Al contestar por favor cite:2023110002145-1

Bogotá, 2 de marzo de 2023

Ingeniero
LUIS AUGUSTO OLAYA PALACIOS
Subdirector de Sistemas
CLAUDIA YADIRA CIFUENTES SOSA
Líder Almacén
E.S.E. HOSPITAL UNIVERSITARIO DE LA SAMARITANA
E. S. D.

Ref.: Informe final Auditoria verificación de cumplimiento y normas en materia de derechos de autor sobre software 2022

Cordial saludo.
Adjunto informe de Auditoria de la referencia para su conocimiento y se otorgan 5 días (jueves 9 de marzo de 2023), para él envió del correspondiente Plan de Mejoramiento, conforme lo establece el procedimiento Formulación, seguimiento y cierre de Plan Único de Mejora por Procesos - PUMP con código de documento#02GC03-V7.

Atentamente,

YETICA JHASVELLI HERNANDEZ ARIZA
Jefe Oficina de Control Interno

cc. Dr. EDGAR SILVIO SANCHEZ VILLEGAS.- Gerente
cc.Dra. SANDRA ELIANA RODRIGUEZ GARCIA - Directora Administrativa

INFORME DE VERIFICACIÓN DE CUMPLIMIENTO DE LAS NORMAS EN MATERIA DE DERECHOS DE AUTOR RELACIONADA CON EL SOFTWARE 2022

1. ASPECTOS GENERALES

OBJETIVO

Verificar el cumplimiento de la normatividad establecida en cuanto a la protección de Derechos de Autor sobre el uso del SOFTWARE en la E.S.E. Hospital Universitario de la Samaritana vigencia 2022.

ALCANCE

De acuerdo a lo establecido en la Directiva presidencial y Circulares externas con respecto a los Derechos de Autor, el consejo asesor del gobierno nacional en materia de control interno expidió la circular 04 de 2006 mediante la cual solicita a los representantes legales y Jefes de la oficina de Control Interno de las entidades de carácter nacional y territorial, la información relacionada con la verificación, recomendaciones y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre SOFTWARE.
Teniendo en cuenta lo anterior se establece la presentación del informe de ley, bajo el cumplimiento de las normas, el licenciamiento del SOFTWARE y conforme al Plan de Auditorías Internas Independientes 2022 de la oficina de Control Interno de la E.S.E. Hospital Universitario de la samaritana.

METODOLOGIA

Con el Memorando No. 005 de 01 de febrero se da inicio a la VERIFICACIÓN DE CUMPLIMIENTO Y NORMAS EN MATERIA DE DERECHOS DE AUTOR SOBRE SOFTWARE 2022.
Mediante oficios radicados a la Subdirección de Sistemas y al Líder de Proyecto de Almacén se solicitó la información correspondiente a la verificación de cumplimiento de las normas en materia de derechos de autor, relacionada con el software de la vigencia 2022; la articulación del informe de Derechos de autor con el modelo integrado de planeación y gestión - MIPG y Acreditación; correos electrónicos precisando el alcance y aplicabilidad del Manual de seguridad informática.
Para la verificación se realizó verificación en campo de una muestra de sesenta equipos de cómputo, el 7.6% del total del hardware instalado en la E.S.E. Bogotá, verificación que contó con el apoyo absoluto de la subdirección de sistemas.
Una procesada la información es cotejada, analizada y verificada y con los resultados se construye el presente informe y se registra y rinde todo lo referente a la DNDA, informe que fue rendido el pasado 17 de febrero de 2022,

BASE LEGAL

- ✓ CONSTITUCIÓN POLÍTICA.
- ✓ Ley 603 de 2000 Software legal Directiva Presidencial No. 01 de febrero de 1999
- ✓ Directiva Presidencial No. 02 de febrero de 2002
- ✓ Circular No. 04 de diciembre de 2006 de la Unidad Administrativa Especial Dirección Nacional de Derechos de Autor
- ✓ Circular Externa No. 12 de febrero de 2007 de la Unidad Administrativa Especial Dirección Nacional de Derechos de Autor
- ✓ Circular Externa No. 017 de junio de 2011 de la Unidad Administrativa Especial Dirección Nacional de Derechos de Autor
- ✓ LEY 87 de 1993, establece que todas las entidades públicas, debían organizar e implementar sus propios procedimientos de evaluación y autoevaluación, con miras a garantizar la integralidad y efectividad en el ejercicio de las funciones y el buen uso de los recursos públicos.
- ✓ LEY 1273 de 2009, Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.
- ✓ LEY 1474 de 2011, Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- ✓ Decreto 1499 de 2017 Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015
- ✓ Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. •
- ✓ Decreto 1008 del 14 de junio de 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
- ✓ Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
- ✓ Ley 1266 de 2008 Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- ✓ Ley 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- ✓ Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento de la Función Pública.
- ✓ Norma ISO 27001 - Gestión de la seguridad de la información, y su Anexo

ELEMENTOS ESTRATEGICOS

OBJETIVOS

El acuerdo No. 027 de agosto de 2022, por medio del cual aprueba la nueva plataforma estratégica 2021 - 2024; el mapa de procesos y el modelo de atención de la E.S.E. Hospital Universitario de la Samaritana,

establece en el Artículo primero la aprobación de ocho (8) objetivos estratégicos, alineados a cinco (5) perspectivas: Social, cliente, financiera, procesos internos, crecimiento y aprendizaje y se ha priorizado dándoles un peso porcentual a cada uno; en el Artículo cuarto registra una transición de seis (6) meses contados a partir de la **promulgación** del Acuerdo, para su implementación. Transcurrido este plazo su aplicación e implementación será un documento integrador en la entidad y base para la Evaluación por dependencias.
Dado lo que establece el Artículo Cuarto, la presente Evaluación por dependencias se desarrolla basada en los seis (6) objetivos estratégicos vigentes a 31 de diciembre de 2022; objetivos que dentro de lo publicado en el sistema de gestión de Calidad integrado – ALMERA no se evidencian medición alguna.

Los objetivos estratégicos de la E.S.E. Hospital Universitario de la Samaritana que respaldan los logros del quehacer institucional en materia de software son:

- ✓ Fortalecer la Prestación de Servicios de Salud - dentro de las competencias asignadas en el modelo de red Departamental.
- ✓ Garantizar un Sistema de Información - integral, eficiente y eficaz
- ✓ Fortalecer el Sistema Integrado de Gestión de la Calidad - que permita conformar Centros de Excelencia.

POLITICA

La E.S.E., cuentas con diez y seis (16) políticas institucionales, la política Institucional de la presente Auditoria señala:

"COMUNICACIÓN ADECUADA, EN EL MOMENTO ADECUADO, POR LA VIA ADECUADA"

'El Hospital se compromete a desarrollar procesos confiables y adecuados de generación, análisis y archivo de la información, que permitan la toma de decisiones oportunas y coherentes con las metas institucionales; promoviendo una cultura de comunicación transparente y veraz hacia los diferentes grupos de interés a través de los medios disponibles'. Código del documento 01DE12-V1, elaborada y aprobada el 31/01/2018

MODELO INTEGRADO DE PLANEACION Y GESTION – MIPG

El Modelo Integrado de Planeación y Gestión MIPG es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio[1]. De la evaluación realizada a Diciembre de 2021 se destacan:

De la 3ª. Dimensión: Gestión con valores para resultados (puntaje de resultado 70.6) se derivan las Políticas de Gestión y Desempeño Institucional: **POL 06 – GOBERNO DIGITAL[2] y POL07- SEGURIDAD DIGITAL.**
El índice de la política de gestión y desempeño POL 06 – GOBERNO DIGITAL contiene un índice de resultado 81.3, el mayor puntaje obtenido en las políticas Institucionales de 2021.

[1] Decreto 1083 de 2015 ARTÍCULO 2.2.22.3.2. *Definición del Modelo Integrado de Planeación y Gestión MIPG.*
[2] La Política de MIPG - Gobierno Digital es la política que busca promover el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones -TIC, para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.

Siendo esta una política transversal se relaciona con las demás políticas del MIPG, facilitando su implementación y potenciando los beneficios tanto para la E.S.E., como para los servidores públicos, usuarios y sus familias.

Con los resultados de la política se generaron cincuenta y ocho recomendaciones[3] para su respectivo plan de mejora y/o actividad de mejora a esta política; la actividad de mejora reportada por el subdirector de sistemas de la E.S.E. es: '*Se realizó el proceso de actualización del catálogo de sistemas de información (documento de catálogo de sistemas de información)'* y se *'realizo el proceso de actualización del Directorio de elementos de infraestructura de TI (documento de directorio de infraestructura TI)*'.

Política POL07- SEGURIDAD DIGITAL4 de la 3ª. Dimensión, con un índice de resultado de 69.4

El Comité Institucional de Gestión y Desempeño debe articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de esta política. Para ello, se debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área transversal que haga parte de la Alta Dirección[5]. Esta política contiene veinte (20) recomendaciones[6], para esta política, la actividad de mejora reportada por el subdirector de sistemas de la E.S.E. es: *'Se realizaron campañas de concientización en temas de seguridad de la información (soportes campañas de videos, fondos de pantalla)'*.

De la 5ª Dimensión: Información y Comunicación registra un índice de la gestión de desempeño de 72.4 para la E.S.E., se localiza la política de **POL09 - TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y LUCHA CONTRA LA CORRUPCIÓN**[7] con un índice de la política del 72.6 y noventa y cinco (95) recomendaciones para dar cumplimiento, la E.S.E. tiene la obligación de divulgar activamente la información pública sin que medie solicitud alguna (transparencia activa); así mismo, tienen la obligación de responder de buena fe, de manera adecuada, veraz, oportuna y gratuita a las solicitudes de acceso a la información pública (transparencia pasiva), lo que a su vez conlleva la obligación de producir o capturar dicha información[8]. De las recomendaciones establecidas en la Evaluación de desempeño institucional 2022, la E.S.E. ha desarrollado: *'Seguimiento trimestral a las publicaciones realizadas en la página WEB para dar cumplimiento a la ley 1712'*

De las recomendaciones establecidas para esta política, como Elaborar y actualizar los documentos de arquitectura de los desarrollos de software de la entidad (17) y definir e implementar una metodología de

---

[3] se destacan dentro de las recomendaciones establecidas por MIPG para la E.S.E., para el presente informe las siguientes:

- Elaborar y actualizar los documentos de arquitectura de los desarrollos de software de la E.S.E. (16)
- Definir e implementar una metodología de referencia para el desarrollo de software y sistemas de información (17).
- Definir un proceso de construcción de software que incluya planeación, diseño, desarrollo, pruebas, puesta en producción y mantenimiento (19).

[4] Con la política se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia.

[5] Manual Operativo MIPG versión 4 Marzo 2021.

[6] algunas de las recomendaciones establecidas para la E.S.E. en esta política son: ° Fomentar la promoción de los espacios para capacitar a los líderes de los procesos y sus equipos de trabajo sobre la metodología de gestión del riesgo con el fin de que sea implementada adecuadamente entre los líderes de proceso y sus equipos de trabajo, por parte del comité institucional de coordinación de control interno (1). efectuar evaluaciones de vulnerabilidades informáticas (18). ° Establecer un procedimiento de gestión de incidentes de seguridad de la información, formalizarlo y actualizarlo de acuerdo con los cambios de la entidad (17) ° Actualizar los mapas de riesgos de la entidad de acuerdo a los resultados del monitoreo o seguimiento (3). ° Establecer controles para evitar la materialización de riesgos de seguridad y privacidad de la información (2).

[7] Esta política le permite a la entidad articular acciones para la prevención, detección e investigación de los riesgos de en los procesos de la gestión administrativa y misional de las entidades públicas, así como garantizar el ejercicio del derecho fundamental de acceder a la información pública a los ciudadanos y responderles de buena fe, de manera adecuada, veraz, oportuna y gratuita a sus solicitudes de acceso a la información pública.

[8] Manual Operativo MIPG versión 4 Marzo 2021

referencia para el desarrollo de software y sistemas de información (18), no se observa ninguna acción y/o actividad de mejora.

Condición

Dadas las recomendaciones generadas en la Evaluación de Desempeño Institucional , No hay evidencia de la instauración de actividades y/o acciones de mejora para subsanar las recomendaciones.

Criterio

- Circular Externa No. 12 de febrero de 2007 DNDA
- Circular Externa No. 017 de junio de 2011 DNDA
- Decreto No. 1499 de 2014
- Decreto 1083 de 2015

Causa

Debilidad En El Cumplimiento De Las Recomendaciones tales como:

a) definir y e implementar una metodología de referencia para el desarrollo del software y sistemas de información;

b) fomentar la capacitación a los líderes y a sus equipos de trabajo en cuanto la seguridad de la información; c) efectuar evaluaciones informáticas; d) elaborar un procedimiento de incidentes de seguridad de la información;

e) fortalecer la información cualitativa y cuantitativa en seguridad de la información lo que permitirá establecer oportunamente alertas de seguridad en la información.

Efecto

Falta de conocimiento y capacitación por parte de los servidores públicos en general en cuanto a las estrategias implementadas, las herramientas y contenidos en cuanto al software que posee la E.S.E.

Probabilidad de exposición de la seguridad de los datos, cuando los datos de los cuales es responsable la E.S.E., en cabeza de los servidores públicos están expuestos a continuos riesgos, que si se materializan generan incidentes de seguridad, hechos que dan lugar a la vulneración de la confidencialidad, disponibilidad o integridad de los datos, a la SEGURIDAD DIGITAL y a la política de GOBERNO DIGITAL.

ACREDITACIÓN

Al Subdirector de Sistemas como líder del **Estándar de gestión de la información,** se le solicitó mediante oficio radicado No. 2023110000959-1 con referencia: 'Articulación informe DNDA con MIPG y ACREDITACIÓN, a lo cual se recibe la siguiente respuesta:

- Estándar 144: *Código I3: 'Se cuenta con un sistema de información integral y confidencialidad disponible ALMERA, que cubre la necesidad de obtención de datos de la organización y la generación de informes para la toma de decisiones. De igual forma, se establecieron indicadores asistenciales de satisfacción al usuario, asistenciales, administrativos y financieros, que son presentados en comités directivos, donde se realizan los respectivos análisis y se convierten en fuente de información para la toma de decisiones.*

  Diseño de cuadro de mando de GESTION DIRECTIVA donde se definieron indicadores que le apuntan a los objetivos estratégicos del hospital.

  Se realizan análisis trimestrales de los indicadores trazadores de calidad de la resolución 256 en reuniones de comité directivo de donde se generan acciones de mejora en los casos en que se han presentado desviaciones en el resultado de los mismos en comparación con el meta establecido en la ficha de cada uno de los indicadores.

  Se realiza seguimiento a los indicadores mediante reuniones interdisciplinarias que lidera la Dirección científica donde se realiza la revisión de los datos, así como la evaluación de la calidad de los mismos a partir de los reportes estandarizados publicados en DGH para generación de informes asistenciales –

Resolución 408 de 2018 ministerio de salud y protección social para la evaluación del informe anual sobre el cumplimiento del plan de gestión institucional'.

- Estándar 145 *Código G14 'Dentro de la planeación y la identificación de necesidades se estima la adquisición de software, hardware y el mantenimiento de acuerdo al manual de contratación, logrando robustecer, mejorar y mantener la infraestructura informática (Elaboración y publicación del plan anual de adquisiciones 02GBS07) (identificación necesidades de información 05GIS44)'.*
- Estándar 146 *Código G15 'La institución cuenta con un Manual de seguridad de información cuyo objetivo es preservar. Proteger y asegurar la información del HUS definiendo reglas, contraseñas, creación y asignación de cuentas, inactivación y activación de cuentas, uso de antivirus, responsabilidad en el uso de equipos informáticos, control de acceso a la red de datos entre otras.*
  SE cuenta con un procedimiento de Back ups en donde se determina la periodicidad, las copias en medios electrónicos y físicos y los mecanismos de almacenamiento de los medios de Back ups.
  SE cuenta con una oficina de gestión documental, encargada de la estandarización, implementación y evaluación de la información de la organización, a fin de garantizar la seguridad y confidencialidad de la misma.
  Se cuenta con la matriz de información actualizada definiendo los índices de información clasificada y reservada con criterio de confidencialidad de acuerdo a los parámetros establecidos en la ley 1712 de2014 –ley de transparencia y del derecho al Acceso de información.
  El plan institucional de archivos - PINAR instrumento archivístico de Gestión Documental establece el seguimiento y articulación de la planeación estratégica con la función archivística.
  Convalidación de las TRD Y TVD de la entidad ante el Consejo Departamental del archivo de la Gobernación de Cundinamarca, se realizó inscripción en el registro Único de series documentales RUSD ante el archivo General de la Nación.
  Se cuenta con un archivo centralizado del área de Estadística donde se tiene la custodia, consulta y acceso restringido a los expedientes físicos de la historia clínica.
  Indicador de seguridad: Porcentaje de cumplimiento en la realización de back ups programados. – Porcentaje de ataques informáticos que afectan el sistema de información'.
- Estándar 147 *Código G16: Se t cuenta con un sistema de información DGH que integra la información asistencial, financiera y administrativa de la entidad con facilidad de acceso.*
  Se cuenta con nuevos mecanismos de información basados en el sistema de historia clínica electrónica en donde se integran aspectos administrativos y asistenciales como es el caso del aplicativo egresos, el cual es de fácil acceso para el personal asistencial y administrativo en donde se realiza el control en tiempo real de los egresos diarios que se emiten por servicios, el aplicativo ayuda a realizar la trazabilidad del proceso desde el momento que es emitida la salida por parte medica en el sistema hasta el momento de emisión de la boleta de salida (paz y salvo) por parte de facturación, esta medición nos ha permitido mejorar los tiempos de4 respuesta para agilización del proceso de egreso del paciente y mejorar la oportunidad de asignación de las camas.
  Se cuenta con un APP disponible para los sistemas Android o IOS, en la cual contamos con acceso en tiempo real al censo de urgencias, hospitalización, UCI, UCIntermedio, salas de recuperación, que permite la localización más fácil para las especialidades interconsultantes y acceso de información básica de los pacientes; adicionalmente el APP cuenta con la información de las interconsultas por especialidad que se encuentran pendientes, esto mejora la oportunidad de notificación a las especialidades interconsultantes.
  Se cuenta con diseño de interfaces entre aplicativos (DGH) hacia los aplicativos de apoyo diagnostico (LABCORE, PATCORE, PAXS-RIS) que permite la visualización de las solicitudes realizadas por parte del personal asistencial o administrativo y visualización de su posterior resultado.
  Diseño de aplicativo por parte del área de sistemas respecto a las necesidades de cada servicio'.
- Estándar 149 *Código G18 'Se cuenta con DGH que integra información asistencial, financiera y administrativa en la entidad con facilidad y acceso.*

Se cuenta con un sistema de información integral y confidencial disponible ALMERA que cubre la necesidad y obtención de datos..... De igual forma se establecieron indicadores asistenciales de satisfacción....'

RIESGOS

Dentro de las matrices de riesgos institucionales III trimestre 2022 y matriz de riesgos de corrupción, publicadas en el sitio WEB de la E.S.E., se evidencia que la gestión de riesgos de seguridad de la información es limitada

MATRIZ DE RIESGOS DE CORRUPCION

Esta matriz de riesgos de corrupción de la vigencia 2022, cuenta con once (11) riesgos de corrupción[9], no se identifican riesgos de corrupción transversales a los procesos institucionales, se identifica del proceso de gestión de la información un riego de corrupción: POSIBILIDAD DE ACCESO INDEBIDO A LOS SISTEMAS DE INFORMACIÓN PAR EL USO NO APROPIADO DE INFORMACION CONTENIDA EN LOS SISTEMAS EN FENECIMIENTO PROPIO O UN TERCERO; tiene como única causa '*que los controles existentes son insuficientes*', la zona de riesgo inherente está en ALTO y los controles establecidos son: a) procedimiento de retiro de talento humano – actividad 1, b) Manual de seguridad informática, c) Inducción y entrenamiento en puesto de trabajo -actividad 6 y 7, d) control de préstamos documentales; aplicados y valorados los controles la zona de riesgos residual continua siendo ALTO.

MATRIZ DE RIESGOS INSTITUCIONALES III TRIMESTRE 2022

La matriz de riesgos institucionales III trimestre 2022 de la E.S.E., del proceso de gestión d la información registra el siguiente Riesgo:
'POSIBILIDAD DE PÉRDIDA DE INFORMACIÓN DEL HUS Y SUS SEDES DEBIDO AL INADECUADO MANEJO DE LOS SISTEMAS DE INFORMACIÓN E INCONSISTENCIA EN LA EJECUCIÓN DE LOS PROCEDIMIENTOS PARA EL MANEJO DE LA DOCUMENTACIÓN'.

PROCESO	CAUSA / CAUSA RAIZ	DESCRIPCIÓN DEL CONTROL	DESCRIPCIÓN DEL RIESGO
GESTIÓN DE LA INFORMACIÓN	Manejo inadecuado de los archivos durante su ciclo vital, gestión, control e histórico.	- Procedimiento Estadístico de Egreso hospitalario actividades 1, 6, 12 - Procedimiento entrada y salida de historia clínica al archivo actividades 1, 3, 4 y 5.	Posibilidad de Perdida y del HUS y sus sedes debido al inadecuado manejo de los sistemas de información e

[9] *POSIBILIDAD DE QUE POR ACCIÓN U OMISIÓN, SE USE EL PODER PARA DESVIAR LA GESTIÓN DE LO PUBLICO HACIA UN BENEFICIO PRIVADO"*

PROCESO	CAUSA / CAUSA RAIZ	DESCRIPCIÓN DEL CONTROL	DESCRIPCIÓN DEL RIESGO
	Posibles ataques cibernéticos	- Procedimiento Custodia y acervo documental actividades 7 y 8. - Manual de organización del Acervo Documental. - Manual de seguridad Informática.	inconsistencia en la ejecución de los procedimientos para el manejo de la documentación'.
	Daños en los servidores		

Fuente: Matriz Institucional de riesgos 2021

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 fisicos, ley 594 de 2000, la tercera causa encauzada a el hardware utilizado y solo la segunda causa esta 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 de la 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 publica, entre otros.

Criterio

- Decreto No. 1499 de 2014
- Decreto 1083 de 2015

Causas

Debilidad en el tratamiento de los riesgos de seguridad de la información y sus controles asociados.

Efectos

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.

CONTROLES CRIPTOGRÁFICOS

La Criptografía (Kriptos=ocultar, Graphos=escritura) o texto cifrado[10], se pueden utilizar como un **control añadido que proporciona confidencialidad, autenticidad, no repudio y autenticación**.

Respecto a los controles criptográficos para el desarrollo de la presente auditoria se ha preguntado a la subdirección de sistemas – proceso de gestión de la información lo siguiente:

[10] el cifrado es el **proceso de codificación de la información**.

Los soportes de uso de códigos y controles para las aplicaciones, sistemas de información de firmas digitales de los funcionarios expuestos públicamente; quien es el administrador de los mismos y el inventario; cual es el procedimiento, protocolo o guía referente a los procesos de creación, renovación, recuperación y eliminación de estos códigos y controles.

Respuesta:

- Actualmente se cuenta con Firma Digital mediante la empresa (CERTICÁMARA) solamente para el Gerente y esta es administrada directamente desde el área de gerencia.
- Adicionalmente también se realiza todo el proceso de renovación periódica el cual es tramitado y soportado directamente en gerencia.

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 llaves[11] y controles criptográficos.

Criterios

- 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.

EL MANUAL DE SEGURIDAD INFORMATICA

Del proceso de GESTION DE LA INFORMACION se verifico:

Código de documento	NOMBRE/ DESCRIPCION	FECHA APROBACIÓN	OBSERVACIONES
01GIS07-V2	MANUAL - SEGURIDAD INFORMATICA	Diciembre de 2019	Una herramienta de consulta que promueva la seguridad informática, garantizando la **integridad, la confidencialidad, la disponibilidad y la irrefutabilidad** de la información. En su contenido, conforme es un Manual expone e ilustra el uso del sitio Web, correo electrónico, virus informáticos, normas de seguridad y administración del proceso de gestión de la información.

Fuente: Sistema de Gestión de la calidad Integrado - ALMERA

Verificado el Manual de Seguridad Informática se preguntó a la Subdirección de Sistemas lo siguiente:

- **Preguntado**: Dentro del alcance está el establecer medidas y patrones técnicos de administración; cuáles han sido las medidas del seguimiento y evaluación al cumplimiento de la seguridad de la información.
  Respuesta: Se tiene implementado en el aplicativo ALMERA el indicador (PORCENTAJE DE ATAQUES INFORMÁTICOS QUE AFECTAN EL SISTEMA DE INFORMACIÓN en el cual se registran los respectivos ataques informáticos que son registrados mediante el Firewall que tiene implementado la entidad.

[11] "Gestión de llaves" anexo A de la norma ISO 27001

- En el Manual Seguridad Informática se registra: Del numeral 7.7. **Del Contenido página WEB e INTRANET del HUS: El material que aparezca publicado en la página de Internet del Hospital deberá ser enviado aprobado por el Comité de Comunicaciones, la Gerencia y a la Proceso de Gestión de la información, respetando la propiedad intelectual. - El material que aparezca en la Intranet del hospital deberá ser aprobado por el líder del material a publicar y de acuerdo con las normas y procedimientos establecidos...**
  Preguntado: cuales son los criterios aplicados para las publicaciones en cada uno de los link; y suministro de las copias de las actas del Comité 2022.
  Respuesta: Para esta publicaciones no se cuenta con un comité, Se realiza mediante las solicitudes de soporte realizadas al área de comunicaciones ya que el área de comunicaciones es responsable de la administración de las secciones de la página, Adicionalmente dentro de las actividades específicas del área de comunicaciones pero se realiza seguimiento trimestral respecto al cumplimento de publicaciones de la ley 1712 (Ley Transparencia y Acceso a la Información), y dentro del cual se realiza notificación a cada una de las áreas responsables de la información la actualización de cada ítem de ser necesario.
  En el Manual Seguridad Informática se registra: numeral 7.7.

- En el Manual Seguridad Informática se registra del numeral 7.11. **Auditoría del software instalado**: El proceso de gestión de la información y la oficina de Control Interno son **los responsables de realizar revisiones periódicas para asegurar que solo el software con licencia este instalado en los computadores del hospital.**
  ... Corresponderá al proceso de gestión de la información y a la oficina de Control Interno *dictar* las normas procedimientos y calendaros de auditoria
  Preguntado los soportes de las verificaciones realizadas por el líder del proceso de Gestión de la información, como responsable de las revisiones periódicas para asegurar que solo el software con licencia esté instalado. de la información.
  Respuesta: Dentro del proceso de mantenimiento preventivo realizado por el área de sistemas en cada una de sedes se realiza la verificación del software instalado en cada equipo de cómputo y su validación con el respectivo licenciamiento, adicionalmente se programa actividad de verificación con acompañamiento de Control Interno para el día viernes 17 en horas de la mañana (Anexa listado de equipos instalados para sacar muestra y realizar respectiva revisión).

- El Manual Seguridad Informática se registra: Del numeral 7.12 **Software propiedad de la Institución:** todo el software adquirido por el hospital sea por compra, donación, o sesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera. El proceso **de gestión de la información en coordinación con la a oficina asesora de Control Interno deberá tener un registro de todo el software propiedad del hospital....**
  Preguntado: se solicita el Inventario de registro de todo el software y fichas de propiedad de la E.S.E. y/o propiedad intelectual.
  Respuesta:

NOMBRE APLICATIVO	LENGUAJE	TIPO	ESTADO
CITAS WEB	.NET	WEB	PRODUCCIÓN
AUTORIZACIONES	LARAVEL	WEB	PRODUCCIÓN
PROCESO EGRESOS	LARAVEL	WEB	PRODUCCIÓN
ENTREGA TURNO	LARAVEL	WEB	PRUEBAS

NOMBRE APLICATIVO	LENGUAJE	TIPO	ESTADO
DESMATERIALIZADOR	.NET	ESCRITORIO	PRODUCCION
ORDHUS	VISUAL BASIC	ESCRITORIO	DESHABILITADO
DOCENCIA	.NET	WEB	PRODUCCION
OPAGOS	VISUAL BASIC	ESCRITORIO	PRODUCCIÓN

- El Manual Seguridad Informática se registra Numeral 7.13 Uso **del Software Académico Software:** Cualquier Software que requiera ser instalado para trabajar sobre la red del hospital deberá ser evaluado por el proceso de Gestión de la información y deberá ser usado exclusivamente para asuntos relacionados con las actividades de la institución
  Preguntado: se solicita el Inventario de registro de todo el software Académico, de uso exclusivo para asuntos relacionados con las actividades de la E.S.E.
  Respuesta: Se realizó la validación con el área de educación médica y se encontraron los siguientes aplicativos:

NOMBRE APLICATIVO	UTILIDAD	ESTADO
Saberes	Permite el registro de los médicos que rotan en el HUS	OPERATIVO
Biteca	biblioteca virtual	IMPLEMENTACIÓN

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 INFORMÁTICOS QUE AFECTAN EL SISTEMA DE INFORMACIÓN), más 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; QUE 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.
- numeral 7.11. **Auditoría del 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 le 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, auditor 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 orientará, 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 para prevenir, detectar y corregir las desviaciones que se presenten al interior y que puedan afectar el logro de sus objetivos. Y como mecanismos de verificación y evaluación del control interno se utilizarán las auditorias generalmente aceptadas por la normatividad.
  Ahora bien con lo anterior Control interno no es responsable de realizar revisiones y menos dictar las normas 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 en el inventario de software solicitado para la realización de la presente Auditoria..
- Numeral 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.

INVENTARIO DEL SOFTWARE Y HARDWARE

1. HARDWARE

El inventario de equipos de cómputo de la E.S.E. por sedes es el siguiente:

PRODUCTO/ NOMBRE	BOGOTA	S UFZ	S HRZ	TOTAL INVENTARIO 2022
COMPUTADOR PORTATIL	169	20	25	214
EQUIPO DE COMPUTO (ESCRITORIO)	828	222	205	1255
EQUIPO TABLET	33	10	0	43
SERVIDOR	20	4	1	25
TOTAL	1050	256	231	1537

Fuente: Subdirección de sistemas y : Modulo de Inventarios DGH

- De los inventarios de hardware de la E.S.E. Hospital Universitario de la Samaritana, suministrados por la Subdirección de Sistemas, corresponden a la Bogotá, en donde se localiza la Dirección, se ejecuta la Gestión misional, financiera y administrativa, el 68.31%; a la sede Unidad Funcional Zipaquirá el 16.63% y a la sede Hospital Regional Zipaquirá el 15.03%.
- La información de los inventarios suministrada por la líder de proyecto de almacén y contenida en el módulo de DGH y verificada, registra la misma información suministrada por la subdirección de sistemas.
- En la vigencia 2022 se adquirieron 209 equipos de cómputo, conformados por: - 66 COMPUTADOR PORTATIL, 139 EQUIPO DE COMPUTO (ESCRITORIO) y 4 EQUIPO TABLET.
- Mediante resolución No. 354 de 08 de agosto de 2022 por la cual se dan de baja algunos activos fijos, dentro de los que se encuentran once (11) equipos portátiles y dos (2) CPU, conforme al procedimiento de baja de activos fijos.

2. SOFTWARE

El software instalado en los equipos, contenido en el módulo de DGH y suministrado por la subdirección de sistemas y que se encuentra debidamente licenciado está compuesto por:

Suministrada la información por las fuentes a las que fue solicitada la información, es cotejada y comparada con el mismo inventario a diciembre de 2022, como sigue:

EL SOFTWARE INSTALADO EN ESTOS EQUIPOS DE LA E.S.E.

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.

Son soportes del software instalado en la E.S.E. los documentos de la información solicitada y suministrada a la subdirección de sistemas y a la líder de proyecto de almacén y con la verificación al software, realizada el día 17 de febrero, junto con la subdirección de sistemas; de acuerdo a la base de datos suministrada por la subdirección que contiene 785 hardware, a través de números aleatorios se obtuvo una muestra del 7.6% (60 equipos) y se realizó uno a uno su verificación.

DEBIDAMENTE LICENCIADO

Suministrada la información por las fuentes a las que fue solicitada la información, es cotejada y comparada con el mismo inventario a diciembre de 2022, como sigue:

- La E.S.E. registra un total de nueve mil ciento veintiuna (9121) licencias de software, cotejado con el documento radicado 2023403001086-1 de la Subdirección de sistemas y que hacen parte de la presente Auditoria en el Anexo No. 1.
- La vigencia de la LICENCIA DE ANTIVIRUS ESET ENDPOINT SECURITY es anual, por lo tanto se adquiere en cada vigencia, en la vigencia 2022 se adquirieron 1600 licencias de antivirus ESET ENDPOINT SECURITY. Todas estas licencias contienen número de placa en el inventario suministrado. Las licencias de antivirus ESET ENDPOINT SECURITY de 2019, 2020 y 2021, en total identificadas con número de placa son: tres mil cien (3.100), de las cuales están ubicadas por unidades, en BOGOTA dos mil quinientos cincuenta (2.550) y sede HRZ quinientas cincuenta (550).
- 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 han exceptuando aquí las licencias de antivirus ESET ENDPOINT SECURITY de 2019, 2020, 2021 y 2022).
- El software debidamente licenciado se encuentra dispuesto por ubicación así:

DESCRIPCION	NÚMERO DE LICENCIAS	PORCENTAJE DE PARTICIPACION
E.S.E. HOSPITAL UNIVERSITARIO DE LA SAMARITANA - BOGOTA	3977	87,97%
sede HOSPITAL REGIONAL ZIPAQUIRA	529	11,70%
sede UNIDAD FUNCIONAL ZIPAQUIRA	15	0,33%
TOTAL 2022	4521	

Fuente: Líder Proyecto Almacén - módulo de DGH

DE PROPIEDAD DE LA E.S.E. HOSPITAL UNIVERSITARIO DE LA SAMARITANA

El software de propiedad de la E.S.E., inventariado e informado por la Subdirección de sistemas fichas de propiedad de la E.S.E. y/o propiedad intelectual es:

NOMBRE APLICATIVO	LENGUAJE	TIPO	ESTADO
CITAS WEB	.NET	WEB	PRODUCCIÓN
AUTORIZACIONES	LARAVEL	WEB	PRODUCCIÓN
PROCESO EGRESOS	LARAVEL	WEB	PRODUCCIÓN
ENTREGA TURNO	LARAVEL	WEB	PRUEBAS
DESMATERIALIZADOR	.NET	ESCRITORIO	PRODUCCION
ORDHUS	VISUAL BASIC	ESCRITORIO	DESHABILITADO
DOCENCIA	.NET	WEB	PRODUCCION
OPAGOS	VISUAL BASIC	ESCRITORIO	PRODUCCIÓN

Fuente: Subdirección de sistemas

EL SOFTWARE ACADÉMICO

El Inventario identificado de registro de todo el software Académico, de uso exclusivo para asuntos relacionados con las actividades de la E.S.E. es:

NOMBRE APLICATIVO	UTILIDAD	ESTADO
SABERES	Permite el registro de los médicos que rotan en el HUS	OPERATIVO
BITECA	biblioteca virtual	IMPLEMENTACIÓN

EL SOFTWARE LIBRE DE USO EN LA E.SE.

Aun cuando el Manual de seguridad informática establece: en el numeral 7.11. **que solo el software con licencia este instalado en los computadores del hospital,** se evidencio que de uso general y corriente se encuentran instalados SOFTWARE LIBRES entre los que se evidenciaron:

- CDBurnerXP
- Cisco Webex Meetings
- Go to Opener
- Go To Meeting
- Zoom
- Entre otros

OTRO SOFTWARE DE USO EN LA E.S.E.

Son de uso en la E.S.E., el SOFTWARE no identificado como licenciado, de propiedad de la E.S.E. de uso académico, los siguientes:

- EVOLUCION
- Google Chrome
- Intranet
- ORFEO

- Mesa de ayuda
- Sistema de Gestión de calidad integrado ALMERA
- LABCORE - PATCORE
- Camas
- Controlador de Gráficos
- Amazon Redshift ODBC
- Any Desk
- Appeom Multibrowser Plug-in
- Bonjour
- Crystal Reports 2008
- MAVU
- VALIDADOR RIPS IPS
- Sistema de Cifrado y firmado de archivos ADRES
- ZIMBRA, MOODLE,
- entre otros.

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
  - De propiedad de la E.S.E. Hospital Universitario de la Samaritana
  - El SOFTWARE académico
  - El SOFTWARE libre de uso en la E.SE.
  - 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 placa individual, las LICENCIAS DE ANTIVIRUS ESET 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).

INFORME DIRECCION NACIONAL DE DERECHOS DE AUTOR

Para dar cumplimiento a lo establecido por la Dirección Nacional de Derechos de Autor, en las circulares expedidas para tal fin, la E.S.E. Hospital Universitario de la Samaritana, presentó el informe correspondiente, el día 17 de febrero de 2023, la información rendida es como sigue:

EMPRESA SOCIAL DEL ESTADO HOSPITAL UNIVERSITARIO DE LA SAMARITANA
Bogota D.C. (Bogotá)

Le informamos que luego de verificar en nuestros archivos, se encontró que efectivamente el 17-02-2023 usted remitió ante la Dirección Nacional de Derecho de Autor, con éxito el informe de software legal, con los siguientes datos:

Orden	Territorial
Sector	Salud
Departamento	Bogotá
Municipio	Bogota D.C.
Entidad	EMPRESA SOCIAL DEL ESTADO HOSPITAL UNIVERSITARIO DE LA SAMARITANA
Nit	8999990325
Nombre funcionario	YETICA J HERNANDEZ ARIZA
Dependencia	OFICINA DE CONTROL INTERNO
Cargo	JEFE OFICINA CONTROL INTERNO
1.Con cuantos equipos cuenta la entidad	1537
2. El software se encuentra debidamente licenciado?	Si

MINISTERIO DEL INTERIOR	
3. ¿Qué mecanismos de control se han implementado para evitar que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva?	ACTUALMENTE SE CUENTAN CON LAS SIGUIENTES POLITICAS IMPLEMENTADAS PARA RESTRINGIR LA INSTALACION DE APLICATIVOS POR PARTE DE LOS USUARIOS EN LOS EUIPOS DE COMPUTO: -DIRECTORIO ACTIVO. - RESTRICCIÓN DESDE EL DIRECTORIO ACTIVO - APLICA A LOS USUARIOS Y EQUIPOS CONECTADOS AL DOMINIO HUS.CO; PARA LA INSTALACION DE SOFTWARE. - FILTRADO DE CONTENIDO FIREWALL. - SE TIENE CONFIGURADO LA RESTRINCIÓN DE LA DESCARGA E INSTALACION POR INTERNET DE SOFTWARE NO LICENCIADOS Y SOFTWARE MALICIOSOS. - SE CUENTA CON UNA CONSOLA DE ADMINISTRACIÓN DE ANTIVIRUS PARA EL BLOQUEO DE EJECUTABLES PARA LA INSTALACIÓN DE SOFTWARE Y ANALISIS DE VIRUS INFORMATICOS.
4. ¿Cuál es el destino final que se le da al software dado de baja en su entidad?	DEBIDO A QUE LAS LICENCIAS CORRESPONDEN A UN INTAGIBLE, PARA ESTO SE GENERA EL DOCUMENTO DE SALIDA (BAJA) . ESTE ES VALIDADO POR PARTE DEL COMITE DE INVENTARIOS, COMO ESTA DEFINDIDO EN EL PROCEDIMIENTO 02GBS11- BAJA DE ACTIVOS FIJOS Y ESTAS SON DESINTALADAS DE LOS EQUIPOS DE COMPUTO POR PARTE DEL PERSONAL DE SISTEMAS.

YETICA HERNANDEZ A.
Jefe Oficina Control Interno

MARIA CLARA MARTINEZ R.
Profesional Especializado

Bogotá, febrero 21 de 2023

Ruta: Profesional Especializado/ Dirección Nacional de derechos de autor/ INFORME SOFTWARE 2022.doc

Anexo No. 1

SOFTWARE INSTALADO EN ESTOS EQUIPOS DEBIDAMENTE LICENCIADO

CODIGO PRODUCTO	PRODUCTO/ NOMBRE	BOGOTA	HRZ	UFZ	TOTAL 2022
197007002	AMORTIZACION LICENCIAMIENTO SOLUCION WEBSENSE WEB FILTER	2			2
197007003	LICENCIA RIMAGE ROBOT OPTION FOR CD DIRECT	1			1
197007004	LICIENCIAS ADD 1 TAPE DRY ARCHIVE AGENT	1			1
197007005	LICENCIA WORK FLOW MANAGER SW LESS THAN 25K EXAMS PER YEAR	1			1
197007006	LICENCIA PACS 11.3 SW MEDIA-BACKOFFICE SRVRS	2			2
197007007	LICENCIA STREAMING SITE LICENSE LESS 25K EXAMS PER YEAR	8			8
197007008	LICENCIA DBR F/SWFM TEST WFM OR RSF	2			2
197007009	LICENCIA VIRTUAL READING BASIC SW WORKGROUP FOR LAR BUNDLEF	4			4
197007010	LICENCIA VOLUME MATCHING F/ VIRTUAL READ	2			2
197007011	LICENCIA SATELLITE RSF/15K EXAMS/YR	1			1
197007012	LICENCIA DBR WFM/IMS <300K EX/YR	1			1
197007013	LICENCIA 3D ANALY OPT FOR VIRTUAL READING	2			2
197007014	LICENCIA MAMMOGRAPHY FEATURE/ FOR KODAK DV CR CLASSID/ELITE	1			1
197007015	LICENCIA LAR - RIS ENTERPRISE SW < 100 K EX/YR	2			2
197007016	LICENCIA VTL SITE LICENSE< 50K EX/YR	1			1
197007017	LICENCIA VTL SITE LICENSE ADD 25K EX/YR	2			2
197007018	LICENCIA CLUSTER KIT WINDOWS SERVER 2003 ENT	1			1
197007019	LICENCIA RIS OPTION SCANNING <250K/YR	1			1
197007020	LICENCIA WORK FLOW MANAGER SW ADDITIONAL 25K EXAMS PER YEAR	7			7
197007021	LICENCIA VTL SITE LICENSE ADD 100K EX/YR	1			1
197007022	LICENCIA VOICE RECOGNITION OPTION 2.1 SHARED USER LICENSE	5			5
197007023	LICENCIA VUE MOTION UNLIMITED LICENSE & NBSP	1			1
197007024	LICENCIA VUE MOTION UNLIMITED LSW<50K EX/YR	1			1
197007025	LICENCIA CARESTREAM RIS WEB SERVICES DATABASE REGISTRY LICEN	1			1
197007026	LICENCIA VUE MOTION UNLIMITED LICENSE FOR EXISTING SOFTWARE	1			1
197007027	LICENCIA MS WORD FOR USE IN CSH SOLUTIONS	7			7
197007028	LICENCIA DBR WFM/IMS CS/CLSTR < 300K EX/YR	1			1
197007029	LICENCIA TRANSCRIPTION KIT FOR CARESTREAM RIS	3			3
197007030	LICENCIA IMS DATA REPOSITORY <200K ENTRIES	1			1
197007031	LICENCIA ADD TAPEDRY ARCHIVE AGENT 2 CPU WINTEL 1	1			1
197007032	LICENCIA SOFTWARE DE QUEMADO DE CDS COMPATIBLE CON EPSON PP1	5			5

CODIGO PRODUCTO	PRODUCTO/ NOMBRE	BOGOTA	HRZ	UFZ	TOTAL 2022
197007033	LICENCIA DE USO PROGRAMA DINAMICA GERENCIAL	1			1
197007034	LICENCIAS MICROSOFT OFFICE ESTANDAR	189	20	ND	209
197007035	LICENCIAS DE VMWARE Y VCENTER PARA 8 CORES	1			1
197007037	LICENCIA OFFICE	63	44	0	107
197007038	SOLUCIÓN SOFTWARE DE CONTROL DE ACCESO	1			1
197007039	LICENCIA ACROBAT PROFESIONAL 9.0	3			3
197007040	LICENCIA AUTOCAD 2008	1			1
197007041	LICENCIA AVAYA EXTENSIONES UNIVERSAL	103			103
197007042	LICENCIA DE SOFTPHONE AVAYA	5			5
197007043	LICENCIA DE TRONCAL ADICIONAL AVAYA	38			38
197007044	LICENCIA DE TRONCAL IP AVAYA	10			10
197007045	LICENCIA EXCHANGE SERVER - STANDARD 2007	1			1
197007046	LICENCIA FOREFRONT THREAT MANAGEMENT	1			1
197007047	LICENCIA LIFESIZE UVC MULTIPOINT	1			1
197007048	LICENCIA MICROSOFT OFFICE PLUS 2010	15		ND	15
197007049	LICENCIA MICROSOFT OFFICE PROFESSIONAL 2003	450		ND	450
197007050	LICENCIA MICROSOFT VISIO 2007	5			5
197007051	LICENCIA PROJECT SERVER DEVICE PROFESSIONAL 2007	2			2
197007052	LICENCIA PROJECT SERVER - USER CAL 2007	15			15
197007053	LICENCIA PROJECT SERVER 2007	1			1
197007054	LICENCIA SHAREPOINT 2007	1			1
197007055	LICENCIA SOFTWARE DE ADC BASICO PARA AGENTES AVAYA	100			100
197007056	LICENCIA SPSS	1			1
197007057	LICENCIA SQL - USER CAL 2005	500			500
197007058	LICENCIA SQL SERVER - ENTERPRISE 2005	2			2
197007059	LICENCIA SQL SERVER - STANDARD 2005	6			6
197007060	LICENCIA SQL SERVER ENTERPRISE CORE 8 2012	2			2
197007061	LICENCIA SYSTEM CENTER CONFIGURATION MANAGER CLIENT ML 2012	15			15
197007062	LICENCIA SYSTEM CENTER STANDARD 2012	1			1
197007063	LICENCIA SYSTEM MANAGEMENT SERVER - ENTERPRISE 2003	1			1
197007064	LICENCIA SYSTEM MANAGEMENT SERVER - ENTERPRISE W/ SQL 2003	1			1
197007065	LICENCIA SYSTEM MANAGEMENT SERVER CLIENT ML	500			500
197007066	LICENCIA VISUAL STUDIO PROFESSIONAL WITH MSDN PROFESSIONAL 2008	5			5
197007067	LICENCIA WINDOWS 7 X CAJA 7 PROFESSIONAL	114		ND	114
197007068	LICENCIA MICROSOFT WINDOWS SERVER CAL	1500	400	ND	1900
197007069	LICENCIA WINDOWS SERVER 2003	11			11
197007070	LICENCIA WINDOWS SERVER	3	4	0	7

CODIGO PRODUCTO	PRODUCTO/ NOMBRE	BOGOTA	HRZ	UFZ	TOTAL 2022
197007071	LICENCIA WINDOWS TERMINAL SERVER - DEVICE CAL 2003	50			50
197007072	LICENCIA WINDOWS XP	81			81
197007073	LICENCIA WORD FLOW MANEGER SW LESS	1			1
197007074	LICENCIA ADICIONAL DE EXTENSIÓN UNIVERSAL AVAYA	7			7
197007075	LICENCIA UVF SOFTPHONE	8			8
197007076	LICENCIA DE ANTIVIRUS ESET ENDPOINT SECURITY 2019	1750	0	0	1750
197007077	LICENCIA AUTOCAD LT		2		2
197007078	LICENCIA CONCURRENTE AMOVIL	25			25
197007079	LICENCIA AMSI	4			4
197007080	LICENCIA WINDOWS TERMINAL SERVER - DEVICE CAL 2008	25			25
197007081	LICENCIA OFFICE STANDARD 2019		83	ND	83
197007082	SOFTWARE NETWORK VIDEO RECORD SOPORTA 32 CANALES APP-2000-32		3		3
197007083	SOFTWARE SISTEMA CCTV		1		1
197007084	SOFTWARE MONITOREO CCTV		1		1
197007085	LICENCIA DE ANTIVIRUS ESET ENDPOINT SECURITY 2020	1250	0	0	1250
197007086	LICENCIA SISTEMA PERIMETRAL CHECKPOINT	1			1
197007087	LICENCIA SOFTWARE T-DIGITAL-SERVIDOR	1			1
197007088	LICENCIA SISTEMA DE TELEMETRIA Y HOSTING	1			1
197007089	LICENCIA ZOOM PRO	3	0		3
197007090	LICENCIA ZOOM WEBINAR ADD ON	1	0		1
197007091	LICENCIA WORKSPACE BUSINESS STARTER	1	0		1
197007092	LICENCIA SISTEMA DE ROTACIONES UNIVERSITARIAS	1			1
197007094	LICENCIA MSC ONE BUNDLE UNIVERSITY	1			1
197008001	SOFTWARE DGH.NET 3.5	1	0	ND	1
197008002	LICENCIA VITALICIA SOFTWARE DE GESTION KAWAK	1			1
197008003	SISTEMA DE INFORMACIÓN DE TELECONSULTA SINCRONICA Y ASINCRONICA	1	ND	ND	1
197008004	SOFTWARE DE GESTION DE MANTENIMIENTO (S.G.M.)	1	2	ND	3
197008006	SOFTWARE GESTION DE TECNOLOGIAS NOPBS UPC	1	1	ND	2
197008007	SOFTWARE PARA EQUIPOS DE OFTALMOLOGIA	1			1
197008008	SOFTWARE MONITOREO DEL SISTEMA CONTRA INCENDIO		1		1
197008009	SOFTWARE GRAPHNET TS NEONATAL RETROFIT	3			3
	LICENCIA DE ANTIVIRUS ESET PROTECT ADVANCED 2022	1600	ND	ND	1600