EVALUACIÓN AL CUMPLIMIENTO DE LAS NORMAS DE DERECHOS DE AUTOR SOBRE SOFTWARE

Vigencia 2019

Directiva Presidencial 01 de 1999 y 02 de 2002 y circular 4 de 2008

OFICINA ASESORA DE CONTROL INTERNO

JULIO HERNAN VILLABONA VARGAS

Jefe Oficina Asesora de Control Interno

Bucaramanga, Marzo de 2020

TABLA DE CONTENIDO

INTRODUCCIÓN

De conformidad con las Directivas Presidenciales 01 de 1999 y 02 de 2002, relacionadas con el respeto a los derechos de autor, el Consejo Asesor del Gobierno Nacional en materia de Control Interno expidió la Circular 04 del 22 de diciembre de 2006, mediante la cual solicitó a los Representantes Legales y Jefes de las Oficinas de Control Interno de las entidades u organismos públicos del orden 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".

En consecuencia, la Dirección Nacional de Derecho de Autor (DNDA) estableció el procedimiento para el recibo, administración y custodia de dicha información. También emitió la Circular 12 del 2 de febrero de 2007, para la verificación, recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre programas de computador (software).

Posteriormente, expidió la Circular 17 del 1°de junio de 2011, por la cual modificó el numeral 2 del título III de la Circular 12 de 2007, donde se aclaran las condiciones para el recibo de la información y establece que se debe reportar la información sobre el licenciamiento del software de la entidad del año inmediatamente anterior, a través del aplicativo disponible en la página www.derechodeautor.gov.co, a más tardar el tercer viernes del mes de marzo de cada año.

Por lo anterior, la Oficina de Control Interno realizó la verificación del cumplimiento de la normatividad relacionada con el licenciamiento de software para la vigencia de 2019 en la E.S.E. Hospital Universitario de Santander, actividad incluida dentro del Plan Anual de Auditorias y aprobada mediante acta No. 001 del 26 de febrero de 2020 por el Comité Institucional de Coordinación de Control Interno.

OBJETIVO GENERAL

Establecer el cumplimiento por parte de la ESE Hospital Universitario de Santander de las normas en materia de derechos de autor sobre software.

ALCANCE

La evaluación realizada por la Oficina de Control Interno, se centró en las gestiones realizadas por el Grupo de Apoyo Tecnológico y de Información de la ESE Hospital Universitario de Santander, en relación con los equipos que cuenta la entidad tanto propios como de contratistas, software licenciados y de correo electrónico, desarrollo de software, mecanismos de control para evitar la instalación de programas no licenciados.

CRITERIOS DE EVALUACIÓN

- Directiva Presidencial 01 del 25 de febrero de 1999, sobre el respecto al derecho de autor y los derechos conexos.
- Directiva Presidencial 02 del 12 de febrero de 2002, sobre el respecto al derecho de autor y los derechos conexos en lo referente a utilización de programas de ordenador (software)

- Circular 1000-06 del 22 de junio de 2004, del Departamento Administrativo de la Función Pública, que da instrucciones de complementar el informe ejecutivo anual sobre el sistema de control interno – verificación cumplimiento normas uso de software.
- Circular 07 del 28 de diciembre de 2005, del Consejo Asesor del Gobierno Nacional en Materia de Control Interno, sobre la verificación al cumplimiento de las normas de uso de software
- Circular 04 del 22 de diciembre de 2006, del Consejo Asesor del Gobierno
- Comunicado 001 del 12 de enero de 2011, de la Dirección Nacional de Derecho de Autor, sobre la remisión de informes de Software vigencia 2010
- Circular 017 de 2011, de la Dirección Nacional de Derechos de Autor, sobre la modificación circular 12 del 2 de febrero de 2007, sobre recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre programas de computador (software).

METODOLOGIA

La evaluación se realizó mediante solicitud de información, consultas a las bases de datos, verificación documental, con la finalidad de determinar su estado frente al criterio normativo aplicable.

RESULTADOS DE LA EVALUACIÓN

SOFTWARE DE ANTIVIRUS

Se cuenta con software antivirus, con una consola de Administración que envía de forma automática las actualizaciones de Antivirus y de aniSpyware a toda la Red, permitiendo mantener actualizadas las versiones de antivirus, en cada uno de los servidores de aplicaciones y estaciones de trabajo.

Se cuenta actualmente con 470 licencias de este producto.

Se determinó que esta herramienta se encuentra activa y funcionando, constituyéndose en una herramienta efectiva de detección de virus que pueden afectar la funcionalidad de los equipos de cómputo y la seguridad del sistema de información de la entidad.

Así mismo, la Oficina de Control Interno verificó que la licencia de software que respalda el uso de software de Antivirus es ESE ENDPOINT que vence el 06 de diciembre de 2020.

SOFTWARE LICENCIADOS

LICENCIAS	Versión	Cantidad	Fecha Expiración	INSTALADAS
Office Professional	Plus 2007	21	No expira	21
Office Professional	Plus 2010	140	No expira	125
Office Standard	2007	177	No expira	161
SQL - Device CAL	2005	300	No expira	300
S|QL Server - Enterprise	2005	2	No expira	2
SQL Server Enterprise Core	2012	8	No expira	8
Fortiget 600c	5.6.3	2	2020-11-02	2
ESET ENDPOINT ANTIVIRUS	Version 6.4.2	470	2021-01-03	470
Dinámica Gerencial Fox Versión 9.0	9	1	No expira	1
Dinámica Gerencial Hospitalaria	NF 4.0	1	No expira	1
Enterprise TS	Versión	1	2020-11-01	1
Almera		100	No expira	100
Forest	4.0	1	No expira	1
CCERTIHUS	1.1	1	No expira	1
RES16	1.1	1	No expira	1
HOJAS DE VIDA COLABORADORES	1.1	1	No expira	1
MOODLE	5.3	1	No expira	1
DIRECTORIO ACTIVO	6.2	1	No expira	1
MIPRESHUS	1.3	1	No expira	1
Pagina WEB	4.9	1	No expira	1
SoporteHUS	1	1	No expira	1
UCIP	1	1	No expira	1
ATENEA	3	1	No expira	1
EPLUX	1	1	No expira	1
Gestion medica	1	1	No expira	1
HEXABAN	1.28.30.67	1	No expira	1
HIRUKO	2.13.0	1	No expira	1

Fuente: Ing. Ever Barrera Vargas - Profesional Universitario - Grupo de Trabajo Sistemas
Última Actualización: Febrero 26 DE 2020

SISTEMAS DESARROLLADOS

La ESE Hospital Universitario de Santander, cuenta con los siguientes sistemas desarrollados, de su propiedad:

1. **CCERTIHUS.** Permite tener la trazabilidad de los certificados de defunción y certificados de nacidos vivos. Está en uso.
2. **RES16.** Consulta de la Historia Clínica física. Apoya la gestión de búsqueda de Historia Clínica en Estadística. Está en uso.
3. **SISTEMA DE INFORMACIÓN DE EMPLEADOS DEL HOSPITAL UNIVERSITARIO.** Sistema de información que permite el registro de la hoja de vida del personal de apoyo de la ESE HUS. Está instalado en los servidores de la ESE HUS. Es utilizado por el área de Talento Humano.
4. **SOPORTE HUS.** Software registro de mantenimiento equipos de computo
5. **UCIP.** Software de estadística para uci pediátrica
6. **GESTIÓN MÉDICA**. Software de historia clínica

EQUIPOS DE CÓMPUTO

PROPIEDAD DE	CANTIDAD DE EQUIPOS
HUS	**518**
UNION TEMPORAL FACTURACIÓN	**70**
FET – GESTIÓN INTEGRAL	**150**
COOTRASMAR	**30**
ASISTENCIAL SALUD	**14**
SANTANDER MEDICAL GROUP	**5**
SOCIEDAD DE ONCOLOGIA Y RADIOTERAPIA	**1**
ATEK	**13**
ECOSERVIR	**3**
TOTAL EQUIPOS	**804**

Fuente: Ing. Nelly Méndez Meza - Profesional Especializado UFATI
Última Actualización: Febrero 26 DE 2020

Anexo se encuentra la información detallada de equipos de la ESE HUS. Se evidencia la revisión realizada a los equipos registrando el inventario del software instalado.

POLITICAS DE SEGURIDAD INFORMATICA

La ESE Hospital Universitario de Santander cuenta con dos políticas de tecnología, aprobadas según resolución 358 de agosto 03 de 2018, modificada en su artículo segundo por la Resolución 427 de septiembre 28 de 2018 y por la Resolución 476 de agosto 20 de 2019.

1. **POLITICA DE SEGURIDAD DIGITAL.** Donde el Gerente de la E.S.E Hospital Universitario de Santander y sus colaboradores se comprometen a implementar un sistema de gestión de seguridad de la información, estableciendo un marco de confianza en el ejercicio de sus deberes con el Estado y partes interesadas, protegiendo la información , disminuyendo el impacto generado sobre sus activos, identificando los riesgos de manera sistemática con objeto de mantener un nivel de exposición aceptable, asegurando la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés y cumpliendo con los principios de la Función Administrativa.
2. **POLÍTICA DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN.** Donde la gerencia de la ESE Hospital Universitario de Santander y sus colaboradores se comprometen a desarrollar procesos institucionales que cuenten con información segura, confiable, asertiva, cumpliendo con los criterios de oportunidad, integridad disponibilidad, confidencialidad, promoviendo la continuidad de la prestación de servicios de salud.
3. **POLÍTICA DE GOBIERNO DIGITAL.** Donde el Gerente de la E.S.E Hospital Universitario de Santander y sus colaboradores se comprometen a establecer procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información y las comunicaciones, habilitando servicios digitales de confianza y calidad, empoderando a los usuarios, funcionarios, ejecutores, docentes, estudiantes, proveedores y la ciudadanía en general a través de la consolidación de un entorno digital confiable, favoreciendo la toma de decisiones a partir del uso y aprovechamiento de la información que conlleven a la consolidación de una entidad competitiva, proactiva, e innovadora en un entorno de confianza digital.
4. **POLÍTICA DE RENOVACIÓN TECNOLÓGICA.** Donde el Gerente de la Empresa Social del Estado Hospital Universitario de Santander y sus colaboradores se comprometen a Gestionar de la tecnología biomédica, industrial y de hardware, de acuerdo al ciclo de vida de la tecnología, planeando la renovación tecnológica, a partir de la priorización de necesidades y su articulación con el direccionamiento estratégico, evaluando el desempeño del equipo, del proveedor, la relación costo efectividad que genera la tecnología y el impacto en la seguridad del paciente y los colaboradores.

Adicionalmente la Entidad cuenta con el Comité Institucional de Gestión y Desempeño compuesto por los representantes de las distintas dependencias de la Institución, precedida por la Gerencia de la ESE HUS que tiene las siguientes funciones en materia de Seguridad Informática:

- Implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.

- Definición de lineamientos para la implementación de la normatividad relacionada con la estrategia de la Ley de Transparencia y acceso a la información y hacer recomendaciones sobre las decisiones de seguridad, políticas, normas, responsabilidades, proyectos, acuerdos de confidencialidad, mapa de riesgos y sus acciones, incidentes de seguridad y demás componentes del Modelo de Seguridad y Privacidad de la Información – MSPI.

- Definición de lineamientos para la implementación efectiva de políticas y estándares asociados, como la política de actualización del sitio Web (donde deberán estar involucradas las diversas áreas, direcciones y/o programas de la entidad), política de uso aceptable de los servicios de Red y de Internet, política de servicio por medios electrónicos, política de privacidad y condiciones de uso y política de seguridad de datos y del sitio Web, entre otros.

- Hacer seguimiento al cumplimiento de las políticas, normas, pautas y procedimientos de seguridad de la información en la ESE HUS, generando una cultura de seguridad informática.

- Analizar y proponer herramientas tecnológicas de seguridad informática, garantizando un ambiente informático seguro.

MECANISMOS DE CONTROL ESTABLECIDOS

La ESE Hospital Universitario de Santander a través del Grupo de Apoyo Tecnológico y de Información, ha establecido los siguientes mecanismos de control para evitar que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva.

- Verificación del software instalado en los equipos institucionales, en caso de existir software ilegal o no permitido se procede a su desinstalación.
- Los funcionarios o colaboradores del Grupo de sistemas son los únicos autorizados para instalar software en los equipos de cómputo del HUS.
- Se tiene establecidas las políticas de seguridad informática, las cuales se encuentran publicadas en la página web del HUS, haciendo referencia a las prohibiciones de instalación de software ilegal.
- Se realiza socialización periódica en temas de seguridad informática a los funcionarios, contratista y demás personal que labora en la ESE HUS.
- Se cuenta con firewall instalado que ayuda a impedir que hackers o software malintencionado (como gusanos) obtengan acceso al equipo a través de una red o de Internet. El firewall también ayuda a impedir que el equipo envíe software malintencionado a otros equipos.
- En referencia a los equipos de terceros en el contrato se especifica que es responsabilidad de cada una de las empresas velar por la legalidad del software instalado en cada uno de estos equipos.
- Todos los equipos cuentan con antivirus actualizado.
- Se realizan auditorias de software licenciado en los equipos de los servicios.

Sin embargo se está gestionando la compra de una herramienta que permita controlar en tiempo real la instalación de software no legal o no permitido por la institución, así como la conexión de nuevos equipos a la red de datos sin conocimiento del departamento de sistemas.

PROCEDIMIENTO Y DESTINO FINAL DEL SOFTWARE Y EQUIPOS DADOS DE BAJA

El procedimiento y destino final establecido por la ESE Hospital Universitario de Santander para el hardware dado de baja, que en términos generales es el siguiente:

Para dar de baja equipos de cómputo:

1. Se retira previamente el disco duro del equipo que se va a dar de baja, además de retirar otras piezas que sirvan de repuesto para otros equipos de cómputo.
2. El Coordinador del Grupo de Sistemas, da su concepto para dar de baja el hardware e informa a Almacén
3. Almacén elabora la Resolución de baja de bienes y la remite al Secretario General del comité de bajas para su revisión y firma.
4. Almacén, procede a la destrucción del hardware dado de baja y elabora la respectiva acta.

Para dar de baja a software:

La Institución no tiene como política dar de baja al software. Los aplicativos se siguen utilizando porque quedan en modo consulta, necesarios para dar respuesta a los diferentes requerimientos de las áreas.

EQUIPOS DE CÓMPUTO PARA CONTINGENCIA.

La UFATI ha contemplado 5 equipos de contingencia para los diferentes eventos que se presenta. Sin embargo a raíz de las necesidades de los servicios se ha tenido que disponer de estos 5 equipos, sin lograr mantener la contingencia.

RECOMENDACIONES

La Oficina de Control Interno recomienda al Grupo de Sistemas, identificar los riesgos asociados que frente al cumplimiento de normas de uso de software pudieran existir, analizando sus causas, garantizando su administración y la formulación de controles efectivos, con base en la metodología del DAFP; Guía para la Administración del Riesgo, para que sean incluidos dentro del mapa de riesgos de la Entidad.

Se sugiere continuar sensibilizando de manera periódica sobre temas relacionados con la seguridad informática, los costos de la no seguridad y las implicaciones legales por incurrir en piratería de software.

INFORME REGISTRADO EN EL APLICATIVO

En cumplimiento de la Directiva Presidencial 02 del 12 de Febrero de 2002 y del comunicado 0001 del 12 de enero de 2011, de la Dirección Nacional de Derechos de Autor, sobre la remisión de informes de Software, la Oficina de Control Interno registró el Informe de Software en el Aplicativo autorizado para la recolección de la información.

El sistema arrojó el siguiente reporte de cumplimiento:

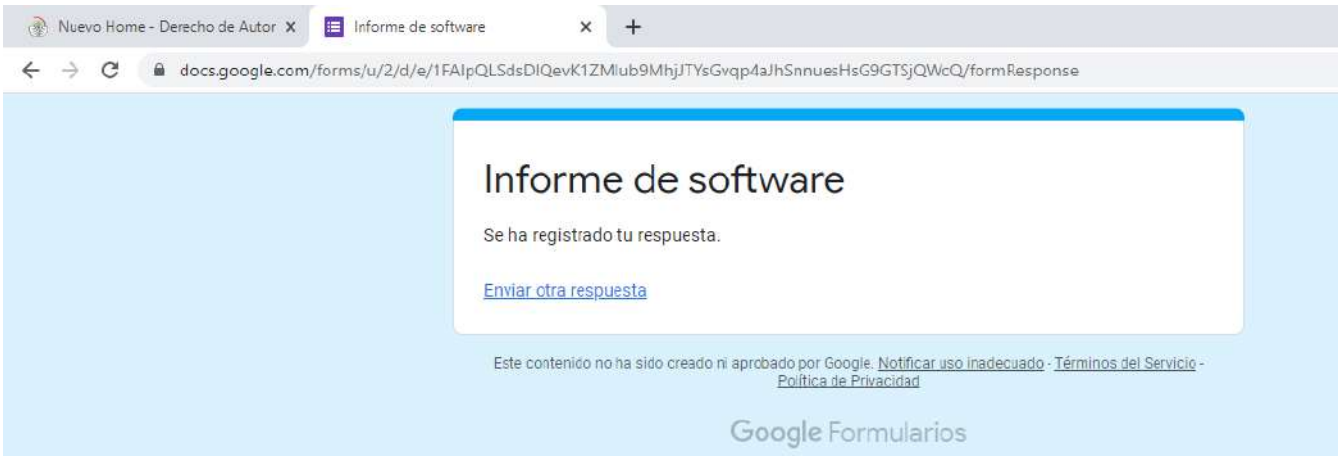

Imagen. Constancia de envío – 20/03/2020

Atentamente,

JULIO HERNAN VILLABONA HERNAN
Jefe Oficina Asesora Control Interno

Proyectó: Sandra Mendoza. Profesional de apoyo de Control Interno. CPS