Bogotá, D.C. Marzo 11 de 2024

Ingeniero
LUIS AUGUSTO OLAYA PALACIOS
Subdirector de Sistemas
E.S.E. Hospital Universitario de la Samaritana
E. S. D.

REFERENCIA: Informe Auditoría Verificación de cumplimiento y Normas en materia de Derechos de Autor sobre Software 2023.

Cordial Saludo:

Adjunto se envía Informe de Auditoría de la referencia para su conocimiento, el cual se realizó para dar cumplimiento a lo establecido en el Plan de Auditorías Independientes de la vigencia 2024

Por lo anterior para que dentro de los cinco (5) días hábiles siguientes se elabore el Plan de Mejoramiento pertinente de acuerdo a las recomendaciones descritas, Plan de Mejoramiento, el cual deberá ser elaborado conforme lo establece el procedimiento identificado con Código 02AC01-V1, Actividad 21 y al Instructivo "Lineamiento Oportunidades de Mejora", Código 06GIC03-V2 y siguiendo los lineamientos enmarcados en el procedimiento "FORMULACIÓN, SEGUIMIENTO Y CIERRE DEL PLAN ÚNICO DE MEJORA POR PROCESOS, identificado con código 02GIC03-V10 .

Nota: Anexo doce (12) Folios

Cordialmente;

YETICA JHASVELLY HERNANDEZ ARIZA
Jefe Oficina Asesora de control Interno

c.c. Edgar Silvio Sánchez Villegas - Gerente

EMPRESA SOCIAL DEL ESTADO HOSPITAL UNIVERSITARIO DE LA SAMARITANA
NIT. 899.999.032-5

INFORME DE VERIFICACIÓN DE CUMPLIMIENTO DE LAS NORMAS EN MATERIA DE DERECHOS DE AUTOR RELACIONADA CON EL SOFTWARE VIGENCIA 2023

INFORME DE AUDITORÍA

Bogotá D.C, MARZO DE 2024

HUS
HOSPITAL UNIVERSITARIO DE LA SAMARITANA
EMPRESA SOCIAL DEL ESTADO

INDICE

1. ASPECTOS GENERALES

1.1. OBJETIVO DE LA AUDITORÍA

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 2023.

1.2. ALCANCE DE LA AUDITORÍA

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 2024 de la Oficina Asesora de Control Interno de la Empresa Social del Estado Hospital Universitario de la Samaritana.

1.3. METODOLOGIA DE LA AUDITORÍA

Con el Memorando No.04 de Marzo 8 se da inicio a la VERIFICACIÓN DE CUMPLIMIENTO Y NORMAS EN MATERIA DE DERECHOS DE AUTOR SOBRE SOFTWARE 2023.
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 2023; 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.

1.4. 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 -** Unidad Administrativa Especial Dirección Nacional de Derechos de Autor
- **Circular Externa No.12 de febrero de 2007 -** Unidad Administrativa Especial Dirección Nacional de Derechos de Autor
- **Circular Externa No. 017 de junio de 2011 -** 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 -** Departamento de la Función Pública.
- **Norma ISO 27001 -** Gestión de la Seguridad de la Información, y su Anexo

2. ELEMENTOS ESTRATÉGICOS

2.1. OBJETIVOS ESTRATÉGICOS

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 1°, 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 4°, 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 4°, la presente Evaluación por Dependencias se desarrolla basada en los ocho (8) Objetivos Estratégicos vigentes a 31 de diciembre de 2023; 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:

Objetivo Estratégico No.3. Fortalecer la integralidad y efectividad en la prestación de los servicios de alta complejidad a través de la articulación de las redes integradas de atención que incremente los niveles de satisfacción y experiencia del servicio, generando valor para el usuario y familia.

Objetivo Estratégico No.4. Fortalecer el desempeño de la gestión clínica en respuesta a las necesidades de la población, haciendo énfasis en los grupos vulnerables.

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.6. Incrementar la generación de conocimiento e innovación a través del desarrollo del modelo integral de Docencia e Investigación, que produzca impacto social en la consolidación institucional como Hospital Universitario.

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

3. POLÍTICA

La E.S.E., cuentas con diecinueve (19) Políticas Institucionales, la Política Institucional de la presente Auditoria "POLÍTICA DE GESTIÓN DE LA INFORMACIÓN Y COMUNICACIONES" 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'. Cuyo Código del documento es 01DE12-V1, elaborada y aprobada el 31/01/2018

4. RIESGOS

Dentro de las matrices: Matriz de Riesgos Institucionales 2023 V2 y Mapa de Riesgos SICOF (Corrupción, Opacidad y Fraude) 2024, publicadas en el sitio WEB de la E.S.E., se evidencia que la Gestión de Riesgos de seguridad de la información es limitada.

4.1. MAPA DE RIESGOS SICOF (Corrupción, Opacidad y Fraude) 2024

Mapa de Riesgos SICOF (Corrupción, Opacidad y Fraude) 2024, cuenta con catorce (14) Riesgos de Corrupción[1], 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 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; tiene las siguientes causas: *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,* la zona de riesgo está en EXTREMO y los controles establecidos son: a) El líder de cada áreas o proceso debe radicar en el área de sistemas el formato de inactivación de usuarios para que el profesional de área de sistemas encargado realice la inactivación del usuario a los diferentes sistemas de información a los cuales tenía acceso, b) El profesional de sistemas que realiza la creación del usuario verifica dentro del formato de activación de usuarios debe asignar el rol descrito dentro del formato el cual cuenta con los permisos asignados y formalizados por cada uno de los líderes de área, c) El profesional de sistemas encargado de la administración del directorio activo realiza la parametrización de la definición de tiempo de caducidad, longitud y demás características para la creación de las contraseñas de acceso a los equipos de cómputo, d) El

[1] El objetivo del SICOF es **Prevenir, controlar y mitigar los riesgos de corrupción, opacidad y fraude**. Busca establecer mecanismos efectivos para detectar y reportar actos irregulares y garantizar la transparencia en las entidades vigiladas"

Ingeniero de Sistemas encargado de la consola de administración de antivirus realiza la restricción de los accesos a dispositivos extraíbles según lo definido en el (Manual de Seguridad Informática).

4.2. MATRIZ DE RIESGOS INSTITUCIONALES 2023 V2

La Matriz de Riesgos Institucionales 2023 V2 de la E.S.E., del proceso de Gestión de 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	CAUSAS ASOCIADAS
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. - Procedimiento Custodia y acervo documental actividades 7 y 8. - Manual de organización del Acervo Documental. - Manual de seguridad Informática.	Manejo inadecuado de los archivos durante su ciclo vital: gestión, central e histórico. Daños en los servidores
	Posibles ataques cibernéticos		
	Daños en los servidores		

Fuente: Matriz de Riesgos Institucionales 2023 V2

5. INVENTARIO DEL SOFTWARE Y HARDWARE

Mediante comunicado 2024110002466 y 2024110002664 de fecha marzo 8 de 2024 se solicitó informe de verificación de las normas en materia de Derechos de Autor relacionada con los Software 2023 a la Subdirección de Sistemas y al Almacén General, dando respuesta la Subdirección de Sistemas, donde se relacionaron lo siguiente:

- **¿CON CUÁNTOS EQUIPOS CUENTA LA ENTIDAD?**

El inventario de equipos de cómputo de la E.S.E. por sedes es el siguiente de acuerdo a comunicado de respuesta por parte de la Subdirección de Sistemas:

PRODUCTO/ NOMBRE	BOGOTA	S UFZ	S HRZ	TOTAL INVENTARIO 2022
COMPUTADOR PORTATIL	169	20	25	214
EQUIPO DE COMPUTO (ESCRITORIO)	828	233	208	1269
EQUIPO TABLET	33	10	0	43
SERVIDOR	26	4	1	31
TOTAL	**1050**	**256**	**231**	**1557**

Fuente: Subdirección de Sistemas 2024

- **¿EL SOFTWARE INSTALADO EN ESTOS EQUIPOS SE ENCUENTRA DEBIDAMENTE LICENCIADO?**

Actualmente todo el software que se encuentra instalado en los equipos de cómputo se encuentra licenciado, por parte del área de sistemas no se realiza instalación de software sin su respectiva licencia.

- **¿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 los siguientes procesos implementados 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 el cual es administrado por el área de sistemas.

Filtrado de Contenido (Firewall)

Se tiene configurado la restricción de la descarga e instalación por Internet de software e licenciados y software malicioso.

Antivirus

Se cuenta con una consola de administración de antivirus para el bloqueo de ejecutables para la instalación de software y análisis de virus informáticos.

- **¿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 activo 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 debe tener en cuenta que alguna de las licencia son adquiridas por un tiempo específico las cuales se desactivan y no se debe realizar ningún proceso de desinstalación para el caso que se requiera estas son desinstaladas de los equipos de cómputo por parte del personal de sistemas.

6. RECOMENDACIONES

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 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 pública, 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.

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 llaves[2] 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.

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

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 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.

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
  - 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).

SOLICITUD: *Las Recomendaciones registradas anteriormente en este Informe de Auditoria, que requieran Plan de Mejoramiento, deben quedar plasmadas conforme se enuncian, no deben ser modificados de manera total ni parcialmente.*

El Código Único Disciplinario, Ley 734 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 reforma 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 es de carácter institucional, la verificación se realiza a información mínima publicada en el sitio WEB de propiedad de la EMPRESA SOCIAL DEL ESTADO HOSPITAL UNIVERSITARIO DE LA SAMARITANA e Intranet, si bien es cierto que la información está bajo la responsabilidad de cada uno de los funcionarios públicos, no puede ser de carácter individual ni tampoco personal, por lo tanto las recomendaciones aquí registradas, como los planes de mejoramiento a que dé lugar esta Auditoria son de carácter institucional.

YETICA JHASVELLY HERNANDEZ ARIZA
Jefe Oficina Asesora de Control Interno

JOHN BONZA DUQUE
Profesional Universitario

Bogotá, D.C. Marzo 26 de 2024