Asunto: INFORME TÉCNICO DEL CONTRATO CO1.PCCNTR.1475828 DE 2020

CUENTA DE COBRO No. 2 – CONTRATO CO1.PCCNTR.1475828 DE 2020

GENERALIDADES DEL CONTRATO

No. DE CONTRATO	CO1.PCCNTR.1475828 DE 2020
CONTRATISTA	INVERSIONES TECNOLOGISTICA S.A.S.
NIT	900.025.976-6
OBJETO	REALIZAR EL MANTENIMIENTO CORRECTIVO Y PREVENTIVO, CON BOLSA DE RESPUESTOS A TODO COSTO DE LOS EQUIPOS DE COMPUTO DE LA CAMARA DE REPRESENTANTES
VALOR	DOSCIENTOS VEINTICINCO MILLONES DE PESOS ($ 225.000.000)
ACTA DE INICIO	03 DE ABRIL DEL 2020
PLAZO	HASTA EL 31 DE DICIEMBRE DE 2020 Y/O HASTA AGOTAR EL PRESUPUESTO CONTRATADO

OBLIGACIONES DEL CONTRATISTA

PAGO DE OBLIGACIONES AL SISTEMA DE SEGURIDAD SOCIAL:

Revisado los documentos presentados con las facturas que pasa el contratista se encuentra que este adjunta certificación de paz y salvo con obligaciones referentes a los sistemas de salud, pensiones, ARL y obligaciones parafiscales suscrita por la representante legal expedida el 16 de juli del 2020. La empresa Inversiones Tecnologística ha cumplido con el pago de aportes y demás obligaciones legales respecto al sistema de seguridad social integral, y en el pago de aportes parafiscales (caja de compensación familiar, SENA e ICBF), de acuerdo a lo establecido en la Ley.

1. ACTIVIDADES DEL PERIODO INFORMADO

Revisadas las disposiciones del contrato NCO 1. PCCNTR. 1475828 se observa que el contratista **TECNOLOGISTICA S.A.S**. CUMPLIO a cabalidad con lo dispuesto en el contrato, haciendo entrega de:

Objetivo del documento

El presente documento tiene como objetivo presentar los resultados obtenidos luego del procedimiento de mantenimiento e instalación de las soluciones corporativas de ESET (cliente-servidor).

- Mantenimiento
- Instalación
- Configuración

Adicional también se informa el cumplimiento de la herramienta en cuanto al desarrollo de la misma se refiere y las características técnicas del producto.

Objetivos Específicos

1. Se estableció la programación para la ejecución de los mantenimientos preventivos, los mismos se realizaron desde el día 8 de julio al 31 de julio según el acuerdo establecido previamente con la entidad ya que se encontraron algunos equipos en riesgo y fue necesario hacerlo prontamente.
2. Se realizó el mantenimiento preventivo de HARDWARE Y SOFTWARE de los equipos informáticos, con las soluciones Endpoint de ESET. A continuación, se envía el informe y las evidencias de cómo se efectuaron los mantenimientos bajo la supervisión de los ingenieros Rodrigo Vargas y Jorge Iregui:

1. Mantenimientos ESET Endpoint Solutions

1. Se realizan mantenimientos e instalaciones necesaria de las soluciones Endpoint de ESET esto ayuda a la protección de los datos, a la navegación y se revisa que esté implementada en los sistemas operativos multiplataforma.
2. Se comprueba que el mantenimiento e instalación de la solución tenga los beneficios nombrados a continuación para que se pueda gozar de las bondades nombradas a continuación:

- Simple y directo
- Bajo consumo de recursos
- Fácil de administrar
- Antivirus y anti espía
- Sistema avanzado de prevención de intrusiones (HIPS)
- Control de dispositivos
- Análisis automático de medios extraíbles
- Protección multiplataforma
- Bajo consumo de recursos
- Múltiples formatos de registros
- Restauración de actualizaciones
- Administración remota
- Mensaje del Administrador
- Detección de redes de confianza
- Cortafuego bidireccional
- Instalación basada en componentes

- MDM Bloqueo remoto
- MDM Borrado remoto de datos
- MDM Comprobación de la tarjeta SIM
- MDM Contactos definidos como administrador
- MDM Protección contra la desinstalación
- MDM Protección en tiempo real
- MDM Análisis bajo demanda
- Funcionamiento mejorado
- Panel de control web en tiempo real
- Servidor local de actualizaciones.

Como beneficio para la entidad y ya que se carecía de este servicio se hace la Instalación de la consola de Administración de ESET Security Management Center, en la misma se podrá hacer la verificación de cada uno de los computadores, actualizaciones, configuraciones y verificaciones de cada uno de los elementos tecnológicos. De esta bondad de valor agregado se capacitó al Ingeniero Jorge Iregui, en la eventualidad que se necesite hacer otra capacitación a grupos o usuarios individuales se deberá solicitar por correo electrónico a Tecnologistica@gmail.com

En el siguiente enlace, se encuentra de una forma más detallada las descripciones de cada componente y/o módulo indicado en el listado anterior: https://cdn1.esetstatic.com/ESET/ES/Docs/Fichas/Empresas/ESET_Endpoint_Protecti on_ Advanced.pdf

2. Procedimiento de Mantenimiento e Instalación

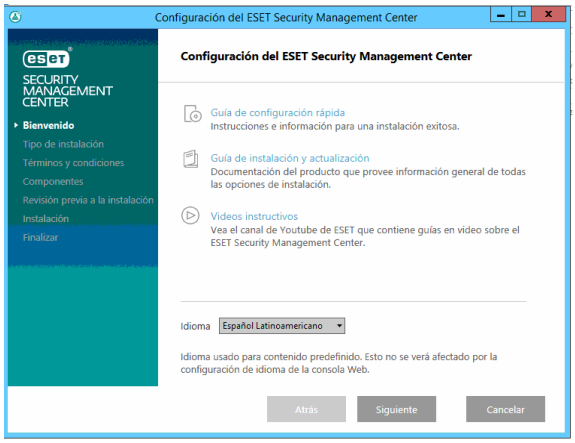
Se realizaron visitas y sesiones virtuales con el acompañamiento de los ingenieros de la Cámara de Representantes a través de:
meet.google.com/ebn-bwzo-kvz y Any desk

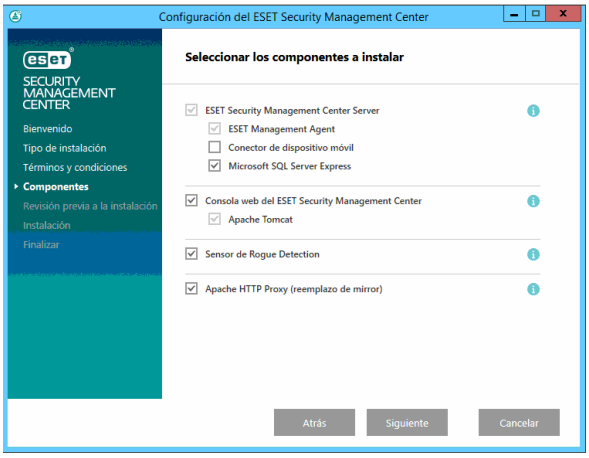
Los ingenieros que nos acompañaron en las reuniones se citan a continuación:

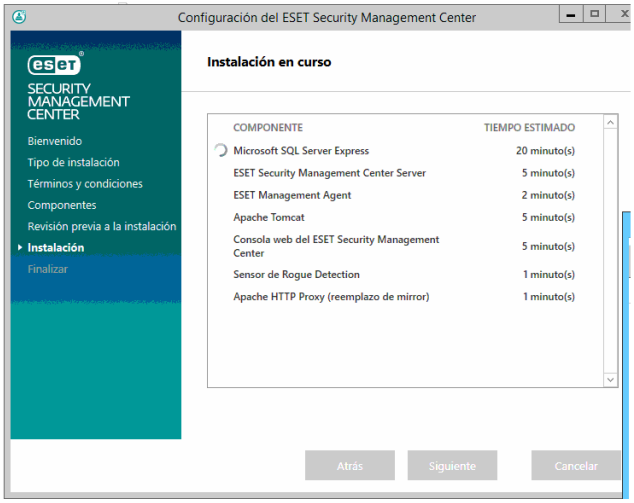
- Cámara de Representantes:
    - Ingeniero Jorge Iregui
    - Ingeniero Rodrigo Vargas
- Tecnologistica SAS:
    - Ingeniero. Mauricio Osorio.
    - Ingeniero Raanvalen Ramos

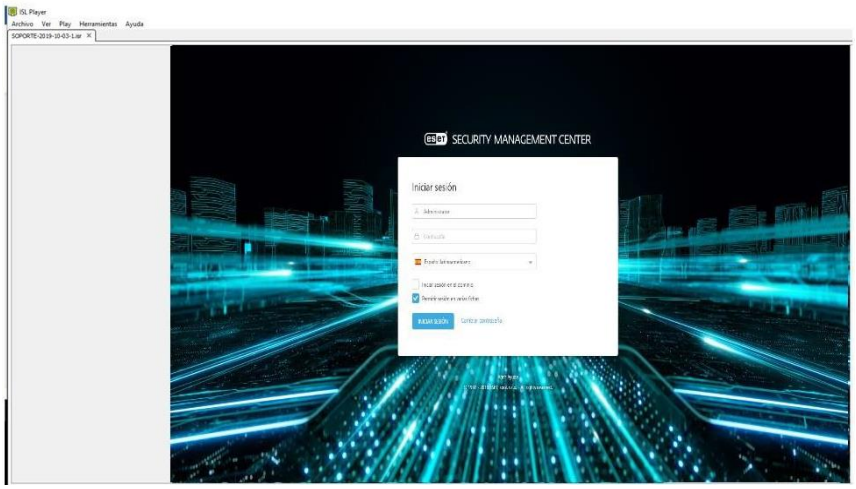
En estas sesiones y visitas se trataron los siguientes temas, de la misma manera se envían los pantallazos de las tareas realizadas:

- Alistamiento y mantenimiento de servidor para instalación de la última versión de la consola de administración. (7.2.1266.0 Server, 7.2.221.0 Consola Web)
- Descarga del software de instalación ESET Security Management Center.
- Descarga de Java.

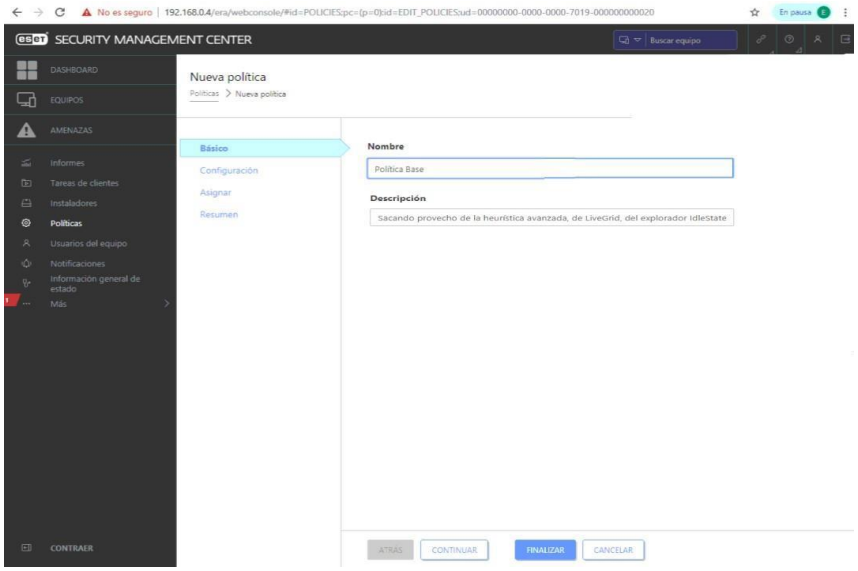




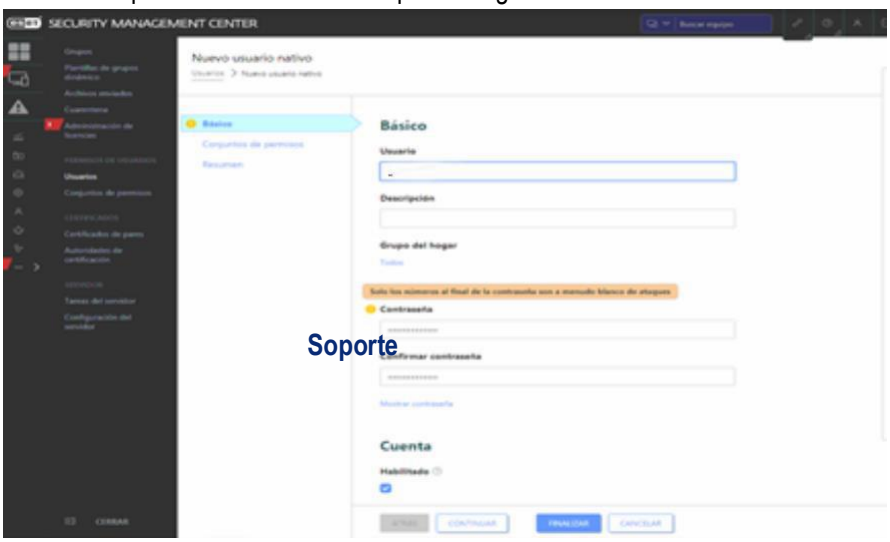


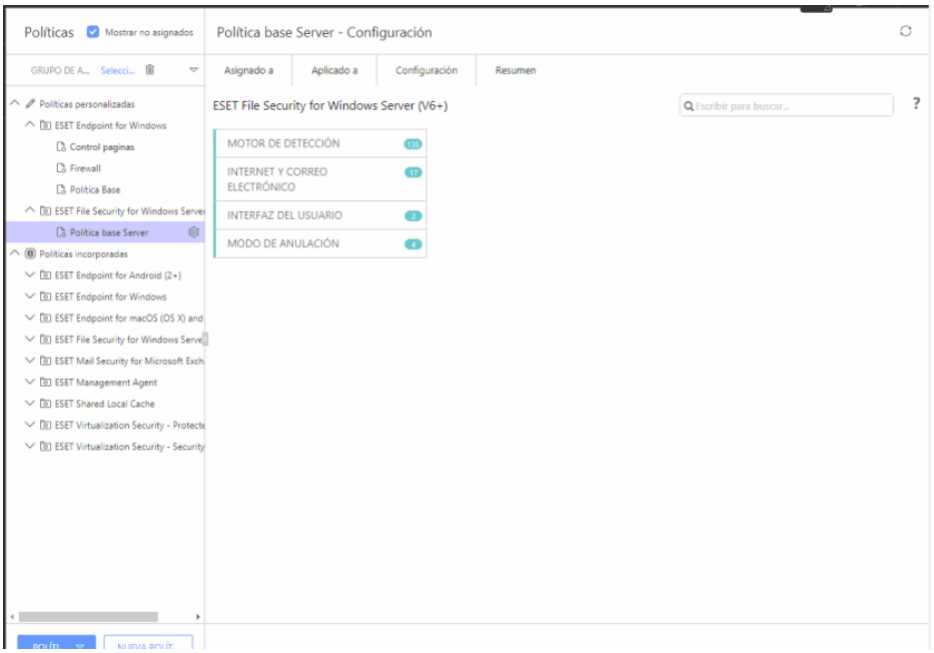


- Creación de políticas base.

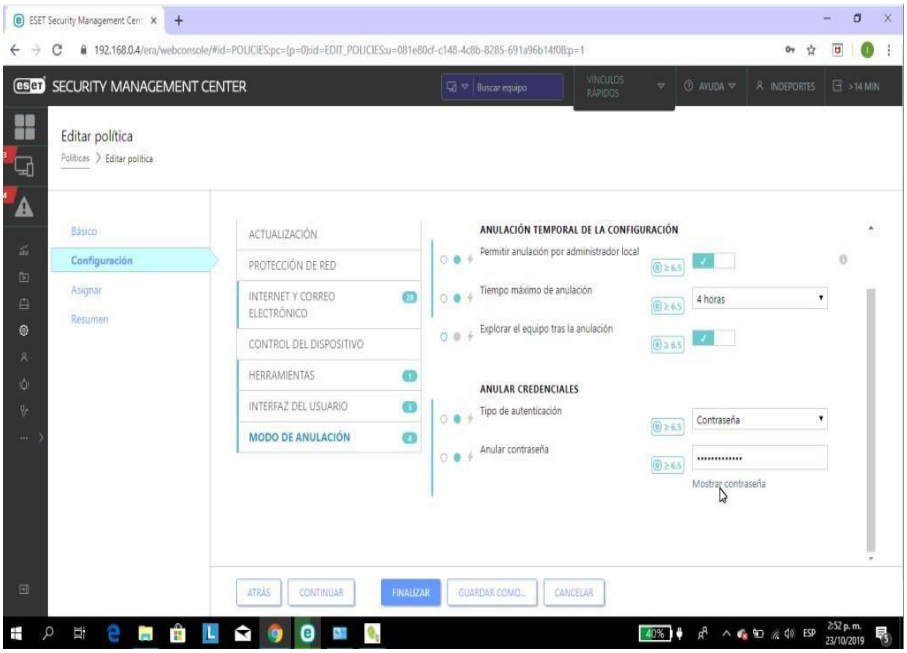


- Creación de usuario, para este caso se creó el usuario: “Soporte” para el personal de Mesa de Ayuda, suministrando las correspondientes credenciales para el ingreso a la consola de administración.



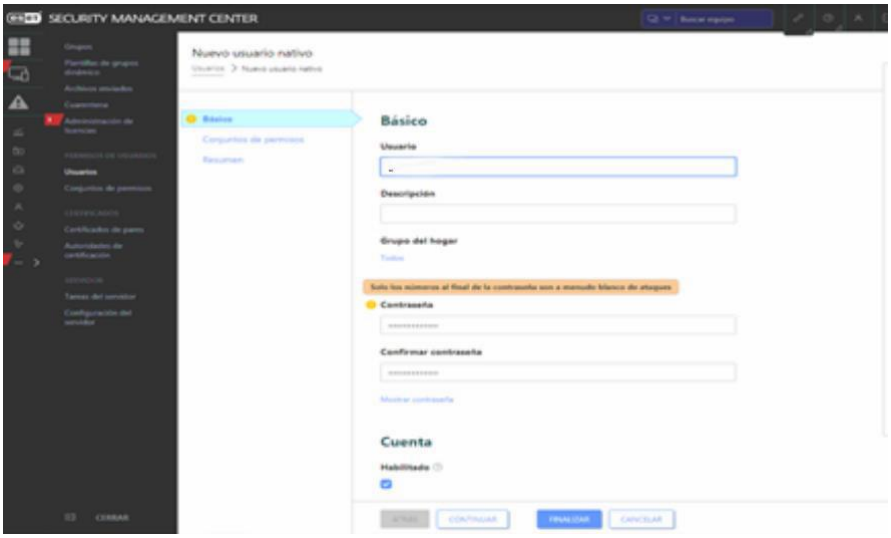


Finalmente, se hace la entrega y modificación del usuario Administrador, predefinido al momento de la instalación de la consola ESET Security Management Center, la nueva contraseña fue indicada por el Ing. Rodrigo Vargas, igualmente indico las contraseñas para la anulación de políticas.



- Se realizó el procedimiento de creación de instaladores para las estaciones de trabajo, posteriormente se procedió a realizar la verificación exitosa de los instaladores.

Se crearon los instaladores para la instalación del producto en los Endpoint o estaciones.
La versión creada corresponde a la última versión



7.3.2036, en el caso de los Server la versión es 7.1.1210.

- Se realizo el mantenimiento preventivo del FIREWALL incluido fortiCare plus Applicatión control, IPS, AV, WEB FILTERING AND ANTISPAM, FORTISANDBOX CLOUD, bajo la supervisión de los profesionales encargados de la Cámara los señores CAMILO RAMÍREZ CASTIBLANCO y JORGE IREGUI, y por otra parte el encargado de la solución tecnológica de nuestra empresa el Ingeniero SERGIO ANDRÉS PERDOMO, arquitecto de soluciones.

Se envía la evidencia del trabajo realizado

3. Evidencia e informe del mantenimiento e instalación del firewall.

A los Veinte (20) días de junio del año 2020, se realizó bajo la supervisión del Ing. CAMILO RAMÍREZ CASTIBLANCO, en su calidad de PROFESIONAL ENCARGADO y el Ing. SERGIO ANDRÉS PERDOMO identificado con la cédula de ciudadanía N° 1.098.770.149 en representación de nuestra empresa se realiza la renovación y mantenimiento de la solución de las licencias de Fortinet asociadas a la descripción que se encuentra a continuación:

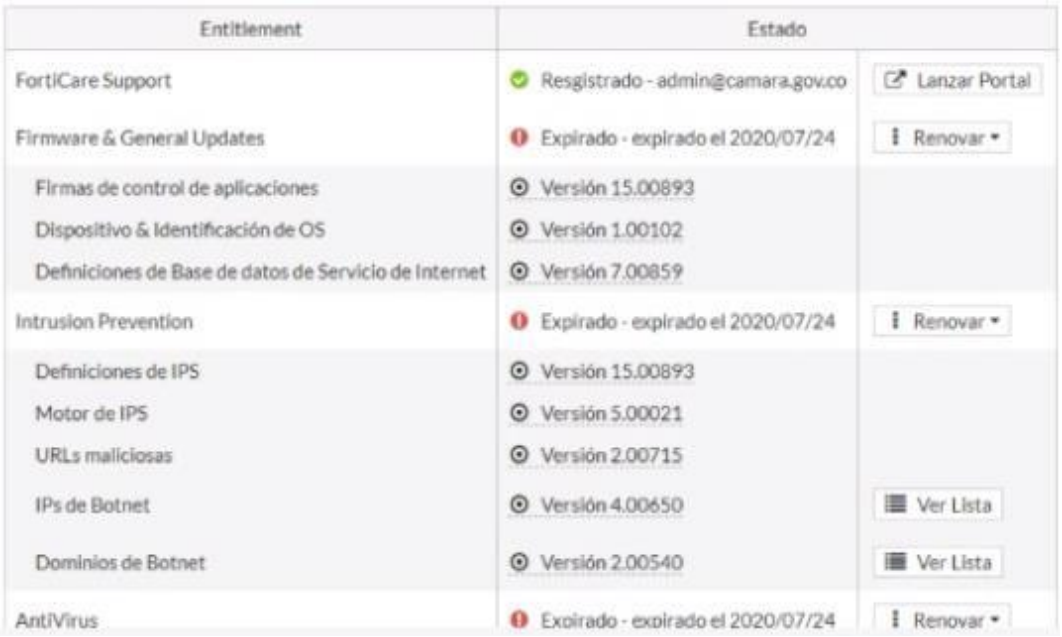
I. Descripción:

PRODUCTO	CANT	DESCRIPCIÓN	ESTADO
FC-10-F6H1E-950-02-12	1	1 Year coverage for FortiGate 601E include: Hardware Advanced HW Firmware & General Updates Enhanced Support 24x7 Telephone Support 24x7 Advanced Malware Protection NGFW Web Filtering AntiSpam	ACTIVADO

II. CONSTANCIA DEL PROCEDIMIENTO:

ANTES:

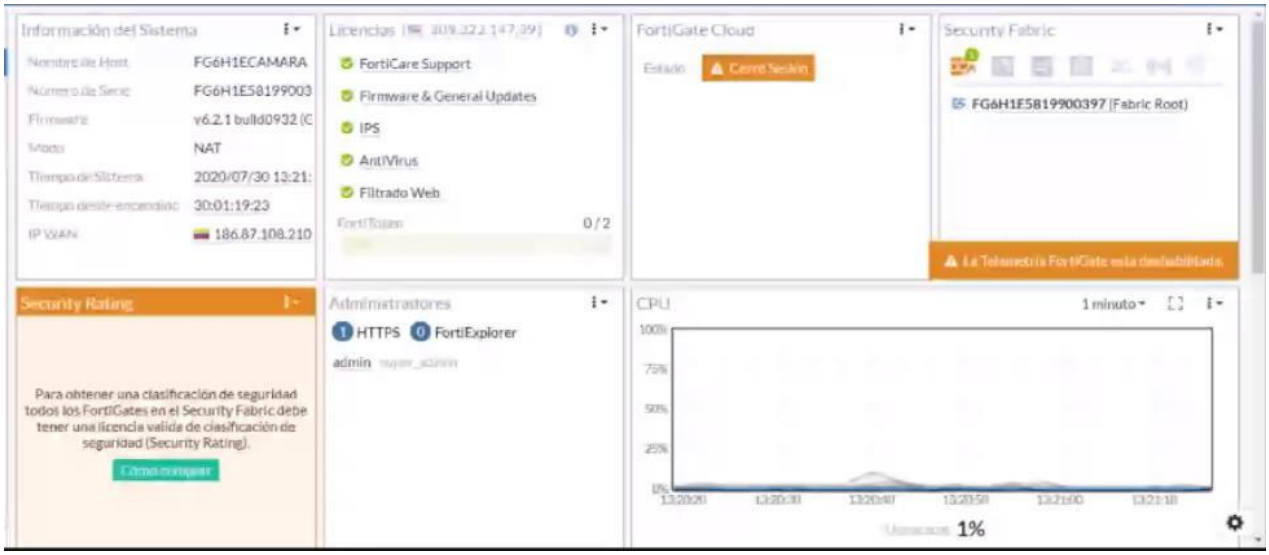
El día 24 de Julio de 2020, expiró la licencia relacionada al Fortigate FC-10-F6H1E-950- 02-12.



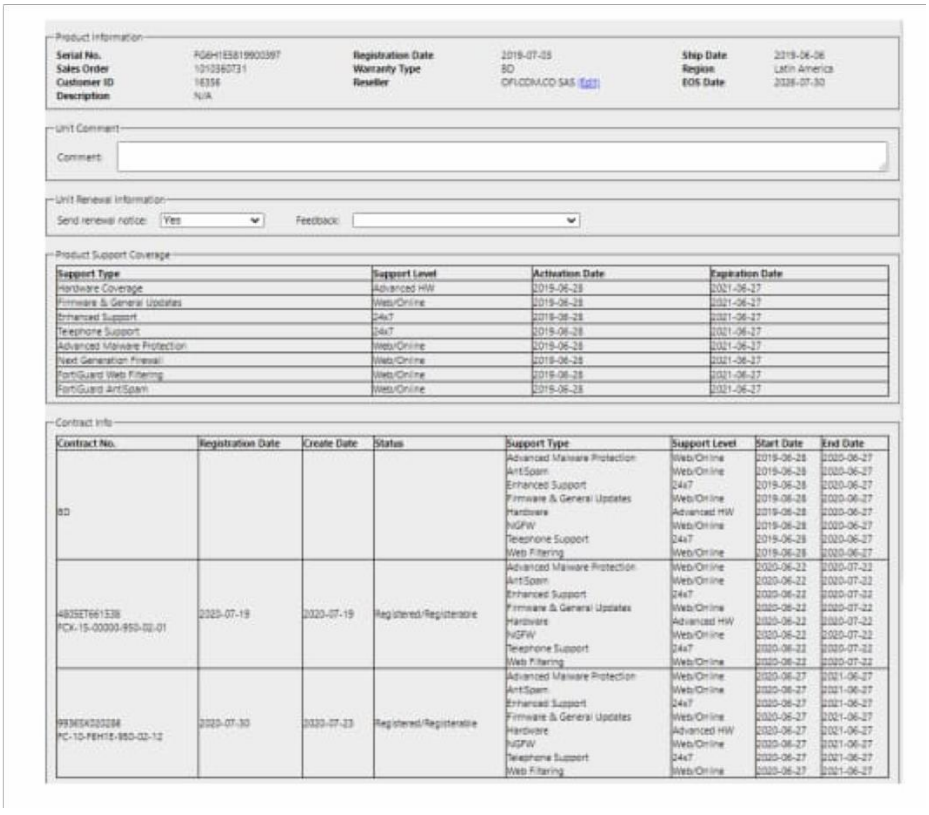
Entitlement	Estado	
FortiCare Support	Resgistrado - admin@camara.gov.co	Lanzar Portal
Firmware & General Updates	Expirado - expirado el 2020/07/24	Renovar
Firmas de control de aplicaciones	Versión 15.00893	
Dispositivo & Identificación de OS	Versión 1.00102	
Definiciones de Base de datos de Servicio de Internet	Versión 7.00859	
Intrusion Prevention	Expirado - expirado el 2020/07/24	Renovar
Definiciones de IPS	Versión 15.00893	
Motor de IPS	Versión 5.00021	
URLs maliciosas	Versión 2.00715	
IPs de Botnet	Versión 4.00650	Ver Lista
Dominios de Botnet	Versión 2.00540	Ver Lista
AntiVirus	Expirado - expirado el 2020/07/24	Renovar

DESPUÉS:

Se procede a la activación y actualización de la licencia de renovación asociada al Forigate FC-10-F6H1E-950-02-12



Verificado lo anteriormente descrito, se deja Constancia que los bienes detallados se recibieron a satisfacción.



Product Information

Serial No.	FG6H1E5819900397	Registration Date	2019-07-05	Ship Date	2019-06-06
Sales Order	1013360731	Warranty Type	BD	Region	Latin America
Customer ID	16356	Reseller	CPUCOM.CO SAS (Edit)	EOS Date	2026-07-30
Description	N/A				

Unit Comment

Comment:

Unit Renewal Information

Send renewal notice: Yes Feedback:

Product Support Coverage

Support Type	Support Level	Activation Date	Expiration Date
Hardware Coverage	Advanced HW	2019-06-28	2021-06-27
Firmware & General Updates	Web/Online	2019-06-28	2021-06-27
Enhanced Support	24x7	2019-06-28	2021-06-27
Telephone Support	24x7	2019-06-28	2021-06-27
Advanced Malware Protection	Web/Online	2019-06-28	2021-06-27
Next Generation Firewall	Web/Online	2019-06-28	2021-06-27
FortiGuard Web Filtering	Web/Online	2019-06-28	2021-06-27
FortiGuard AntiSpam	Web/Online	2019-06-28	2021-06-27

Contract Info

Contract No.	Registration Date	Create Date	Status	Support Type	Support Level	Start Date	End Date
BD				Advanced Malware Protection	Web/Online	2019-06-28	2020-06-27
				AntiSpam	Web/Online	2019-06-28	2020-06-27
				Enhanced Support	24x7	2019-06-28	2020-06-27
				Firmware & General Updates	Web/Online	2019-06-28	2020-06-27
				Hardware	Advanced HW	2019-06-28	2020-06-27
				NGFW	Web/Online	2019-06-28	2020-06-27
				Telephone Support	24x7	2019-06-28	2020-06-27
				Web Filtering	Web/Online	2019-06-28	2020-06-27
4835ET661338 FCX-15-00000-950-02-01	2020-07-19	2020-07-19	Registered/Registerable	Advanced Malware Protection	Web/Online	2020-06-22	2020-07-22
				AntiSpam	Web/Online	2020-06-22	2020-07-22
				Enhanced Support	24x7	2020-06-22	2020-07-22
				Firmware & General Updates	Web/Online	2020-06-22	2020-07-22
				Hardware	Advanced HW	2020-06-22	2020-07-22
				NGFW	Web/Online	2020-06-22	2020-07-22
				Telephone Support	24x7	2020-06-22	2020-07-22
				Web Filtering	Web/Online	2020-06-22	2020-07-22
9936DX203284 FC-10-F6H1E-950-02-12	2020-07-30	2020-07-23	Registered/Registerable	Advanced Malware Protection	Web/Online	2020-06-27	2021-06-27
				AntiSpam	Web/Online	2020-06-27	2021-06-27
				Enhanced Support	24x7	2020-06-27	2021-06-27
				Firmware & General Updates	Web/Online	2020-06-27	2021-06-27
				Hardware	Advanced HW	2020-06-27	2021-06-27
				NGFW	Web/Online	2020-06-27	2021-06-27
				Telephone Support	24x7	2020-06-27	2021-06-27
				Web Filtering	Web/Online	2020-06-27	2021-06-27

4. ALCANCES CONSEGUIDOS CON LAS INSTALACIONES Y MANTENIMIENTOS DE LOS SOFTWARE INSTALADOS.

Con los mantenimientos efectuados se pretende Disminuir las fallas y daños físicos y se mejora la eficiencia en todos los equipos informáticos y de telecomunicaciones.

Se mejora notablemente la eficiencia de todos los equipos tecnológicos haciéndolos más rápidos en todos los procesos, los usuarios tienen ahora la oportunidad de optimizar el tiempo de trabajo en los mismos.

Se establecen los mecanismos con los que se evalúan las condiciones generales de todos los equipos de la informática, al actualizar y hacer los mantenimientos del software de los equipos estos quedan en muy buena condición para el trabajo.

5. PROCEDIMIENTOS REALIZADOS EN EL MANTENIMIENTO DEL SOFTWARE

Los Procedimientos realizados en el mantenimiento preventivo de Software fueron:

Sobre el sistema operativo.

1. Se hizo la instalación de los parches de actualización y seguridad del Software para que puedan correr mejor los programas.
2. Se efectuaron los respectivos vaciados de las papeleras de reciclaje que fueron autorizadas por los usuarios.
3. Se hizo la respectiva eliminación de todos los archivos temporales de todos los equipos en mantenimiento.
4. Se efectuó la respectiva depuración y limpieza de los escritorios de los equipos en mantenimiento.
5. Se depuraron y limpiaron todos los programas no autorizados por la entidad.
6. Se verifico e instaló la imagen o papel tapiz del escritorio de la Entidad.
7. Se efectuó una limpieza de los registros del Software y aplicativos innecesarios del inicio del equipo para que funcione más rápido al momento de su encendido.
8. Se actualizó y se hizo un posterior análisis de sistema con antivirus para corroborar que estuviera corriendo bien dentro de cada equipo de la entidad.
9. Se efectuó una Revisión de cada uno de los discos duros (chkdsk c: - desde CMD) de cada equipo de la Entidad.
10. Se activó la directiva de contraseñas cumpliendo requisitos de complejidad establecidos por la Entidad.
11. Se limpió después de pedir autorización, el historial de ventanas de cada equipo de la Entidad.

12. Se Desinstalaron las aplicaciones no permitidas por la entidad, sin licencia o versiones trial.
13. Se creó el punto de restauración para los equipos.

Para brindar una seguridad en cada uno de los equipos y que únicamente el usuario asignado conozca dicha contraseña, se realizaron las configuraciones respectivas en cada equipo de la entidad.

Navegadores

1. Se Verifican los sitios más frecuentes en los navegadores utilizados.
2. Se efectuó en cada equipo la eliminación de todos los temporales innecesarios para que fluya más rápido la información en el equipo.
3. Se elimina el historial no necesario en los equipos autorizado por los usuarios.
4. Se realizó en todos los equipos la eliminación de las cookies que no eran necesarias.
5. Se quitan todas las extensiones de los equipos que no son útiles para las labores diarias.
6. Se eliminan las descargas que fueron hechas con mucho tiempo de anterioridad en los equipos y no eran necesarias.
7. Se instala o actualiza en cada uno de los equipos los programas de Adobe flash y Java y demás aplicativos que sean necesarios.

Al finalizar cada uno de los procedimientos se hizo en presencia del funcionario asignado, y se documentó el mantenimiento preventivo.

6. PROCEDIMIENTOS REALIZADOS EN EL MANTENIMIENTO DEL FIREWALL

Procedimientos recomendados y realizados en el mantenimiento preventivo del FIREWALL incluido fortiCare plus Application control, IPS, AV, WEB FILTERING AND ANTISPAM, FORTISANDBOX CLOUD:

Se verificó que el firewall quedara en óptimas condiciones para que los sistemas tengan un correcto funcionamiento de las comunicaciones de datos, un adecuado aprovechamiento de los anchos de banda y eliminación de retardos, bucles y cuellos de botella, así como la securización de la red tanto de cara al exterior como usos indebidos desde el interior.

En el mantenimiento preventivo se hicieron test de diagnóstico y pruebas de servicio completo, que identificaron los posibles errores ocultos, los mismos se subsanaron y quedaron verificados para evitar averías y disfunciones tanto físicas como lógicas de los equipos, este mantenimiento se realizó mediante la reparación, sustitución de los elementos afectados y/o reconfiguración lógica de los equipos. Estos test se realizarán dos veces al año sin cargo a las horas de asistencia técnica.

Para realizar las revisiones que requieran una parada planificada, se solicitaran previa conformidad o acuerdo con la

Unidad de Coordinación de Sistemas y Tecnologías de la Información.

El mantenimiento preventivo se acomodará en todo lo posible a las especificaciones y parámetros del fabricante del equipo.

Para finalizar todos los procedimientos realizados, incluido el mantenimiento preventivo del Hardware, software y firewall se verificó el buen funcionamiento de los mismos en cada uno de los equipos, con el acompañamiento del funcionario de la Entidad el Ingeniero Jorge Iregui. Los equipos se entregaron al funcionario asignado, El cual dio su visto bueno del funcionamiento de los mismos.

La empresa Inversiones Tecnologistica SAS y sus ingenieros finalizaron los mantenimientos e instalaciones y quedan a disposición de ustedes para realizar las capacitaciones necesarias del producto, afinamiento, configuración y soporte en el momento que sea requerido y necesario por la entidad.

La empresa Inversiones Tecnologistica SAS y sus ingenieros finalizaron los mantenimientos e instalaciones, adicional se encontrarán disponibles para realizar las capacitaciones necesarias del producto, afinamiento, configuración y soporte en el momento que sea requerido y necesario por la entidad.

CUMPLIMIENTO:

Teniendo en cuenta los documentos aportados y/o requeridos, y a la validación en sitio realizada por los ingenieros asignados por parte de la OPS y a la validación de la ejecución de las actividades realizadas por el contratista, se manifiesta que este cumplió con las actividades de acuerdo a lo acordado dentro del contrato.

De acuerdo a:

Objetivos Específicos

a) Establecer la programación para la ejecución de los mantenimientos preventivos.
b) Realizar el mantenimiento preventivo de HARDWARE Y SOFTWARE de los equipos informáticos.
c) Realizar mantenimiento preventivo del FIREWALL incluido fortiCare plus Application control, IPS, AV, WEB FILTERING AND ANTISPAM, FORTISANDBOX CLOUD.
d) Disminuir los costos por fallas o daños físicos de los equipos informáticos y de telecomunicaciones.
e) Mejorar la eficiencia y eficacia en el soporte tecnológico de los equipos.
f) Establecer los mecanismos para evaluar las condiciones generales de los equipos informáticos.

- **Procedimientos recomendados a realizar en el mantenimiento preventivo de Software:**

- **Sistema operativo**

1. Hacer instalación de parches de actualización y seguridad del SO.
2. Vaciar papelera de reciclaje.
3. Eliminar temporales de equipo.
4. Depuración y limpieza de escritorio.
5. Depuración y limpieza de programas (Eliminar programas no autorizados por la OPS).
6. Verificar papel tapiz del escritorio de la HCR.

7. Ejecutar limpieza del registro del SO y aplicativos innecesarios del inicio del mismo.
8. Actualización y posterior análisis de sistema con antivirus.
9. Revisión de disco duro (chkdsk c: - desde CMD).
10. Activar directiva de contraseñas cumpliendo requisitos de complejidad establecidos por la OPS.
11. Limpiar historial de ventanas.
12. Desinstalar aplicaciones no permitidas por la OPS, sin licencia o versiones trial.
13. Crear punto de restauración.

Durante el acompañamiento y supervisión realizada se observó que fueron cumplidos.

La presente se expide a los treinta y uno de julio (31) días del mes de julio del 2020.

Cordialmente,



JORGE ANDRÉS IREGUI TORO
Ing. De soporte - Contratista