de la red pública
- **Resolución de Calidad en Salud (Resolución 256 de 2016):** Estandariza el reporte obligatorio de variables de calidad, donde sistemas actúa como proveedor de la información base del HUS

- **Norma Técnica Internacional ISO/IEC 27001:2013:** Estándares mundiales para la implementación y auditoría de un Sistema de Gestión de Seguridad de la Información (SGSI)
- **Manual de Contratación de la E.S.E. HUS (Resolución 530 de 2021 y sus modificatorias):** Regula las etapas precontractuales, contractuales y la supervisión técnica de los contratos de tecnología

1.5 Metodología

Para el desarrollo de la auditoría se aplicó una lista de chequeo unificada y estructurada, compuesta por cuarenta y cinco (45) preguntas, orientada a verificar el cumplimiento de los procedimientos establecidos, la implementación de controles y la existencia de los soportes documentales correspondientes.

La revisión comprendió el análisis de la documentación suministrada por el área, incluyendo contratos de licenciamiento, planes estratégicos de sistemas (PETIC, MSPI y Tratamiento de Riesgos), caracterizaciones de procesos e inventarios de activos de información. Asimismo, se realizaron entrevistas con los responsables del proceso, observación directa de las actividades y verificación de aspectos relacionados con la administración de bases de datos, almacenamiento de información, seguridad tecnológica, sistemas de respaldo de energía (UPS), infraestructura física, servicios de soporte y mesa de ayuda, así como la gestión de riesgos tecnológicos y de ciberseguridad. La evaluación de los criterios se realizó considerando la existencia, aplicación y evidencia de los controles, así como las situaciones identificadas durante el trabajo de campo.

2. RECONOCIMIENTO DE BUEN DESEMPEÑO (PROCESOS EN CUMPLIMIENTO)

De acuerdo con la revisión realizada al proceso de Gestión de la Información TIC – Área de Sistemas, se evidenció un adecuado nivel de implementación y operación de los controles asociados a la gestión tecnológica institucional, respaldado por la existencia de procedimientos documentados, mecanismos de seguridad informática, controles sobre los activos tecnológicos y herramientas orientadas a garantizar la disponibilidad, protección y respaldo de la información institucional.

Se destacan positivamente los siguientes aspectos:

- **Gestión de licenciamiento y seguridad informática:** se evidenció la disponibilidad de herramientas de protección antivirus licenciadas y activas para los equipos y servidores de la institución, contribuyendo a fortalecer las medidas de prevención y protección frente a amenazas informáticas.

- **Control e inventario de activos tecnológicos:** se evidenció la existencia de un inventario de equipos informáticos que permite identificar y realizar seguimiento a los activos tecnológicos de la Red Samaritana, mediante el registro de información técnica y de identificación de los dispositivos.
- **Gestión y trazabilidad de la mesa de ayuda:** se evidenció la aplicación de un procedimiento formal para la atención de solicitudes de soporte tecnológico, contemplando las etapas de recepción, asignación, atención y cierre, lo que permite mantener la trazabilidad de los requerimientos y facilitar su seguimiento.
- **Gestión de bases de datos y licenciamiento de software:** se evidenció la implementación de mecanismos de control sobre el software utilizado para la operación de los sistemas institucionales, incluyendo el motor de base de datos requerido para el funcionamiento de las aplicaciones institucionales, favoreciendo el uso autorizado y controlado de los recursos tecnológicos.
- **Gestión de copias de seguridad:** se evidenció la ejecución de actividades orientadas al respaldo de la información institucional mediante mecanismos de almacenamiento local, medios externos y servicios de almacenamiento en la nube, fortaleciendo las condiciones para la recuperación de la información ante posibles eventos que puedan afectar su disponibilidad.
- **Seguridad y disponibilidad de la infraestructura tecnológica:** se evidenció la implementación de mecanismos de seguridad perimetral y conectividad redundante, orientados a fortalecer la protección de la infraestructura tecnológica y la continuidad de los servicios de comunicaciones institucionales.
- **Gestión documentada de los servicios tecnológicos:** se evidenció la existencia de procedimientos y lineamientos institucionales para la ejecución de actividades relacionadas con soporte, administración y operación de los servicios tecnológicos, contribuyendo a la estandarización y control de las actividades desarrolladas por el área.

3. ANÁLISIS DE LAS EVIDENCIAS

Con el propósito de verificar la adecuada aplicación de los procedimientos y controles establecidos para la gestión de la información, la seguridad tecnológica y la operación de la infraestructura de sistemas, se realizó la revisión de los criterios establecidos en la lista de chequeo y de los soportes documentales suministrados por el Área de Sistemas, complementada con entrevistas y verificaciones realizadas durante el trabajo de campo.

Como resultado de la revisión, se evidenció, en términos generales, la existencia de procedimientos y controles orientados a la protección de la información, administración de activos tecnológicos, gestión de licenciamiento, atención de requerimientos, respaldo de la información y operación de la infraestructura tecnológica. No obstante, se identificaron aspectos que requieren fortalecimientos relacionados principalmente con las condiciones de climatización del centro de datos, la obsolescencia de infraestructura tecnológica, la ejecución de actividades previstas en los instrumentos de planeación de TI y la redundancia física de las conexiones de comunicaciones.

En materia de seguridad y condiciones físicas del centro de datos (Datacenter), se evidenció el aislamiento del área, así como la existencia de señalización relacionada con riesgo eléctrico y restricción de acceso a personal no autorizado. Sin embargo, durante la revisión no se identificaron soportes que permitieran evidenciar la existencia de un contrato o esquema formal de mantenimiento especializado para los sistemas de climatización del Datacenter. Esta situación requiere fortalecimiento, considerando la importancia de mantener condiciones ambientales adecuadas para garantizar la disponibilidad y conservación de los equipos que soportan los servicios tecnológicos institucionales.

Respecto de la infraestructura de servidores y administración de identidades, se evidenció que el controlador de dominio principal de la Red Samaritana, identificado como ZIPADC, opera sobre una versión obsoleta del sistema operativo Windows Server 2003, situación que representa una condición de riesgo frente a la disponibilidad de actualizaciones de seguridad y a la atención de vulnerabilidades tecnológicas. Adicionalmente, se observó que los mecanismos utilizados para restringir la instalación o utilización de software no autorizado se apoyan principalmente en controles locales y actividades de verificación, evidenciándose la oportunidad de fortalecer la administración centralizada de políticas de seguridad mediante herramientas asociadas al Directorio Activo.

En relación con la planeación y gestión estratégica de tecnologías de la información, se revisó el seguimiento efectuado en la plataforma Almera SGI a las actividades establecidas para la vigencia 2026. De acuerdo con la información registrada, el Cronograma Unificado de Actividades del Plan de Seguridad de la Información 05GIC42-V3 presenta un avance físico acumulado del 0,0 %, correspondiente a seis (6) actividades programadas y sin actividades registradas como ejecutadas o finalizadas. De igual manera, el Cronograma de Actividades PETIC 2026 presenta un avance físico acumulado del 0,0 %, con ocho (8) actividades programadas y sin avance registrado a la fecha de corte de la revisión. Lo anterior evidencia la necesidad de fortalecer el seguimiento y ejecución de las actividades previstas en los instrumentos de planeación de TI.

Frente a las actividades de seguridad de la información y controles preventivos, se observó que algunas acciones contempladas en los cronogramas de la vigencia no presentan avance registrado, entre ellas actividades relacionadas con campañas de seguridad informática, revisión de cuentas de acceso remoto VPN, seguimiento de registros de eventos del firewall, verificación de accesos al Datacenter y generación de soportes asociados a la ejecución y validación de las copias de seguridad. Esta situación requiere seguimiento por parte del área responsable, con el fin de garantizar que las actividades de control previstas sean ejecutadas y cuenten con los respectivos soportes de evidencia.

En materia de respaldo de la información, se evidenció la existencia de mecanismos orientados a la generación y conservación de copias de seguridad mediante almacenamiento local, medios externos y servicios de almacenamiento en la nube. No obstante, se identificó la necesidad de fortalecer la documentación y trazabilidad de las verificaciones periódicas sobre la ejecución y efectividad de los respaldos, de manera que se cuente con evidencia suficiente que permita demostrar la realización de las pruebas y controles establecidos.

Finalmente, respecto de la redundancia de las comunicaciones, se evidenció que la infraestructura tecnológica dispone de mecanismos de balanceo y conectividad con diferentes proveedores de servicios de internet. Sin embargo, durante la revisión se identificó que las acometidas físicas de fibra óptica no cuentan con una diversidad de rutas que permita garantizar la independencia física de las conexiones. Esta condición se evidenció con un evento ocurrido en mayo de 2026, durante el cual un corte físico de fibra óptica en el exterior de las instalaciones generó una interrupción de los servicios informáticos por un periodo de hasta cuatro (4) horas, evidenciando la necesidad de fortalecer la redundancia física de las rutas de comunicación.

4. OBSERVACIONES

El presente proceso de auditoría se desarrolló tomando como base una lista de chequeo estructurada de cuarenta y cinco (45) preguntas, la cual se adjunta como anexo al presente documento (Anexo 1). Dicha lista contó con una matriz de evaluación que permitió calificar cada criterio bajo los parámetros establecidos para la revisión, considerando la aplicación de los procedimientos, la existencia de soportes documentales y las observaciones derivadas de la evaluación. Con el fin de garantizar la trazabilidad, transparencia y un adecuado soporte documental, se implementó una carpeta en la plataforma Google Drive. En este espacio digital se organizó de manera individual la documentación correspondiente a cada una de las preguntas evaluadas, permitiendo la carga y organización de las evidencias suministradas por el área auditada. La documentación recopilada constituye el soporte de los resultados obtenidos durante el desarrollo de la auditoría y permite evidenciar las actividades de verificación realizadas por la Oficina de Control Interno.

A continuación, se adjunta el enlace de acceso a la carpeta de evidencias para su respectiva revisión y consulta: https://drive.google.com/drive/folders/15RooSag_fbKNimlqwtBTdp3Ka9ncenBT?usp=sharing

5. RECOMENDACIONES Y OPORTUNIDADES DE MEJORA

Con el propósito de fortalecer la gestión de la información TIC, mejorar las condiciones de seguridad y disponibilidad de la infraestructura tecnológica, y promover la continuidad y mejora de los servicios tecnológicos institucionales, se presentan las siguientes recomendaciones derivadas de los aspectos identificados durante la revisión:

- Se recomienda fortalecer la gestión y mantenimiento de la infraestructura física del Datacenter, estableciendo un esquema formal de mantenimiento preventivo y correctivo de los sistemas de climatización y aire acondicionado de precisión, con personal o proveedores que cuenten con la competencia técnica requerida. Lo anterior, con el fin de garantizar condiciones ambientales adecuadas para la operación de los servidores y demás equipos tecnológicos, reducir la posibilidad de interrupciones asociadas a condiciones térmicas y asegurar la disponibilidad de la infraestructura crítica.
- Se recomienda fortalecer la gestión de la infraestructura tecnológica y de seguridad informática, priorizando la actualización o migración del controlador de dominio central ZIPADC, actualmente soportado sobre Windows Server 2003, hacia una plataforma con soporte vigente y condiciones de seguridad acordes con las necesidades institucionales. De igual manera, se recomienda evaluar técnicamente la disposición o sustitución del servidor físico HP ProLiant DL380 G5 y fortalecer la administración centralizada de las políticas de seguridad mediante el Directorio Activo, incluyendo controles para restringir la instalación y ejecución de software no autorizado.
- Se recomienda fortalecer el seguimiento y ejecución de las actividades establecidas en los instrumentos de planeación de TI, especialmente las correspondientes al Plan de Seguridad de la Información y al PETIC de la vigencia 2026, cuyos cronogramas registran un avance físico acumulado del 0,0 % a la fecha de corte de la revisión. Para ello, se sugiere establecer responsables, fechas de ejecución y mecanismos periódicos de seguimiento que permitan verificar el cumplimiento de las actividades programadas y registrar oportunamente los avances y soportes en la plataforma Almera SGI.
- Se recomienda fortalecer la documentación y trazabilidad de los controles asociados a la seguridad de la información y las copias de respaldo, particularmente en lo relacionado con la revisión de cuentas de acceso remoto VPN, seguimiento de registros de eventos de seguridad, control de

accesos al Datacenter, campañas de sensibilización y verificación de la ejecución y efectividad de los backups. Lo anterior, procurando que las actividades realizadas cuenten con los respectivos registros, actas, planillas o soportes que permitan evidenciar su ejecución y facilitar el seguimiento posterior.

- Se recomienda fortalecer la redundancia física de las conexiones de comunicaciones de la entidad, complementando los mecanismos de redundancia lógica actualmente disponibles mediante el balanceador de carga y los diferentes canales de conectividad. Para ello, se sugiere evaluar conjuntamente con los proveedores de servicios de telecomunicaciones la viabilidad técnica de disponer de rutas físicas de fibra óptica independientes, de manera que la falla o interrupción de un enlace o de un tramo de infraestructura no genere una afectación simultánea sobre las demás conexiones. Esta medida contribuiría a reducir los puntos únicos de falla y fortalecer la continuidad y disponibilidad de los servicios de comunicación, considerando la interrupción ocasionada por el corte de fibra óptica registrado durante mayo de 2026.

EL ÁREA AUDITADA NO PRESENTÓ CONTROVERSIA FRENTE A LAS RECOMENDACIONES FORMULADAS, POR LO CUAL ESTAS SE MANTIENEN EN EL PRESENTE INFORME FINAL.

6. TABLA CONSOLIDADA DE RECOMENDACIONES ACEPTADAS

Ítem	Recomendaciones
1.	Se recomienda fortalecer la gestión y mantenimiento de la infraestructura física del Datacenter, estableciendo un esquema formal de mantenimiento preventivo y correctivo de los sistemas de climatización y aire acondicionado de precisión, con personal o proveedores que cuenten con la competencia técnica requerida. Lo anterior, con el fin de garantizar condiciones ambientales adecuadas para la operación de los servidores y demás equipos tecnológicos, reducir la posibilidad de interrupciones asociadas a condiciones térmicas y asegurar la disponibilidad de la infraestructura crítica.
2.	Se recomienda fortalecer la gestión de la infraestructura tecnológica y de seguridad informática, priorizando la actualización o migración del controlador de dominio central ZIPADC, actualmente soportado sobre Windows Server 2003, hacia una plataforma con soporte vigente y condiciones de seguridad acordes con las necesidades institucionales. De igual manera, se recomienda evaluar técnicamente la disposición o sustitución del servidor físico HP ProLiant DL380 G5 y fortalecer la administración centralizada de las políticas de seguridad mediante el Directorio Activo, incluyendo controles para restringir la instalación y ejecución de software no autorizado.

- | | |
|----|---|
| 3. | Se recomienda fortalecer el seguimiento y ejecución de las actividades establecidas en los instrumentos de planeación de TI, especialmente las correspondientes al Plan de Seguridad de la Información y al PETIC de la vigencia 2026, cuyos cronogramas registran un avance físico acumulado del 0,0 % a la fecha de corte de la revisión. Para ello, se sugiere establecer responsables, fechas de ejecución y mecanismos periódicos de seguimiento que permitan verificar el cumplimiento de las actividades programadas y registrar oportunamente los avances y soportes en la plataforma Almera SGI. |
| 4. | Se recomienda fortalecer la documentación y trazabilidad de los controles asociados a la seguridad de la información y las copias de respaldo, particularmente en lo relacionado con la revisión de cuentas de acceso remoto VPN, seguimiento de registros de eventos de seguridad, control de accesos al Datacenter, campañas de sensibilización y verificación de la ejecución y efectividad de los backups. Lo anterior, procurando que las actividades realizadas cuenten con los respectivos registros, actas, planillas o soportes que permitan evidenciar su ejecución y facilitar el seguimiento posterior. |
| 5. | Se recomienda fortalecer la redundancia física de las conexiones de comunicaciones de la entidad, complementando los mecanismos de redundancia lógica actualmente disponibles mediante el balanceador de carga y los diferentes canales de conectividad. Para ello, se sugiere evaluar conjuntamente con los proveedores de servicios de telecomunicaciones la viabilidad técnica de disponer de rutas físicas de fibra óptica independientes, de manera que la falla o interrupción de un enlace o de un tramo de infraestructura no genere una afectación simultánea sobre las demás conexiones. Esta medida contribuiría a reducir los puntos únicos de falla y fortalecer la continuidad y disponibilidad de los servicios de comunicación, considerando la interrupción ocasionada por el corte de fibra óptica registrado durante mayo de 2026. |

7. CONCLUSIÓN

La gestión de la información TIC cuenta con una estructura de controles y procedimientos que permite soportar la operación tecnológica de la Red Samaritana, evidenciándose mecanismos relacionados con la administración de infraestructura, gestión de usuarios, protección de los equipos, licenciamiento, atención de requerimientos, copias de seguridad y seguridad perimetral. Estos elementos constituyen una base para mantener la disponibilidad y continuidad de los servicios tecnológicos y mitigar riesgos asociados al manejo de la información.

No obstante, se identificaron aspectos que requieren fortalecimiento, principalmente en los componentes relacionados con la infraestructura crítica, actualización tecnológica, ejecución de los instrumentos de planeación, conectividad y trazabilidad de los controles de seguridad. En particular, las condiciones ambientales del Datacenter requieren mecanismos de mantenimiento especializado que permitan prevenir afectaciones sobre los equipos y garantizar condiciones adecuadas para su operación.

En materia de infraestructura tecnológica, se evidenció la existencia de equipos con tecnologías obsoletas, como el servidor de dominio ZIPADC que opera sobre Windows Server 2003. Esta condición limita la disponibilidad de actualizaciones y mecanismos de soporte de seguridad asociados a la plataforma, por lo que resulta pertinente avanzar hacia una plataforma con soporte vigente y limita la capacidad de implementar mecanismos de seguridad acordes con las necesidades actuales, por lo que resulta necesario avanzar hacia plataformas soportadas y fortalecer la administración centralizada de políticas de seguridad.

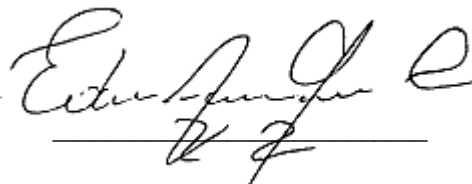
Respecto de la planeación tecnológica y de seguridad de la información, se observa una brecha entre las actividades programadas y su ejecución y/o registro en los instrumentos institucionales. Esta situación limita el seguimiento efectivo, la medición de avances y la trazabilidad de las acciones previstas, especialmente frente a controles relacionados con seguridad, acceso remoto, monitoreo, infraestructura y protección de la información.

De igual manera, si bien existen mecanismos para la realización de copias de seguridad y controles asociados a la protección de la información, se requiere fortalecer su documentación, seguimiento y evidencia de ejecución y efectividad. La trazabilidad de estas actividades resulta fundamental para demostrar la operación periódica de los controles y su capacidad de respuesta ante eventos que puedan comprometer la disponibilidad o integridad de la información.

En cuanto a la conectividad y disponibilidad del servicio de Internet, se cuenta con mecanismos de redundancia mediante diferentes proveedores; sin embargo, la afectación presentada en mayo, asociada a un corte físico de fibra que generó una interrupción de hasta cuatro horas, evidencia que la redundancia lógica o

la disponibilidad de varios operadores no elimina completamente el riesgo cuando existen dependencias de infraestructura física. Por lo anterior, resulta necesario continuar fortaleciendo la diversidad de las rutas de comunicación y reducir los posibles puntos comunes de falla que puedan afectar simultáneamente los servicios de conectividad.

En términos generales, la gestión TIC presenta una base operativa y de control que soporta los servicios tecnológicos institucionales; sin embargo, el fortalecimiento de la infraestructura crítica, la actualización de componentes tecnológicos, la ejecución y trazabilidad de la planeación, la gestión de respaldos y la diversificación física de la conectividad permitirá reducir la exposición a riesgos tecnológicos y mejorar las condiciones de disponibilidad, integridad, seguridad y continuidad de la información y de los servicios institucionales.



EDWIN ALCIDES GONZALEZ COY
JEFE OFICINA ASESORA DE CONTROL INTERNO

8. ANEXOS

Anexo 1. Lista de Chequeo

E.S.E. HOSPITAL UNIVERSITARIO DE LA SAMARITANA					SAM				
CONTROL INTERNO									
LISTA DE CHEQUEO									
R05CIN01-V1					05GIC92-V1				
FECHA DE AUDITORIA:					TURCOS				
OBJETIVO:					Evaluar la eficacia de la gestión de tecnologías de la información mediante auditorías internas, verificando los controles sobre la seguridad de la información, la confiabilidad de los datos, la administración de accesos y la integridad de los datos, con el fin de asegurar la disponibilidad, confiabilidad y confiabilidad de la información durante la vigencia 2025.				
RESPONSABLE DEL AREA:					Luis Augusto Olave Palacios - Líder Gestión De La Información-Sistemas				
ITEM		CUMPLE	NO CUMPLE	NO APLICA	OBSERVACIONES				
1	¿El área de sistemas cuenta con inventario actualizado de los equipos de la institución? Adjunte los reportes correspondientes.	X							
2	¿El área de sistemas cuenta con Plan Estratégico de tecnologías de la información y comunicaciones? Adjunte el PTEC.	X							
3	¿El área de sistemas cuenta con banca del aplicativo Dinamica General Hospitalaria? Adjunte los reportes correspondientes.	X							
4	¿Los equipos del hospital cuentan con antivirus licenciado? Indique el porcentaje y adjunte los reportes correspondientes.	X							
5	¿El área de sistemas cuenta con el plan de tratamiento de riesgos de seguridad y privacidad de la información? Anexe el Plan e indique y certifique el porcentaje de avance a la fecha.	X							
6	¿El área de sistemas cuenta con el Plan de seguridad y privacidad de la información. Anexe el Plan e indique y certifique el porcentaje de avance a la fecha.	X							
7	¿Los servidores de la institución cuentan con el funcionamiento de sistema operativo? Indique el porcentaje de funcionamiento y certifique.	X							
8	¿El área de sistemas cuenta con el cronograma de mantenimiento para los equipos de cómputo? Anexe el Cronograma y la ejecución a la fecha.	X							
9	¿El área de sistemas cuenta con reportes de capacitación en el software dinámico general? Anexe los reportes correspondientes.	X							
10	¿El área de sistemas cuenta con mesa de ayuda para copias en la institución? ¿Es proceso de encuesta documentado? ¿Tiene cronograma de programación? Adjunte las evidencias.	X			Anexo PTEC, E, B, B, B, B				
11	¿El área de sistemas cuenta con medio de comunicación para publicaciones en la página web? ¿Envía las cuentas al personal evaluado, la entidad pública en su sitio web oficial, en la sección "Transparencia y acceso a la información pública" la siguiente información:	X							¿El área de sistemas realiza las publicaciones en la
12	1. Mecanismos para reportar (PQRS).	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
13	2. Localización física, sucursales y registros, horarios y días de atención al público.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
14	3. Funciones y labores de la entidad.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
15	4. Organigrama de la entidad.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
16	5. Derechos de información de servidores públicos, empleados y contratistas en relación a SUSP.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
17	6. Identidad general de la entidad.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
18	7. Clases de la entidad (Programas, servicios, trámites y otros procedimientos administrativos).	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
19	8. Políticas de seguridad de la información del sitio web protección de datos personales.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
20	9. Clases de empleo.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
21	¿La entidad contó con un proceso de identificación de infraestructura crítica, la aplicó y comunicó los resultados al personal evaluado? Adjunte los reportes correspondientes.								https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
22	¿Indique el porcentaje de datos abiertos actualizados y difundidos respecto del total de datos estadísticos identificados en el periodo evaluado.								https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
23	¿Indique el porcentaje de trámites y Otros Procedimientos Administrativos (OPA) en línea de la entidad que cuentan con actualización de usuarios respecto del total de trámites y servicios en línea, para el periodo evaluado. Adjunte los evidencias.								https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
24	¿Cuántos equipos de cómputo, ¿cantidad control con un formulario en su página web para la recepción de comentarios, quejas, reclamos y denuncias? Adjunte las evidencias.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
25	¿El área de sistemas cuenta con software de base de datos licenciado? Adjunte las evidencias.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
26	¿El área de sistemas cuenta con servidor firewalls para la protección y manejo de reglas de seguridad? Adjunte los reportes correspondientes.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
27	¿El área de sistemas cuenta con un servidor de correo para evitar instalación de software no permitido? Adjunte las evidencias.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
28	¿El área de sistemas cuenta con correo corporativo para uso institucional? Adjunte las evidencias.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
29	¿El área de sistemas cuenta con procedimientos de backup de la base de datos propia? Anexe el Procedimiento.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
30	¿El área de sistemas cuenta con un servidor externo para el registro de la información? Anexe reportes y características.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
31	¿El área de sistemas cuenta con herramientas para monitorear la red? Cuáles? Describa brevemente.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
32	¿Existen lugares de acceso restringido, explique cuáles, y el porqué.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
33	¿Se cuenta con infraestructura para garantizar y salvaguardar los servidores de la institución? Adjunte reportes.								https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
34	¿La instalación eléctrica se realizó específicamente para el centro de cómputo? Adjunte reportes.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
35	¿Se tiene contrato de mantenimiento para los equipos que proporcionan el control ambiental? Anexe el contrato.	X							https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
SEGUIMIENTO A LA MATRIZ DE RIESGOS DEL PROCESO									
36	¿Cuenta con la evidencia y los reportes que demuestran que se está realizando seguimiento continuo a los riesgos propios del proceso y los riesgos de control identificados en la matriz de riesgos institucionales?								https://www.hus.gov.co/portal/seguridad-informacion/quejas-y-sugerencias
CONCEPTO GENERAL Y/O RECOMENDACIONES:									