CONTRALORÍA
DEPARTAMENTAL DEL TOLIMA
· La Contraloría del ciudadano ·

ESTUDIO TÉCNICO Y TECNOLÓGICO SOBRE LA ADQUISICIÓN DE LICENCIAS DE SOFTWARE DE SEGURIDAD PARA COMPUTADORES

CONTRALORÍA DEPARTAMENTAL DEL DEPARTAMENTO DEL TOLIMA

Ibagué (Tolima) – Colombia

Ing. Luis Fernando Niño Ospina

27 de noviembre de 2022

TABLA DE CONTENIDO

Pág.

1. JUSTIFICACIÓN DE ESTE ESTUDIO

Se retoma para este estudio lo consignado en el estudio técnico correspondiente al proceso de compra de equipos de cómputo[1] elaborado para la entidad en la presente vigencia, pues las consideraciones y sustentos normativos son casi idénticos en una gran parte.

"Teniendo en cuenta que en la Ley de Ingeniería (https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003), mediante la cual se establece que como ejercicio de la ingeniería se encuentra el desempeño de actividades como los estudios, proyectos y diseños de computación, de sistemas y de teleinformática".

[Así como que en la Clasificación Nacional de Ocupaciones – Diccionario Ocupacional e Índice Alfabético de Denominaciones Ocupaciones (https://observatorio.sena.edu.co/Content/pdf/cno_version_2020_2.pdf), para los Ingenieros de Tecnologías de la Información 'CNO 2145', quienes "Investigan, planifican, diseñan, evalúan, integran e implementan soluciones informáticas, sistemas operativos, almacenes de datos y software de tecnologías de la información y las comunicaciones", establece, dentro de las funciones de estos ingenieros, el "Establecer requisitos de la solución de tecnologías de la información y las comunicaciones de acuerdo con estándares y procedimiento técnico"].

[Por su parte, la resolución 736 de 2017, emitida por la entidad, en su artículo 12, respecto a los "lineamientos para procesos de negociación y contratación relacionados con tecnología", entre otros aspectos, establece que en procura de que "La Dirección de Tecnología (o la que haga sus veces), analizará la información presentada y procurará establecer la opción más viable y óptima para la entidad, de tal forma que la solución que se indique dé cumplimiento a los lineamientos del Gobierno Nacional relacionados con la Estrategia de Gobierno en Línea y esté en armonía con los planes y proyecciones que para la entidad se hayan realizado en el corto, mediano y largo plazo en el ámbito tecnológico" - (Se aclara que la Estrategia de Gobierno en Línea es ahora la Política de Gobierno Digital)].

[A la vez, las funciones establecidas en la entidad para el Profesional Universitario que se encuentra asignado al proceso de Gestión TIC, se han estipulado, entre otras, las de: **/\-**Coordinar la adquisición, recepción e instalación de cualquier elemento de cómputo: Equipos, impresoras, programas, licencias, software operativo, aplicativo, instaladores, entre otros; **/\-**Diagnosticar y evaluar, en coordinación con las diferentes dependencias y organismos, las necesidades de suministro de bienes y prestación de servicios informáticos; **/\-**Elaborar los términos de referencia, protocolos y estándares a seguir para adquisición, mantenimiento y/o actualización de equipos y programas, así como emitir concepto técnico para la adquisición de equipos de cómputo y software].

Es obligatorio para toda entidad, incluyendo este ente de control, el adoptar todas las medidas de seguridad que sean pertinentes para procurar la disponibilidad, así como la integridad y confiabilidad de la información, tanto de la que se captura, procesa y almacena en diversos equipos y medios en la entidad, como también la que se gestiona en los equipos de cómputo que emplean los distintos funcionarios que laboran en ella.

Todos los sistemas y aplicaciones de software presentan vulnerabilidades o fallos involuntarios que han quedado después del proceso de codificación del software, los cuales son aprovechados por ciberdelincuentes y malware para espiar, recopilar información de distinto tipo, estafar, robar, secuestrar información, afectar el funcionamiento de sistemas informáticos, usar inadecuadamente la infraestructura informática para realizar ataques a terceros, y, en general, para hacer daño, afectando no solo reputacionalmente a las

[1] https://www.contraloriatolima.gov.co/documentos/2022/otros/EstudioTecnicoNecesidadComputadoras2022v4.pdf

organizaciones sino también generando problemas de funcionamiento, riesgos para la vida de personas y afectaciones económicas.

Siendo la información un activo más de toda organización y siendo también cuantificable su valor en dinero, es obligatoria su adecuada protección, su seguridad y preservación, tal como se hace con cualquier otro activo, pues de no hacerlo y, ante un evento de seguridad, se generarían pérdidas de diversos tipos, lo cual es evitable, previsible técnicamente, adoptando herramientas y controles adecuados, como lo son los sistemas informáticos de seguridad, tales como software antimalware, antivirus, solucione endPoint, EDR, XDR, entre otros.

Por lo anterior, el Profesional Universitario del proceso de Gestión TIC, de la Contraloría General del Departamento del Tolima, expone el análisis y razones para sustentar la "**ADQUISICIÓN DE LICENCIAS DE SOFTWARE DE SEGURIDAD PARA DETECCIÓN Y RESPUESTA DE PUNTOS FINALES CON PLATAFORMA DE ADMINISTRACIÓN CENTRALIZADA**", correspondiente a un requerimiento técnico obligatorio para el funcionamiento controlado y bajo un sistema de protección de cada uno de los computadores de la entidad, de forma permanente y automatizada, tanto en un contexto de computador sin conectividad, como en los casos en que se encuentre conectado a cualquier entorno de red, tanto al interior de la entidad como desde otras ubicaciones, especialmente en lo que se refiere a quienes desarrollan actividades laborales fuera de la entidad, ya sea en sus lugares de residencia o en otras entidades durante procesos de auditorías fiscales o derivado de procesos de investigación fiscal, mejorando de esta manera el nivel de protección que permita el acceso a diversos recursos y servicios locales, en línea y en medios extraíbles, minimizando el riesgo de una infección por malware o un ataque informático, logrando así el desarrollo de procesos seguros y confiables que favorezcan la seguridad de la información digital, por ende, protegiendo los activos de información digitales de la entidad.

2 FUNDAMENTOS QUE JUSTIFICAN LA DE COMPRA DE LAS LICENCIAS DE SOFTWARE DE SEGURIDAD PARA LOS COMPUTADORES

2.1 Política de Gobierno Digital

[*Respecto al ámbito de TI en el sector estatal, se tiene establecido que las entidades del estado deben implementar la Política de Gobierno Digital, según la nueva versión de tal política que se encuentra establecida por el Decreto 767 de 2022 (https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=186766), que modifica, a la vez, el Decreto Único Reglamentario -DUR-1078 de 2015 del sector de Tecnologías de la Información y las Comunicaciones, https://www.mintic.gov.co/portal/inicio/Normatividad/Decreto-Unico-Sector-TIC/, la cual se entiende como "el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el objetivo de impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio"* (Ministerio de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2022)*, lo cual corresponde también al objeto de la política*] (Niño Ospina, Estudio Técnico y Tecnológico sobre la Necesidad de Adquisición de Computadores Versión 4, 2022).

[Se encuentran, dentro de los principios de la Política de Gobierno Digital (Ministerio de Tecnologías de la Información y las Comunicaciones - República de Colombia, 2022), que las entidades del estado se deben regir a la función y procedimientos administrativos consagrados en la normatividad vigente, debiendo observar, para este proceso, entre otros, los principios de:

- Según el artículo 209 de la Constitución Política: Economía, eficacia, celeridad.
- Según la Ley 489 de 1998: Celeridad, economía, eficacia, eficiencia.
- Según la Ley 1437 de 2011, artículo 3 incisos 11, 12 y 13: Eficacia, economía y celeridad.
- Según la Ley 1712 de 2014, artículo 3: Facilitación, gratuidad, celeridad, eficacia, calidad de la información, divulgación proactiva de la información.
- Según el decreto 767 de 2022, artículo 2.2.9.1.1.3: Principios de la Política de Gobierno Digital]

[Se encuentran, dentro de los habilitadores de la Política de Gobierno Digital, entre otros, el habilitador de "Arquitectura", así como el de "Servicios Digitales", mediante los cuales se desarrollan capacidades para la ejecución las líneas de acción de la política: Para el fortalecimiento institucional a través del enfoque de "Arquitectura Empresarial"; y, "mediante soluciones tecnológicas" para mejorar la interacción con la ciudadanía].

{Se reafirma, del estudio realizado para la entidad con el fin de sustentar la contratación de unos requerimientos que ofrece LACNIC, que [Es la Política de Gobierno Digital una "Política de Gestión y Desempeño Institucional", tal como quedó establecido en el Plan Nacional de Desarrollo 2018-2022 (**Ley 1955 de 2019**), subsección 6 Legalidad – Otras disposiciones, en su **artículo 148**, **GOBIERNO DIGITAL COMO POLÍTICA DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL**, mediante el cual se modificó el artículo 230 de la *Ley 1450 de 2011* (P.N.D. 2010-2014)][2] (Niño Ospina, Estudio Técnico y Tecnológico sobre la Necesidad de Adquisición de la Membresía, Pool de Direcciones IPv6 y ASN, con LACNIC, 2022)}.

[2] Plan Nacional de Desarrollo 2018-2022. Ley 1955 de 2019: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=93970

[Establece la Política de Gobierno Digital, según lo consignado en su "Manual Interactivo de Gobierno Digital"[3], dentro del material de apoyo del habilitador de arquitectura, en el "Documento Maestro del Modelo de Gestión y Gobierno de TI" (Documento Maestro del MGGTI) que este modelo "…permite generar las capacidades institucionales de TI que se requieren para prestar servicios de TI a los usuarios de cada entidad mediante el uso adecuado de las tecnologías de la información y las comunicaciones" (Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC, 2019)(pp.9), a su vez, en este documento se establecen unos principios considerados como reglas "…que se deben tener en cuenta al momento de gestionar las tecnologías de la información y las comunicaciones a nivel sectorial, institucional y territorial", dentro de los que se resaltan, para el objeto de este estudio, los de: 4.2. Costo/Beneficio; 4.3. Racionalización; 4.4. Estandarización; 4.7. Calidad; 4.10. Neutralidad tecnológica; 4.11. Foco de las necesidades; 4.12. Vigilancia tecnológica].

[Conforme a lo consignado en el documento anteriormente referenciado (Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC, 2019), mediante los lineamientos del MGGTI, distribuidos en los 5 dominios del modelo, se establecen las directrices que se den aplicar para lograr la alineación de las necesidades haciendo uso adecuado de las TIC, encontrando que la entidad debe contar con procedimientos, según los lineamientos:

- Del "6.1. Dominio de estrategia de TI", el lineamiento "6.1.3. MGGTI.LI.ES.03 – Políticas de TI" especifica que "La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar y definir las políticas y estándares que faciliten la gestión y la gobernabilidad de TI, contemplando por lo menos los siguientes temas: …adquisición tecnológica, …acceso a la tecnología y uso de las facilidades por parte de los usuarios".

- Del "6.2. Dominio de gobierno de TI", el lineamiento "6.2.4. **MGGTI.LI.GO.04** – Gestión de Incidentes de TI" establece que se debe contar con soporte a incidentes en los 3 niveles de atención técnica; El lineamiento "6.2.5. **MGGTI.LI.GO.05** – Gestión de problemas de TI" indica que se deben gestionar los incidentes recurrentes tratándolos como problemas;

- Del "6.5 Dominio de infraestructura tecnológica", el lineamiento "6.5.2 **MGGTI.LI.IT.02** – Capacidad de la infraestructura tecnológica" especifica, entre otras, que "se debe velar por la correcta operación de la infraestructura de TI"].

[Teniendo en cuenta los lineamientos generales del MGGTI, en especial los indicados anteriormente, la entidad la entidad cuenta con unos lineamientos internos para la adquisición de tecnología "lineamientos para procesos de negociación y contratación relacionados con tecnología" (Contraloría Departamental del Tolima, 2018)(pp. 12); también cuenta con un procedimiento para la atención de incidentes, mediante el soporte técnico que se encuentra establecido dentro de los procesos del Sistema de Gestión de la Calidad SGC adoptado por la entidad y contemplado dentro de la actividad "Soporte para el funcionamiento de software y hardware", para lo cual se tienen establecidos los registros "RGT-02 Cronograma de comprobación y mantenimiento TIC", "RGT-08 Soporte Técnico", … (Contraloría Departamental del Tolima, 2018) (pp.187-192)].

[3] Manual Interactivo de la Política de Gobierno Digital: https://app.powerbi.com/view?r=eyJrIjoiOTRiM2JkMzktMDlmOC00MTI4LWIyZDItYjAwZmM3ODg0MjhjIiwidCI6IjFhMDY3M2M2LTI0ZTEtNDc2ZC1iYjRkLWJhNmE5MWEzYzU4OCIsImMiOjR9

De igual forma, se considera, según lo mencionado en el mismo estudio elaborado para la entidad con respecto a IPv6-LACNIC, que "Los lineamientos del dominio de arquitectura de infraestructura tecnológica, especificados en el Modelo de Arquitectura Empresarial[4] (https://www.mintic.gov.co/arquitecturati/630/articles-144764_recurso_pdf.pdf) que soporta la Política de Gobierno Digital, tienen como fin que las entidades del estado garanticen la disponibilidad y operación permanente de los sistemas y servicios de información en beneficio de todos los usuarios" (Niño Ospina, Estudio Técnico y Tecnológico sobre la Necesidad de Adquisición de la Membresía, Pool de Direcciones IPv6 y ASN, con LACNIC, 2022).

[El Documento Maestro del Modelo de Arquitectura Empresarial MAE.G.GEN.01 se constituye en la carta de navegación para la implementación del habilitador de "Arquitectura", encontrando los diversos principios (comunes al MGGTI), dominios y lineamientos[5] que se deben aplicar según el objetivo de tal documento, correspondiente a "brindar a las Entidades Públicas a través del Líder Estratégico de TI (director o Jefe de Tecnologías de la Información y las Comunicaciones) y del Comité/Grupo de Arquitectura de cada Entidad, o quienes hagan sus veces, un entendimiento detallado de la estructura del Modelo de Arquitectura Empresarial, el cual debe ser implementado para mejorar las capacidades institucionales mediante el uso adecuado de las TIC y su alineamiento con las necesidades de la entidad…" (Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC, 2019)]

[El Modelo de Arquitectura Empresarial -MAE- se estructura en 7 dominios, con sus correspondientes lineamientos los cuales son en total 39, que, para el caso de este estudio técnico, corresponden a:

- Del "7.1. Dominio de planeación de la arquitectura" (PA), el lineamiento "7.1.3. **MAE.LI.PA.03** – Definición del grupo de arquitectura", establece que se debe contar con un grupo de trabajo de arquitectura empresarial, acorde a la madurez de la implementación del MAE, que hace las veces de comité técnico de arquitectura empresarial encargado de evaluar los impactos de las inversiones, adquisiciones o modernizaciones de TI.

- Del "7.2. Dominio de arquitectura misional" (AM), el lineamiento "7.2.4. **MAE.LI.AM.04** – Apoyo de TI a los procesos", establece que hay que identificar, entre otras, las necesidades de *"…apoyo tecnológico que requieren los procesos y procedimientos de la entidad, de tal manera que se incorporen facilidades tecnológicas que contribuyan a mejorar la articulación, calidad, eficiencia, seguridad y reducir los costos de operación*".

- Del "7.5. Dominio de arquitectura de infraestructura tecnológica" (AIT), el lineamiento "7.5.4. **MAE.LI.AIT.04** – Continuidad y disponibilidad de los elementos de infraestructura", establece que se debe garantizar la continuidad y disponibilidad de la infraestructura tecnológica, atención y resolución de incidentes, para mantener la operación y prestación de los servicios].

- Del "7.6. Dominio de Arquitectura de Seguridad" (AS), el lineamiento "7.6.3. **MAE.LI.AS.03** - Seguridad y privacidad de los sistemas de información",

[4] El Modelo de Arquitectura Empresarial -MAE- corresponde a un conjunto de orientaciones que permite definir lógicamente la estructuración y el direccionamiento de una organización mediante una concepción global e integrada de todas las áreas y procesos de la organización, facilitando su alineación con el plan estratégico y con el plan de acción.

[5] Los lineamientos establecidos en el Documento Maestro del Modelo de Arquitectura Empresarial se refieren a "…orientaciones de carácter general y corresponden a disposiciones o directrices que deben ser ejecutadas en las entidades del Estado colombiano para implementar el Modelo de Arquitectura Empresarial" (Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC, 2019)(pp. 29)

estipula que "*La Dirección de Tecnologías y Sistemas de la Información debe analizar e incorporar aquellos componentes de seguridad y privacidad de la información que sean necesarios durante todas las fases del ciclo de vida de los sistemas de información*"; el lineamiento "7.6.4. **MAE.LI.AS.04** - Auditoría y trazabilidad de los sistemas de información", establece que "*La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe desarrollar mecanismos que aseguren el registro histórico de las acciones realizadas por los usuarios sobre los Sistemas de Información, manteniendo la trazabilidad y apoyando los procesos de auditoria*"; el lineamiento "7.6.6. **MAE.LI.AS.06** - Seguridad informática", establece que "*La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe diseñar los controles de seguridad informática para gestionar los riesgos que atenten contra la disponibilidad, integridad y confidencialidad de la información identificados durante la ejecución de los ejercicios de arquitectura empresarial*".

Para lo cual, la entidad tiene definidas funciones claras y procedimientos sobre la adquisición de nuevos recursos de TI, soporte técnico y requerimientos, dentro de las funciones del personal de TI de la entidad y en los procesos del Sistema de Gestión de la Calidad adoptado, especialmente en las funciones que corresponden al profesional universitario del proceso de Gestión TIC y en todo lo relacionado al plan de adquisiciones para poder realizar la compra de licencias de software de seguridad; Se cuenta también con un sistema de seguridad perimetral mediante un Firewall UTM, para que los funcionarios puedan interactuar en la red interna y navegar por la Internet bajo un nivel básico de seguridad, permitiéndoles así desempeñar a sus funciones y mantener la operación así como la prestación de los servicios misionales y administrativos, con una adecuada relación costo-beneficio, bajo un contexto seguro y de confianza digital que se fortalecerá con el software para cada uno de los computadores de la entidad.

2.2 Directivas Presidenciales

Mediante la Directiva Presidencial No 02 de 2022[6], el gobierno nacional, con el propósito de "garantizar la implementación segura de la Política de Gobierno Digital", estableció entre sus directrices que las entidades del Estado debemos "*Adoptar la seguridad digital con un enfoque preventivo y proactivo basado en la gestión efectiva de riesgos en el entorno digital, priorizando la protección de datos personales e información sensible de la entidad o que goza de reserva legal, al igual que de los servicios y sistemas de información e infraestructuras críticas*", como también que "*Realizar un monitoreo permanente a la infraestructura de los servicios utilizados, incluyendo a los que usen los teletrabajadores o trabajadores en casa, con el fin de analizar posibles acciones no autorizadas*", entre otras directrices, las cuales se suman a las directrices que ya habían sido establecidas mediante la Directiva Presidencial No 03 de 2021[7].

2.3 Reportes de seguridad

Teniendo en cuenta la relación directa del Firewall con el actual proceso de adquisición de licencias para software de seguridad para los equipos de cómputo, se retoman los tres informes referenciados y descritos en el estudio técnico relacionado con firewall de la entidad (Niño Ospina, Estudio técnico y tecnológico – mercado y precios, sobre la necesidad de actualización de las licencias del FIREWALL UTM USG110 ZYXEL, 2022):

[De acuerdo con el reporte de seguridad para Latinoamérica 2022 (https://www.welivesecurity.com/wp-content/uploads/2022/07/ESET-security-report-

[6] Directiva Presidencial No 02 de 2022: https://funcionpublica.gov.co/eva/gestornormativo/norma.php?i=179306
[7] Directiva Presidencial No 03 de 2021: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=160326

LATAM-2022.pdf)[8], realizado por la compañía ESET, se encontró que Colombia ocupa el tercer lugar en la región con mayores detecciones, siendo el más reiterado el ataque por "Troyanos" y el "Phishing" el canal de infección más común. A nivel general, para Latinoamérica, las mayores preocupaciones se focalizan en "Infección con códigos maliciosos" y el "robo de información", presentando que casi la mitad ha sufrido algún incidente de seguridad. Se presentó un elevado aumento en la cantidad de vulnerabilidades detectadas. Se han presentado campañas de espionaje para las cuales el target principal son las entidades del estado, como es el caso de la campaña "Operación Discordia" (https://www.welivesecurity.com/la-es/2022/05/20/campana-espionaje-malware-njrat-organizaciones-colombia/), detectada en mayo de 2022, que mediante la implantación del malware njRAT se busca capturar información sensible. Colombia ocupa el séptimo puesto en afectaciones por malware espía en la región y el noveno puesto en distribución de las detecciones de troyanos. Dentro de los controles sugeridos en el reporte, para la prevención, se encuentran los Firewalls, entre otros controles, además de soluciones de seguridad, todos de forma combinada, complementándose unos con otros.

El CAI Virtual de la Policía Nacional, en el último balance de cibercrimen (https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf), el cual fue realizado en el año 2020, presenta como parte de los mayores delitos informáticos de mayor frecuencia, los de: Suplantación de Sitios web; Interceptación de datos informáticos; Violación de datos personales; Obstaculización ilegítima de sistema informático o red de telecomunicaciones; Daño informático; Transferencia no consentida de activos; Acceso abusivo a un sistema informático; Hurto por medios informáticos y semejantes; y, el uso de software malicioso. Las principales modalidades se presentan en: Estafa por compra y/o venta de productos; Phishing; Suplantación de identidad; Vishing (Voice phishing); Malware; Amenazas a través de redes sociales; Injuria y/o calumnia a través de redes sociales. Se evidencia el aumento de la cibercriminalidad, según lo reportado tanto en el último balance de cibercrimen como en lo que se observa en el informe "Tendencias Cibercrimen en Colombia 2019-2020" (https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf).

El Tanque de Análisis y Creatividad de las TIC (TicTac) – Programa de Seguridad Aplicada al Fortalecimiento Empresarial (SAFE) en su último estudio presentado, en julio de 2022, denominado "Estudio semestral Tendencias del cibercrimen: Ciberseguridad en la era de la movilidad digital" (https://www.ccit.org.co/estudios/estudio-semestral-tendencias-del-cibercrimen-ciberseguridad-en-la-era-de-la-movilidad-digital/)[9], evidencia un crecimiento en lo que respecta al "Acceso abusivo a sistema informático", con un +46% respecto al año anterior, así como un crecimiento del "Hurto por medios informáticos", con un +15%].

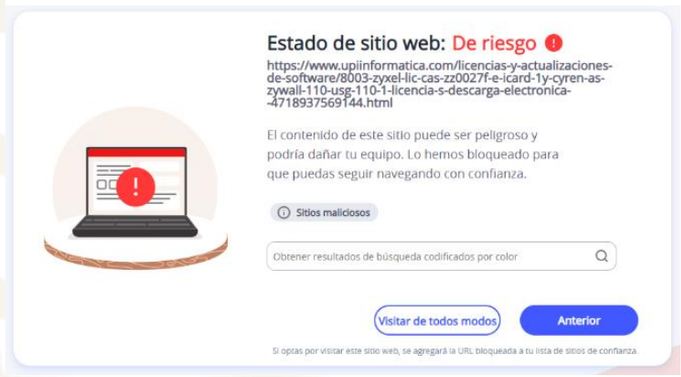
También se reitera, del ya mencionado estudio técnico, según el contenido de los informes anteriormente citados, que con "el aumento de la cibercriminalidad, no solo en Colombia, sino en el mundo entero" se hace necesario redoblar esfuerzos, adoptando "todos los controles necesarios para minimizar el riesgo de ser afectado por un ataque cibernético", controles como bien se considera el software de seguridad para cada uno de los computadores, según lo ya indicado en párrafos atrás.

[8] https://www.welivesecurity.com/la-es/2022/08/04/empresas-america-latina-incidentes-seguridad/
[9] https://www.ccit.org.co/wp-content/uploads/ciberseguridad-en-la-era-de-la-movilidad-digital-version-digital.pdf

3 ANTECEDENTES Y DIAGNÓSTICO GENERAL DEL ESTADO ACTUAL

Aunque no se han encontrado referencias recientes de la contratación de algún software de seguridad para los equipos de cómputo, pues revisando las contrataciones de TI desde el año 2015 no se encontró nada al respecto, sin embargo, en el año 2018 se realizó un proceso de bajas de varios bienes de la entidad, dentro de ellos las licencias de **Antivirus Kaspersky**, para las cuales, el Profesional Universitario del proceso de Gestión TIC emitió el respectivo concepto a través del informe técnico con el asunto "Reporte Técnico para comité de bajas de 2018" con fecha Julio 31 de 2018, remitido a la Secretaría Administrativa y Financiera de la entidad mediante correo electrónico el 10 de agosto del mismo año.

Figura 1. Imagen propia. Captura de pantalla detección de sitio malicioso



Debido a que no se cuenta con un software licenciado para la protección de los computadores de la entidad, se han venido empleando herramientas gratuitas tales como el software del propio Windows, como lo es Windows Defender, como también herramientas libres como ClamWin[10] el cual es OpenSource, la versión gratuita de AVG[11], como también herramientas en línea tales como VirusTotal[12], Eset OnLine Antivirus[13], McAfee WebAdvisor[14], sin embargo, casi todas son herramientas que permiten realizar escaneos en momentos específicos y no permanentemente o en tiempo real, pues carecen de un software residente en la RAM que se ejecute y active automáticamente al encender las computadoras, además, el software gratuito no es tan efectivo como el software licenciado, aún con un gestor de seguridad local y residente en memoria RAM, pues pese a tener un gestor residente, como en el caso de Windows Defender y de AVG, se presentaron casos de infecciones que fueron detectadas al momento de usar dispositivos extraíbles (previamente utilizados en equipos de la entidad) en equipos personales con antivirus legalmente licenciado, además de presentarse inconvenientes en el funcionamiento de computadoras que luego fueron diagnosticadas como infectadas.

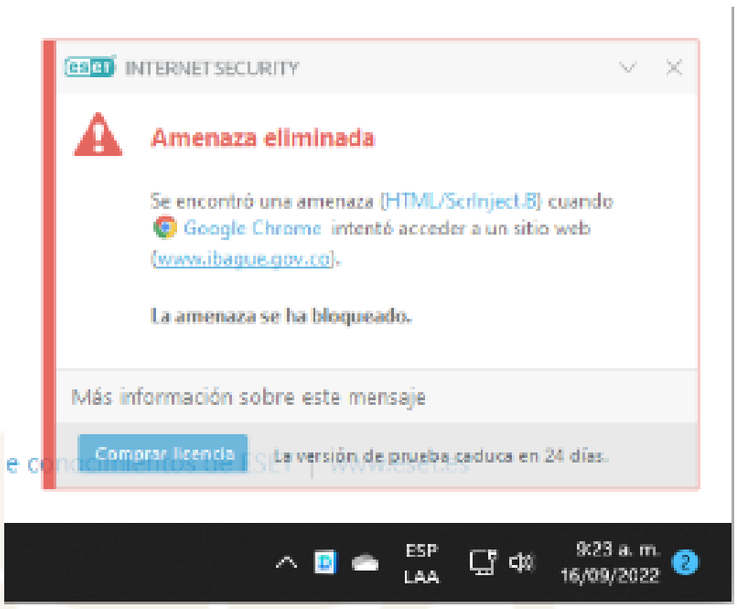
Durante el presente semestre (semestre 2 de 2022), se han evaluado 2 herramientas de software para protección de los computadores, primeramente, se evaluó el Eset Internet Security, luego el CORTEX de Palo Alto.

Debido a que se venían presentando problemas en el funcionamiento de varias computadoras en la entidad, pérdida de archivos e inconvenientes en la conectividad, tanto en el ámbito local como al navegar por Internet, inicialmente se trató de diagnosticar algún inconveniente, para lo cual se empleó el ESET OnLine Scanner, herramienta gratuita que no arrojó inconvenientes, luego se procedió a desinstalar el antivirus gratuito AVG y se instaló el ESET Internet Security como versión de prueba por 30 días con el fin de determinar si se trataba de malware, donde casi de inmediato, luego de la instalación en los primeros computadores, se empezaron a presentar reportes de amenazas presentes en algunos

[10] ClamWin: http://es.clamwin.com/ y https://sourceforge.net/projects/clamwin/
[11] AVG Antivirus: https://www.avg.com/es-co/
[12] Virus Total: https://www.virustotal.com/
[13] Eset OnLine Antivirus: https://www.eset.com/co/hogar/deteccion-de-malware-online/
[14] McAfee WebAdvisor – Herramienta Gratuita: https://www.mcafee.com/es-co/safe-browser/mcafee-webadvisor.html

equipos, afectando a la red, encontrando así la causa de los bloqueos a nivel de red que se venían presentando, además del origen de otros problemas con la información.

Figura 3. Imagen propia. Captura de pantalla amenaza en sitio web bloqueada



A diario se presentan múltiples amenazas e intentos por vulnerar la seguridad de la red y de los distintos dispositivos de la entidad, encontrando, luego de probar diversas herramientas, que cada herramienta de seguridad detecta gran cantidad de amenazas, aunque algunas detectan más que otras, por ejemplo, McAfee WebAdvisor logró detectar algunos sitios maliciosos y/o infectados, pero cuando se instaló el ESET Internet Security se encontró que y algunos sitios en la Internet, aparentemente confiables, podrían ser vectores de propagación de malware, como es el caso del sitio web de la Alcaldía de Ibagué, muy visitado por muchas personas, incluyendo personal de la contraloría, para informarse sobre las novedades en la ciudad, sin embargo, al ingresar durante unas cuantas semanas a ese sitio web, el ESET lo bloqueaba e informaba que se encontraba infectado por el malware "**HTML/ScrInject.B Troyano**", evitando de esta manera que se inyectara y propagara el código malicioso en la red y equipos de cómputo de esta contraloría.

Figura 2. Imagen propia. Captura de pantalla de amenaza detectada en sitio web www,ibague.gov.co

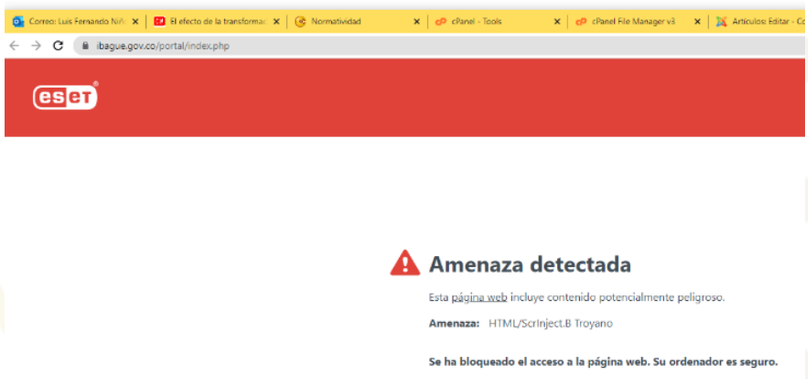
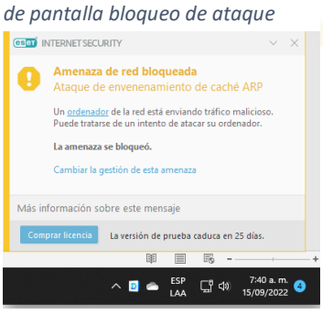


Figura 4. Imagen propia. Captura de pantalla bloqueo de ataque



A la vez, durante el periodo de prueba del ESET, se logró erradicar el problema que se estaba presentando con la red LAN, estableciendo los dispositivos fuente de los ataques, los cuales fueron desinfectados con el mismo antivirus, estableciendo que entre los ataques que se estaban presentando se encontraban los de envenenamiento de caché ARP, el cual corresponde a un ataque a las redes informáticas a las que ciberdelincuentes acceden para analizar el tráfico, modificarlo o impedirlo. Mediante este tipo de ataques es posible descubrir la información que está siendo transmitida en, desde y hacia los dispositivos conectados en la red, a la vez, se puede identificar cada una de las direcciones MAC y las direcciones IP de cada uno de los dispositivos conectados, así que se determinó que esta la causa por la cual se estaba perdiendo el acceso a la red, quedando todos los equipos sin conectividad de ningún tipo, identificando dos dispositivos como fuente del ataque, uno de tipo móvil y otro correspondiente a una computadora.

Figura 5. Imagen propia. Captura de pantalla bloqueo ataque ARP desde computadora

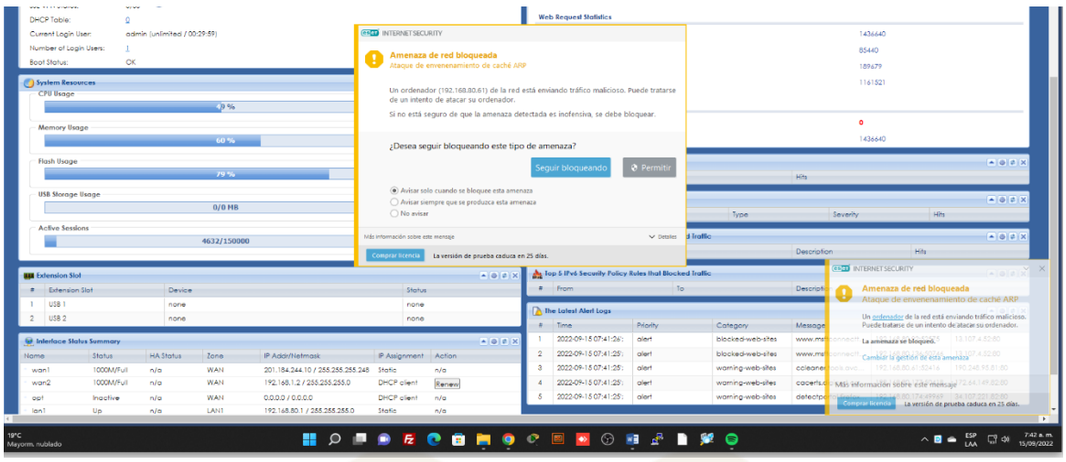
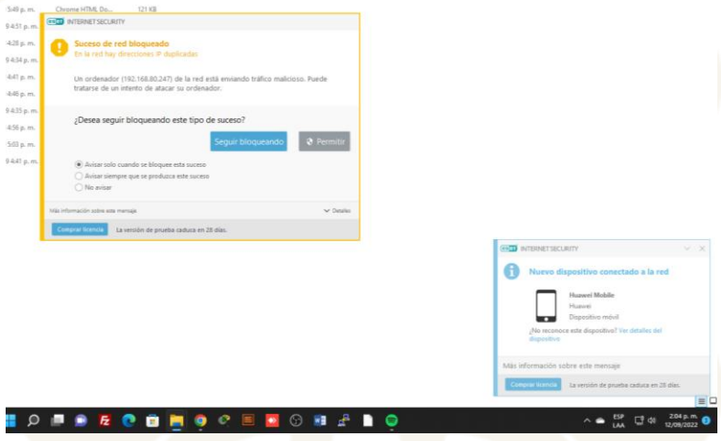


Figura 6. Imagen propia. Captura de pantalla bloqueo ataque ARP desde dispositivo móvil



Antes de la fecha de finalización del periodo de prueba del ESET, se desinstaló para instalar una nueva herramienta para pruebas y evaluación, como fue el CORTEX XDR de Palo Alto, mediante la cual se logró identificar algunas otras amenazas que no fueron identificadas con el ESET, a la vez, se identificaron diversos incidentes de seguridad y vulnerabilidades en cada uno de los dispositivos en los cuales se instaló la herramienta.

Figura 7. Imagen Propia. Pantallazo CORTEX XDR Reporte de Incidentes

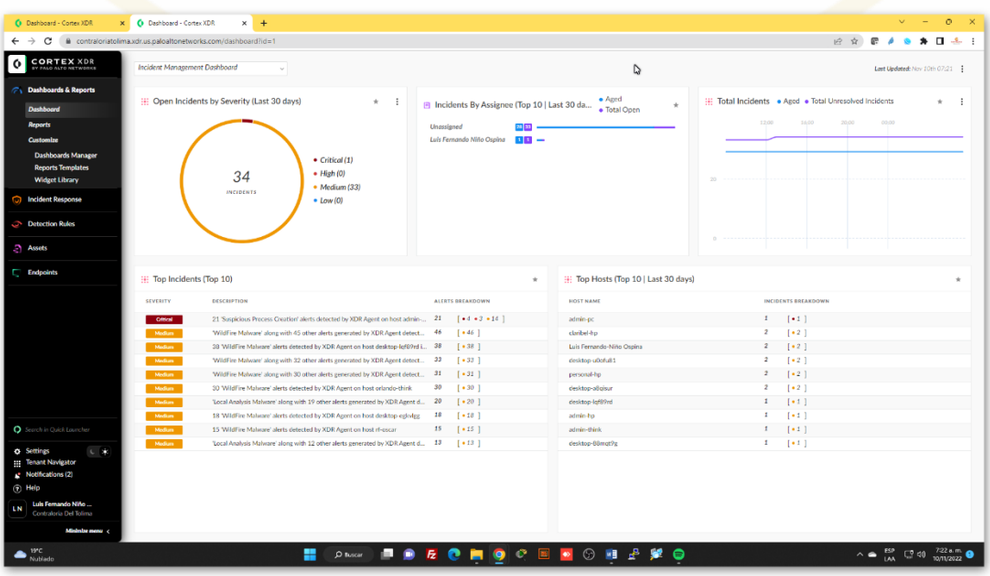


Figura 8. Imagen Propia. Pantallazo CORTEX XDR Reporte de porcentaje de Incidentes

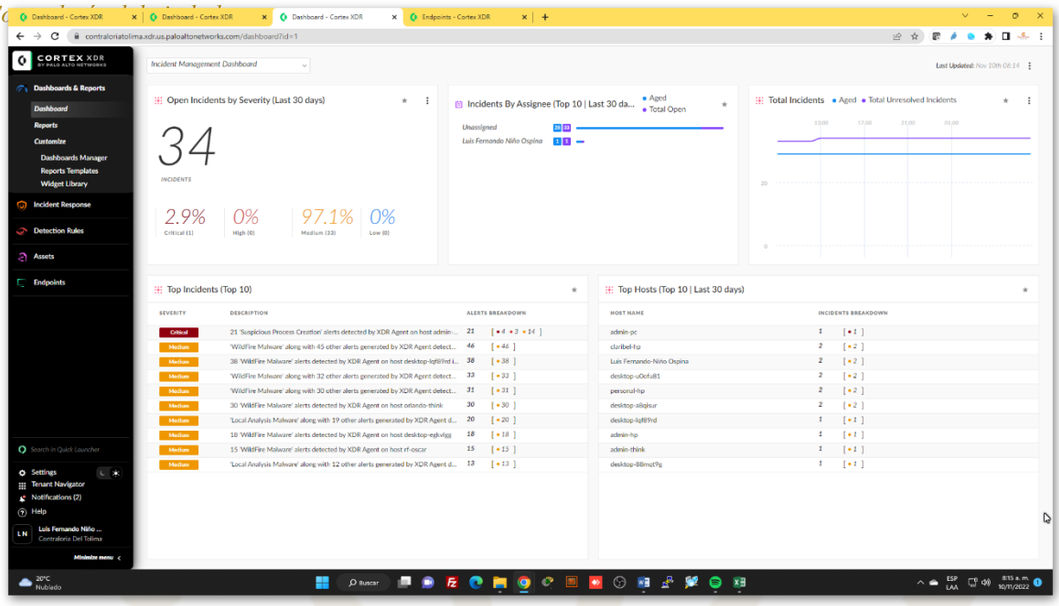
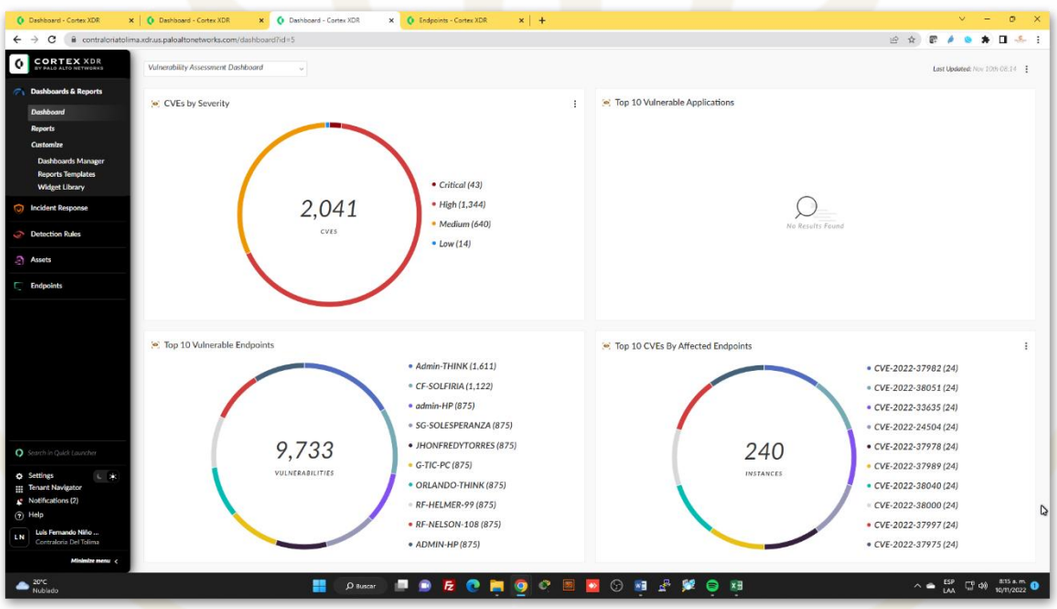


Figura 9. Imagen Propia. Pantallazo CORTEX XDR Reporte de vulnerabilidades identificadas



En ambos casos, ESET y CORTEX, se cuenta con un agente local en cada uno de las computadoras, en cada punto final (EndPoint), pero mientras el software de seguridad ESET Internet Security presenta gran efectividad contra malware local, en la red y en la web, con eliminación automática de las amenazas, el XDR es muy efectivo en la detección y gestión de amenazas según su comportamiento dañino, de acuerdo con la matriz MITRE ATT&CK, a la vez, identificando las vulnerabilidades de cada dispositivo según el listado de vulnerabilidades y exposiciones de seguridad conocidas y documentadas en las bases de datos CVE.

Por tanto, las dos herramientas tienen sus características particulares, sin excluirse una a la otra sino complementándose, para mejorar el nivel de seguridad tanto de cada uno de los dispositivos como también de la red informática, brindando información vital para que el equipo de respuesta a incidentes pueda realizar la respectiva gestión del incidente, contención, investigación (trazabilidad) y definición de controles adecuados para minimizar el riesgo de repetición del evento, todo a través de una plataforma centralizada de gestión en la nube, facilitando así el proceso de gestión de riesgos, seguridad e incidentes.

Además de las amenazas e incidentes identificados según lo descrito en los párrafos anteriores, mediante la protección del Firewall UTM de la entidad se han logrado contener más de 8000 eventos de seguridad en un mismo día, por lo que es claro que sean acciones focalizadas contra la entidad o de ataques aleatoriamente dispersados, la entidad requiere fortalecer la seguridad tanto de la red como de cada uno de los computadores y dispositivos usados.

La dinámica de trabajo que se presenta al interior de la entidad lleva a los funcionarios a que no solamente deban contar con protección en su computadora, para la conexión segura en la LAN e Internet, sino que también se deba contar con un software adecuado que permita detectar y eliminar las amenazas que llegan a través del correo electrónico, así como a través de información que es enviada al personal de la entidad en ocasión de procesos de denuncias, auditorías, investigaciones, rendiciones de cuentas e información requerida por el ente de control, sumado al hecho de que en ocasiones se requiere la conexión de sus computadoras a las redes informáticas de las entidades sobre las cuales están realizando el control fiscal, las cuales en ocasiones carecen de la más básica protección contra malware y demás amenazas; todo lo anterior se identifica como el origen de los incidentes que se han presentado en los últimos años en la entidad.

4 ESPECIFICACIONES TÉCNICAS Y REQUERIMIENTOS

Teniendo en cuenta las diversas pruebas realizadas, así como los diferentes eventos de seguridad presentados, la proliferación de amenazas a nivel mundial, el contexto de la entidad y algunas de las diversas vulnerabilidades identificadas durante las pruebas realizadas, el software de seguridad para la protección de la información que se gestiona en cada uno de los computadores de este ente de control, deberá contar con las siguientes características mínimas:

1. El licenciamiento debe ser por volumen y no individual
2. Buena puntuación en el último informe de investigación de Gartner[15], ubicándose dentro del grupo de líderes o de retadores del último cuadrante mágico[16]
3. No debe afectar el rendimiento de las computadoras o dispositivos donde se encuentre funcionando
4. Compatible con todas las versiones de Windows, desde Windows 7 en adelante
5. Plataforma centralizada de gestión/administración en la nube
6. Fácil uso y gestión/administración
7. EPP y EDR (Puede ser XDR), unificados en una aplicación o con herramientas separadas pero compatibles e integradas en su funcionamiento
8. Protección en tiempo real mediante un gestor residente en cada dispositivo
9. Control remoto de los dispositivos
10. Tecnología de Inteligencia Artificial integrada
11. Tecnología de Aprendizaje Automático integrada
12. Protección contra amenazas desconocidas
13. Protección contra Ransomware
14. Protección contra Spyware
15. Protección contra Adware
16. Protección de Punto Final (EndPoint), Aplicaciones y Red
17. Protección contra intrusiones
18. Herramienta Antivirus y Antimalware, automáticas para eliminación y cuarentena de amenazas conocidas
19. Detección y respuesta automatizada contra amenazas avanzadas, así como contra amenazas persistentes
20. Informes de uso, detección y gestión

Además de lo anterior, el contratista, por sí mismo o por medio del personal de soporte de la fábrica del software, deberá de desarrollar lo siguiente:

a) Asistencia y capacitación para el proceso de instalación, configuración y gestión/administración
b) Video del proceso de instalación, configuración y gestión/administración de la herramienta de protección y de su consola
c) Soporte técnico durante el periodo de licenciamiento

Cantidad de licencias:

- **100 (1 para cada dispositivo a proteger)**
- **1 Licencia para servidor VPS CentOs con 5 dominios**
- **1 Licencia para servidor Físico con Linux Ubuntu**

[15] Sitio web de Gartner: https://www.gartner.es/es/tecnologia-de-la-informacion
[16] ¿Qué es el cuadrante mágico de Gartner?: https://www.gartner.es/es/metodologias/magic-quadrant

5 CONDICIONES TÉCNICAS EXIGIBLES

- Se trata de un proceso de comercialización de software para computadoras, pero se requiere que el contratista tenga conocimientos sobre la instalación, configuración y gestión o administración de la herramienta de protección, para que pueda brindar la adecuada capacitación inicial al supervisor del contrato, proceso del cual se dejará la evidencia en video para que sirva de material de consulta para el personal de la entidad.

- Tratándose de un proceso de selección de Mínima Cuantía, desde el punto de vista mercantil, solamente se requiere que disponga de matrícula mercantil vigente y que el objeto de la empresa se lo permita, o la normatividad al respecto.

6 CONDICIONES TECNOLÓGICAS EXIGIBLES

- Plataforma en la nube del fabricante del software para la gestión centralizada de las licencias del software y para la gestión/administración de sus funcionalidades, especialmente las que se refieren a la característica de EDR.

7 ASPECTOS ADICIONALES

Se realizó la consulta del posible código en el Clasificador de Bienes y Servicios[17], del cual se obtuvieron los siguientes resultados:

- Código UNSPSC 81112501 Producto : Servicio de licencias del software del computador

- Código UNSPSC 43233205 Producto : Software de seguridad de transacciones y de protección contra virus

[17] https://www.colombiacompra.gov.co/clasificador-de-bienes-y-servicios

8 GESTIÓN COMO ACTIVO DE LA ENTIDAD

Debido al manejo que se les dio con anterioridad a las licencias del antivirus Kaspersky, se debe tener presente que estas licencias no son a perpetuidad ni sobrepasan el periodo de licenciamiento de 1 año, por lo cual se pueden considerar un elemento consumible.

El licenciamiento de cualquier software de protección contra malware y similares se puede considerar más un servicio de protección, pues requiere de estar conectado para poder acceder a actualizaciones y herramientas que se encuentran en la nube del fabricante del software, durante el periodo de licenciamiento adquirido.

Luego del periodo de licenciamiento, se dejará de tener acceso a la plataforma de gestión centralizada del fabricante del software, en la nube, como tampoco se tendrá acceso a actualizaciones ni ninguna otra herramienta de protección, quedando nuevamente vulnerables todos los computadores y dispositivos donde se haya registrado el software de protección.

Por lo anteriormente indicado, **no se trata de un activo**, por lo cual **no se debe incorporar al inventario**, sino que se debe tener en cuenta como un servicio que requiere renovarse anualmente.

9 CONCLUSIONES DEL ESTUDIO

Se recomienda, teniendo en cuenta las necesidades presentadas, según lo ya indicado en este estudio técnico y tecnológico, se adelanten el proceso requerido, partiendo por la correspondiente justificación, para la cual se sustentará la necesidad haciendo referencia al presente estudio, el cual debe formar parte integral de la documentación del respectivo proceso de contratación, por lo que se considera que deben iniciarse los "**Adquisición de Licencias de Software de Seguridad para Detección y Respuesta de Puntos Finales con Plataforma de Administración Centralizada"** a nombre de la Contraloría General del Departamento del Tolima.

Para constancia de lo anterior, se firma el presente estudio técnico y tecnológico, hoy, veintisiete (27) de noviembre de dos mil veintidós (2022).

LUIS FERNANDO NIÑO OSPINA
Ingeniero de Sistemas
T.P. No 70255167519TLM
Profesional Universitario Gestión TIC

NOTA ACLARATORIA: En el presente estudio se emplea el nombre completo de la entidad, según el registro legal de la misma, tal como figura en el RUT respectivo, correspondiendo tal nombre al de CONTRALORÍA GENERAL DEL DEPARTAMENTO DEL TOLIMA, sin embargo, por costumbre y tradición se conoce a la entidad como CONTRALORÍA DEPARTAMENTAL DEL TOLIMA, tal como aparece en el logo usado en este documento.

10 REFERENCIAS BIBLIOGRÁFICAS

Contraloría Departamental del Tolima. (24 de diciembre de 2018). *Resolución No. 667 de 24 de diciembre de 2028.* Obtenido de Por medio de la cual se modifican y adicionan políticas en el área de gestión de las tecnologías de la información y las comunicaciones: https://www.webcontraloria.gov.co/documentos/2018/resoluciones/Resoluci%C3%B3n_667_2018modificaRes736_2017_OCR_conFirmas.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones - República de Colombia. (16 de mayo de 2022). *Política de Gobierno Digital.* Recuperado el 09 de 2022, de MINTIC - Normatividad - Decretos (https://mintic.gov.co/portal/inicio/Normatividad/Decretos/): https://mintic.gov.co/portal/715/articles-210461_recurso_1.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC. (31 de octubre de 2019). *Arquitectura TI - MAE.G.GEN.01 – Documento Maestro.* Obtenido de Sitio del Manual Interactivo de la Política de Gobierno Digital: https://www.mintic.gov.co/arquitecturati/630/articles-144764_recurso_pdf.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC. (31 de octubre de 2019). *Arquitectura TI - MGGTI.G.GEN.01 – Documento Maestro.* Recuperado el 29 de septiembre de 2022, de Accedido a través del Manual Interactivo de la Política de Gobierno Digital: https://mintic.gov.co/arquitecturati/630/articles-9401_pdf_02.pdf

Niño Ospina, L. F. (28 de 09 de 2022). *Estudio técnico y tecnológico – mercado y precios, sobre la necesidad de actualización de las licencias del FIREWALL UTM USG110 ZYXEL.* Recuperado el 27 de 11 de 2022, de Contraloría Departamental del Tolima: https://contraloriatolima.gov.co/documentos/2022/otros/Estudio_Tecnico_Necesidad_Actualizaci%C3%B3n_Software_Firewall_20220928.pdf

Niño Ospina, L. F. (22 de septiembre de 2022). Estudio Técnico y Tecnológico sobre la Necesidad de Adquisición de Computadores Versión 4. Ibagué, Tolima, Colombia. Recuperado el 24 de 11 de 2022, de https://www.contraloriatolima.gov.co/documentos/2022/otros/EstudioTecnicoNecesidadComputadoras2022v4.pdf

Niño Ospina, L. F. (27 de septiembre de 2022). *Estudio Técnico y Tecnológico sobre la Necesidad de Adquisición de la Membresía, Pool de Direcciones IPv6 y ASN, con LACNIC.* Obtenido de Contraloría General del Departamento del Tolima: https://www.contraloriatolima.gov.co/documentos/2022/otros/Estudio_Tecnico_Necesidad_LACNIC_2022.pdf

Fuentes bibliográficas adicionales:

- Las ya indicadas en los pies de página.
- https://www.antivirusguide.com/best-antivirus/
- https://www.top10cybersecurity.com/
- https://blog.conzultek.com/licencia-symantec-endpoint
- https://www.nordsterntech.com/post/edr-vs-antivirus-diferencias-similitudes-y-cu%C3%A1l-fortalece-mejor-tu-ciberseguridad
- https://www.mcafee.com/es-co/antivirus/mcafee-total-protection.html
- https://go.kaspersky.com/es_mx_cloud2022.html
- https://www.sophos.com/es-es/products/endpoint-antivirus
- https://www.eset.com/es/empresas/pack-enterprise-protection/

11 LICENCIA SOBRE ESTE ESTUDIO TÉCNICO

Aunque este documento se considera un documento público de propiedad del Estado, el contenido del mismo se encuentra protegido por las normas legales vigentes respecto a propiedad intelectual, por lo que se autoriza el uso de este estudio técnico y tecnológico, según las condiciones de la licencia que se indica a continuación:

https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es