
 UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS	INFORME DE SUPERVISIÓN	Código: GC-PR-003-FR-036	 Sistema Integrado de Gestión
	Macroproceso: Gestión de Recursos	Versión 01	
	Proceso: Gestión Contractual	Fecha de Aprobación: 21/06/2019	

FORMATO INFORME DE SUPERVISIÓN

FECHA ELABORACIÓN DEL INFORME

07

06

2024



DIA

MES

AÑO

INFORME SUPERVISIÓN DEL 01 AL 31 DE MAYO DEL AÑO 2024

1. INFORMACIÓN GENERAL	
No. de Contrato	CONTRATO DE PRESTACIÓN DE SERVICIOS NO. 2038 DEL 21 DE DICIEMBRE DE 2023
OBJETO	ADQUIRIR, INSTALAR, CONFIGURAR Y PUESTA EN CORRECTO FUNCIONAMIENTO DE COMPONENTES QUE PERMITAN DAR CONTINUIDAD Y MEJORAMIENTO A LA SEGURIDAD INFORMÁTICA DEL PARQUE INFORMÁTICO PROPIEDAD DE LA UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS, CONFORMADOS POR: COMPONENTE UNO: DETECCIÓN, PREVENCIÓN Y RESPUESTA DE RED (NDR) Y COMPONENTE DOS: SOFTWARE DE SEGURIDAD ANTIVIRUS.
CONTRATISTA	UNIÓN TEMPORAL INFOCOMUNICACIONES S.A.S - LAN SECURITY NETWORKS S.A.S
NIT CONTRATISTA	Nit No. 901.783.379-3, sociedad compuesta por las empresas INFO COMUNICACIONES S.A.S identificada con Nit No. 830.044.415-3 y LAN SECURITY NETWORKS S.A.S identificada con Nit No. 900.505.780-1
NOMBRE REPRESENTANTE LEGAL	BIBIANA DEVIA CAMELO
C.C.	51.890.948
NOMBRE REPRESENTANTE LEGAL ACTUAL	BIBIANA DEVIA CAMELO
C.C.	51.890.948
FECHAS DE PERFECCIONAMIENTO Y LEGALIZACIÓN	21 de diciembre del 2023
PLAZO INICIAL DEL CONTRATO	El plazo para la ejecución será el siguiente: Para el componente 1: El plazo para la ejecución del contrato es de dos (2) meses para realizar la adquisición, instalación, configuración, y puesta en correcto funcionamiento de la solución seguridad informática. El tiempo total del contrato que incluye licenciamiento y servicio de soporte de la solución será por doce (12) meses, así como lo los dos (2) meses de instalación y configuración de la solución. Para el componente 2: El plazo para la ejecución del contrato es de dos (2) meses para realizar la adquisición, instalación, configuración, y puesta en correcto funcionamiento de la solución seguridad informática. El tiempo total del contrato que incluye licenciamiento y servicio de soporte de la solución será por veinticuatro (24) meses, así como lo los dos (2) meses de instalación y configuración de la solución.
TOTAL PRORROGAS	0
TOTAL SUSPENSIONES	0
VALOR TOTAL DEL CONTRATO	El valor del presente contrato corresponde a la suma de MIL SIETE MILLONES TRESCIENTOS TREINTA Y SEIS MIL CIENTO NOVENTA PESOS M/CTE (\$1.007.336.190) distribuidos así: • Componente 1: SEISCIENTOS NOVENTA MILLONES DOSCIENTOS MIL PESOS (\$690.200.000), valor que incluye el IVA y demás impuestos, tasas, contribuciones, costos directos e indirectos • Componente 2: TRESCIENTOS DIECISIETE MILLONES CIENTO TREINTA Y SEIS MIL CIENTO NOVENTA PESOS (\$317.136.190), valor que incluye el IVA y demás impuestos, tasas, contribuciones, costos directos e indirectos.
ADICION	\$ 0

 UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS	INFORME DE SUPERVISIÓN	Código: GC-PR-003-FR-036	
	Macroproceso: Gestión de Recursos	Versión 01	
	Proceso: Gestión Contractual	Fecha de Aprobación: 21/06/2019	



FECHA ACTA DE INICIO	28 de diciembre de 2023
FECHA TERMINACIÓN DEL CONTRATO	27 de diciembre de 2025

2. INFORMACION PRESUPUESTAL		
DISPONIBILIDAD PRESUPUESTAL		
CERTIFICADO (S) DE DISPONIBILIDAD PRESUPUESTAL No.	Fecha Expedición	Valor
4065	08 de noviembre de 2023	\$ 321.000.000
4066	08 de noviembre de 2023	\$ 698.886.665
CERTIFICADO (S) DE REGISTRO PRESUPUESTAL No.	Fecha Expedición	Valor
10021	26 de diciembre de 2023	\$ 690.200.000
10022	26 de diciembre de 2023	\$ 317.136.190
INFORMACION PRESUPUESTAL DE ADICIONES		
CERTIFICADO (S) DE DISPONIBILIDAD PRESUPUESTAL No.	Fecha Expedición	Valor
No aplica	No aplica	No aplica
CERTIFICADO (S) DE REGISTRO PRESUPUESTAL No.	Fecha Expedición	Valor
No aplica	No aplica	No aplica

3. DATOS DEL SUPERVISOR		
NOMBRE	Martha Cecilia Valdés Cruz	
CARGO	Líder Red de Datos UDNET	
SEDE	Sede Aduanilla de Paiba	
CORREO ELECTRONICO	udnet@udistrital.edu.co	
TELEFONO	3239300	EXT. 1301
ACTO DE DESIGNACIÓN (Si aplica)	No aplica	

4. DATOS DE LA PÓLIZA						
COMPAÑÍA ASEGURADORA	Seguros del Estado S.A.					
NÚMERO DE POLIZA	21-45-101432466					
FECHA DE APROBACIÓN DE PÓLIZA	DIA	02	MES	01	AÑO	2024

POLIZA ACTA DE INICIO							
TIPO DE AMPAROS	VALOR ASEGURADO (\$)	VIGENCIA					
		FECHA INICIAL			FECHA FINAL		
		DÍA	MES	AÑO	DÍA	MES	AÑO
Cumplimiento	\$ 201.467.238.00	28	12	2023	28	06	2026
Salarios y Prestaciones Sociales	\$ 100.733.619.00	28	12	2023	28	02	2029
Calidad y correcto funcionamiento del bien o Servicio	\$ 201.467.238.00	SI AMPARA 2 AÑOS, 0 MESES Y -1 DÍAS- ESTE AMPARO INICIA VIGENCIA UNA VEZ SE HA FINALIZADO LA EJECUCION DEL CONTRATO Y/O CON LA FIRMA DEL ACTA DE ENTREGA A SATISFACCION DEL MISMO CON EL PRESENTE ANEXO Y SEGUN ACTA DE INICIO DE FECHA 28/12/2023, SE AJUSTAN LAS VIGENCIAS DE LOS AMPAROS ARRIBA DESCRITOS.					

 UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS	INFORME DE SUPERVISIÓN	Código: GC-PR-003-FR-036	 SIGUD
	Macroproceso: Gestión de Recursos	Versión 01	
	Proceso: Gestión Contractual	Fecha de Aprobación: 21/06/2019	

5. BALANCE FINANCIERO

De acuerdo con la ejecución del contrato, los recursos presentan el siguiente balance financiero:

VALOR INICIAL DEL CONTRATO:	\$ 1.007.336.190
VALOR ADICIONADO:	\$ 0
VALOR TOTAL DEL CONTRATO:	\$ 1.007.336.190
VALOR PAGADO AL CONTRATISTA:	\$ 0
VALOR EJECUTADO Y POR PAGAR AL CONTRATISTA:	\$ 1.007.336.190
VALOR NO EJECUTADO Y A LIBERAR A FAVOR DE LA UNIVESIDAD	No Aplica

5.1. GESTIÓN DE PAGOS

De acuerdo con el desarrollo de la ejecución de la Orden de Servicios N°. 2038-2023, hasta la fecha no se han realizado pagos.

5.1. AVANCE FINANCIERO DEL CONTRATO:

Recursos girados: (relacionar los pagos realizados a la fecha del informe)

Porcentaje de pagos realizados: 0%

Porcentaje de pagos pendientes a realizar: 100%

5.2. AVANCE EN CUMPLIMIENTO DE EJECUCION DEL CONTRATO

Plazo Inicial: 2 Meses

Porcentaje avance en tiempo: 100 %

Porcentaje de ejecución (en relación con los bienes y/o servicios recibidos): 100 %

5.3. AVANCE FISICO DEL CONTRATO:

ACTIVIDADES REALIZADAS:

Para este periodo se desarrollaron las siguientes actividades en el marco de la Orden de Servicio No. 2038- 2023:



- Monitoreo de alertas en el componente Kaspersky Anti Targeted Attack Platform.
- Inclusión de equipos en las consolas de antivirus respectivas.
- Afinación configuraciones Kaspersky Security Mail Gateway y Kaspersky Web Traffic Security.
- Se revisó la documentación relacionada para el pago del contrato, dichos documentos se pueden revisar en la siguiente ruta \\10.40.25.200\seguimientocontratos\$\Contratos_Juridica\CONTRATO DE PRESTACION DE SERVICIOS 2038-2023\

NOTA: Para ingresar es necesario tener Cuenta de dominio udistrital.edu.co y pertenecer a las áreas de Jurídica o Red de Datos UDNET

6. INCUMPLIMIENTO DEL CONTRATISTA O PROBLEMAS EN LA EJECUCION ATRIBUIBLES AL CONTRATISTA:

No ☒ SI ☐

Describir brevemente los hechos de incumplimiento y las acciones emprendidas:

 UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS	INFORME DE SUPERVISIÓN	Código: GC-PR-003-FR-036	 SIGUD Sistema Integrado de Gestión
	Macroproceso: Gestión de Recursos	Versión 01	
	Proceso: Gestión Contractual	Fecha de Aprobación: 21/06/2019	

7. INCUMPLIMIENTO POR PARTE DE LA UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS EN LA EJECUCION ATRIBUIBLES A LA UNIVERSIDAD

No ☐ X ☒ SI ☐

Describir sucintamente los hechos de incumplimiento y las acciones emprendidas:

8. LA EJECUCION DEL CONTRATO ESTA ESTRUCTURADO SOBRE UN CRONOGRAMA DE ACTIVIDADES:

No ☐ X ☒ SI ☐

En caso afirmativo deberá anexarse el cronograma con el porcentaje de avance de cada tarea o actividad.

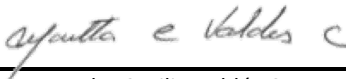
NOTA: Como supervisor del contrato certifico que el contratista se encuentra desarrollando a satisfacción las actividades inherentes a la ejecución del contrato de prestación de servicios N° 2038 – 2023, sin presentar ningún contratiempo y cumpliendo con las condiciones establecidas en el contrato.

Con el presente informe y de acuerdo con lo establecido en los numerales 32 y 33 del Artículo 18° de la Resolución de Rectoría No. 629 de 2016- Manual de Interventoría y Supervisión, certifico que los informes físicos, técnicos, financieros y administrativos sobre el avance de la ejecución del objeto contractual, así como los demás documentos del proceso, reposan en el expediente del contrato de prestación de servicios N° 2038 del 2023.

Al presente informe se anexan los siguientes documentos:

- 05.01. DT - Informes de Implementacion C2038-2023.pdf, Folios (52)
- 05.02. FEV-1 - C2038-2023.pdf, Folios (1)
- 05.02. FEV-3 - C2038-2023.pdf, Folios (1)

Por lo anterior se firma a los **07** días del mes de **Junio** de **2024**.

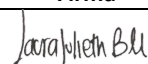
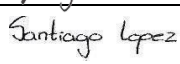


Martha Cecilia Valdés Cruz
Líder Unidad Red de Datos
UDNET Supervisor



Alejandro Paolo Daza Corredor
Jefe Oficina Asesora de Tecnologías e
Información

Supervisor de la Orden de Servicios N°. 2038 – 2023

	Nombre	Cargo y/o vinculación	Firma
Revisó	Laura Julieth Betancourt	CPS UDNET	
Elaboró	Santiago López Gómez	CPS UDNET	
	Juan Sebastian Gil B	CPS UDNET	JUAN SEBASTIAN GIL B.

The Kaspersky logo, consisting of the word "kaspersky" in a lowercase, bold, sans-serif font. The background of the slide features a teal-to-green gradient with a large, white, abstract geometric shape that resembles a stylized shield or a piece of paper with rounded corners.

INSTALACIÓN DE KASPERSKY ANTI TARGETED ATTACK PLATFORM

Índice

- 1. OBJETIVOS 3
- 2. PRODUCTOS 3
- 3. ESTRUCTURA 4
 - 3.1 Diagrama de tráfico 4
 - 3.2 Informaciones de los servidores 7
 - 3.3 Implementación de Kaspersky Anti Targeted Attack Platform..... 8
- 4. CONCLUSIÓN..... 28

1. Objetivos

Documentar todas las configuraciones realizadas durante la fase de implementación del productor Kaspersky Anti Targeted Attack Platform.

2. Productos

Kaspersky Anti Targeted Attack Platform: es una solución que facilita la detección temprana de ataques dirigidos, amenazas persistentes avanzadas (APT), ataques de día cero y otras amenazas sofisticadas. Kaspersky Anti Targeted Attack Platform está compuesta por dos bloques funcionales: Kaspersky Anti Targeted Attack (en adelante también denominada KATA) y Kaspersky Endpoint Detection and Response (en adelante también denominada KEDR). KEDR puede comprarse por separado.

3. Estructura

3.1 Diagrama de arquitectura original

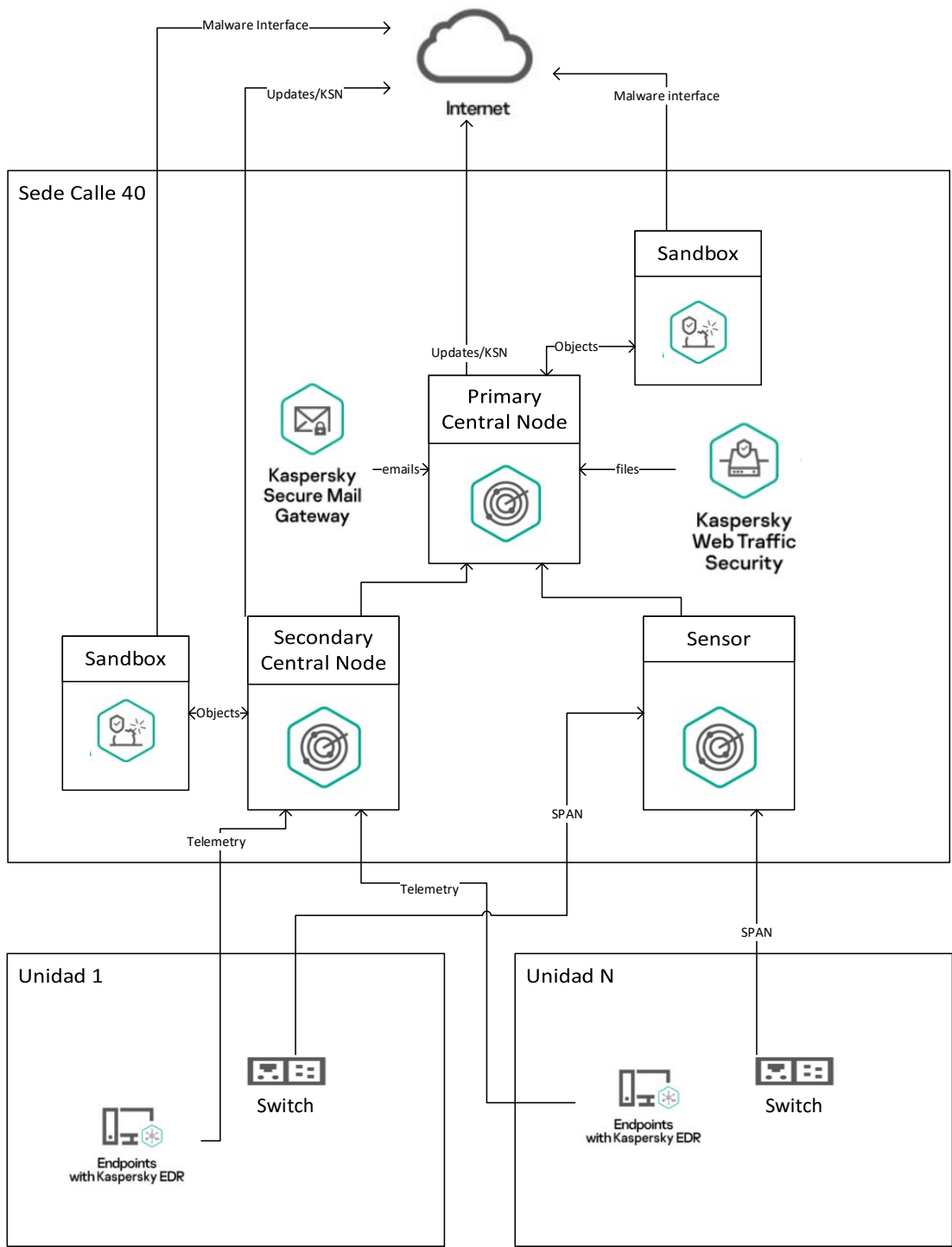
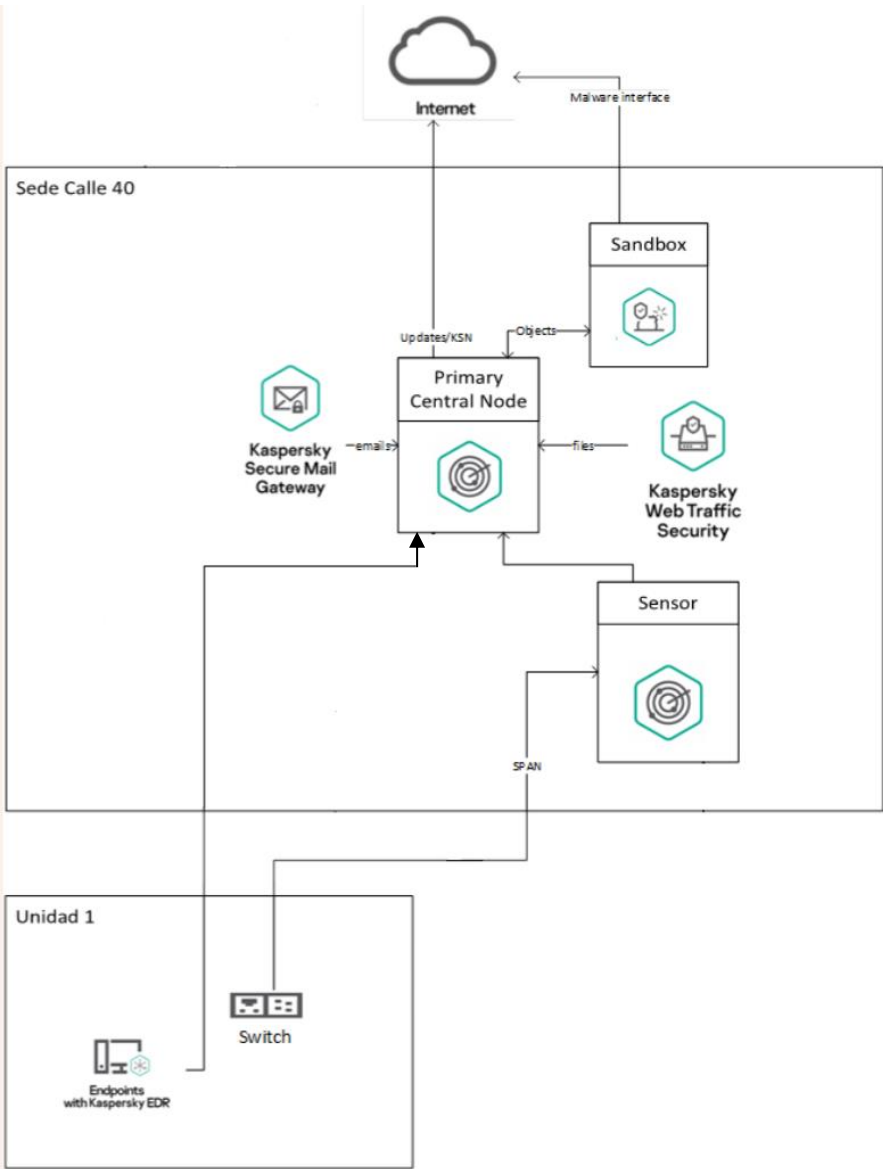


Diagrama de arquitectura actual



PUERTOS

- Los siguientes puertos deben estar abiertas:

Source	Destination	Port	Protocol
Primary Central Node	Internet	443	TCP
Primary Central Node	Internet	80	TCP
Primary Central Node	Internet	1443	TCP
Primary Central Node	Sandbox	443	TCP
Secondary Central Node	Internet	443	TCP
Secondary Central Node	Internet	80	TCP
Secondary Central Node	Internet	1443	TCP
Secondary Central Node	Sandbox	443	TCP
Sandboxes	Internet (malware NIC)	ANY	ANY
Sensor	Primary Central Node	9081	TCP
Sensor	Primary Central Node	53	UDP
Primary Central Node	Sensor	53	UDP
SMTP Server	Sensor	25	TCP
ICAP Server	Sensor	1344	TCP
Management Device	Sensor	22	TCP
Management Device	Central Nodes	22	TCP
Management Device	Central Nodes	8443	TCP
KWTS and KSMG	Primary Central Node	443	TCP
KES	Secondary Central Node	443	TCP
Management Device	Sandboxes	22	TCP
Management Device	Sandboxes	8443	TCP
KES	KSC	13000	TCP
KSC	KES	15000	UDP
KES	KSC	13111	TCP
KSC	Internet	80 y 443	TCP
KSC	KES	139 y 445	TCP
KSC	KES	137 y 138	UDP

KES = Kaspersky Endpoint Security

KSC = Kaspersky Security Center

KWTS = Kaspersky Web Traffic Security

KSMG = Kaspersky Secure Mail Gateway

3.2 Información de los servidores

Abajo la descripción y función de los servidores.

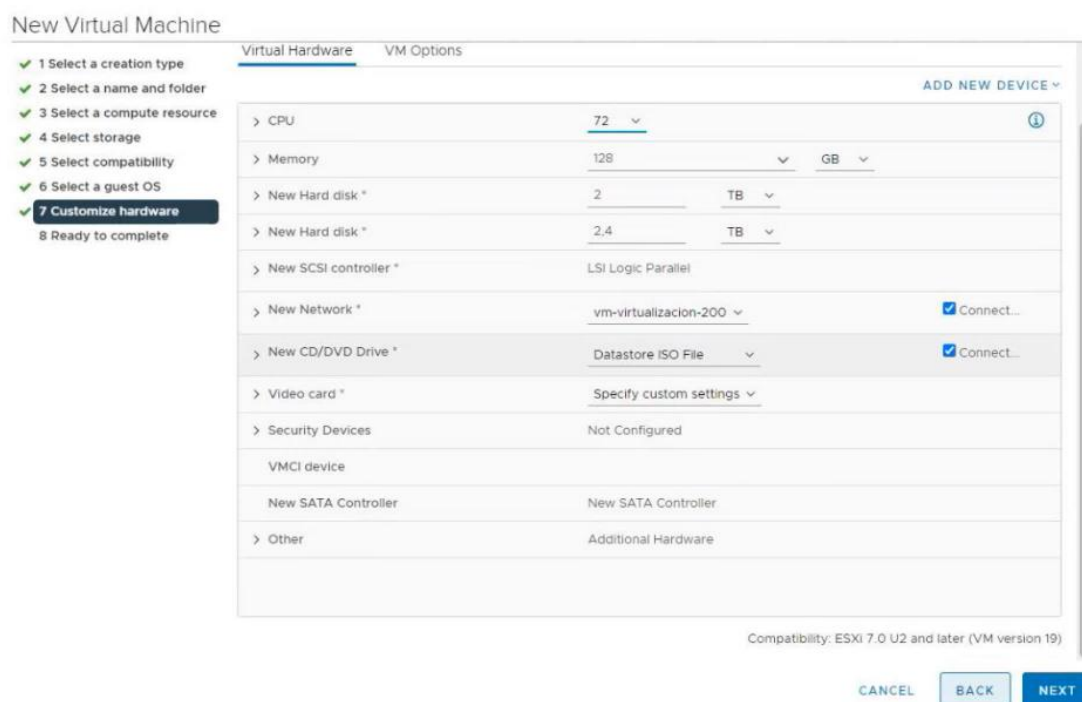
NOMBRE	FUNCIÓN	DESCRIPCIÓN	IP
<i>Kata-central-node-01</i>	Nodo Central	Orquestador principal de la solución KATA/KEDR que incluye la base de datos principal de telemetría TAA.	10.20.200.220
<i>Kata-sensor</i>	Sensor	Nodo encargado del análisis de tráfico de red, incluyendo análisis mediante KSN e IDS. Integraciones via SPAN, ICAP, POP3, SMTP.	10.20.200.222
<i>Kata-Sandbox</i>	Sandbox	Nodo encargado del análisis de artefactos enviados desde el Nodo Central para su análisis dinámico.	10.20.200.230

3.3 Implementación de Kaspersky Anti Targeted Attack Platform

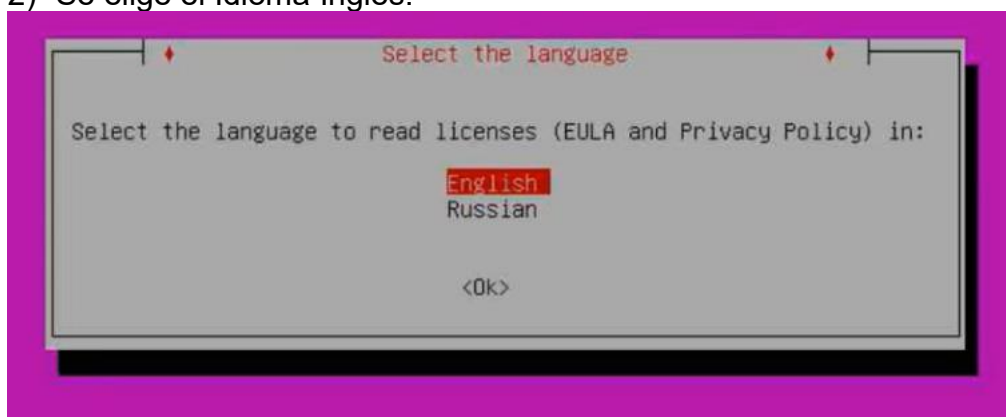
En esta sesión vamos a detallar el proceso de instalación de Kaspersky Anti Targeted Attack Platform.

Central Node

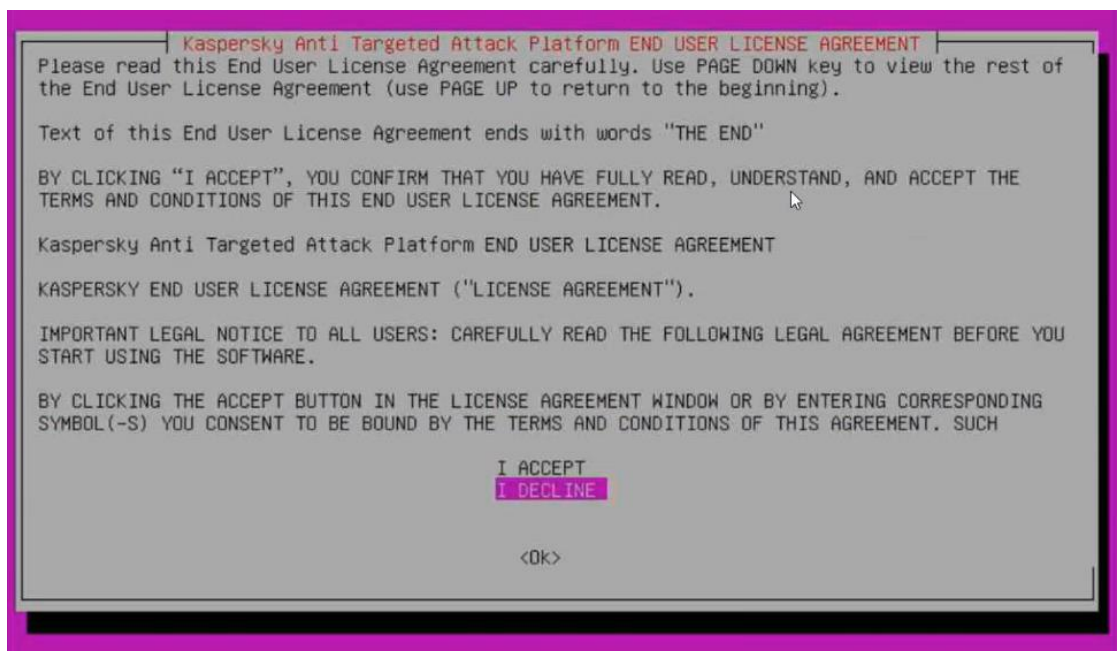
- 1) Validar la configuración de la máquina virtual antes del despliegue y montar la ISO para su instalación:



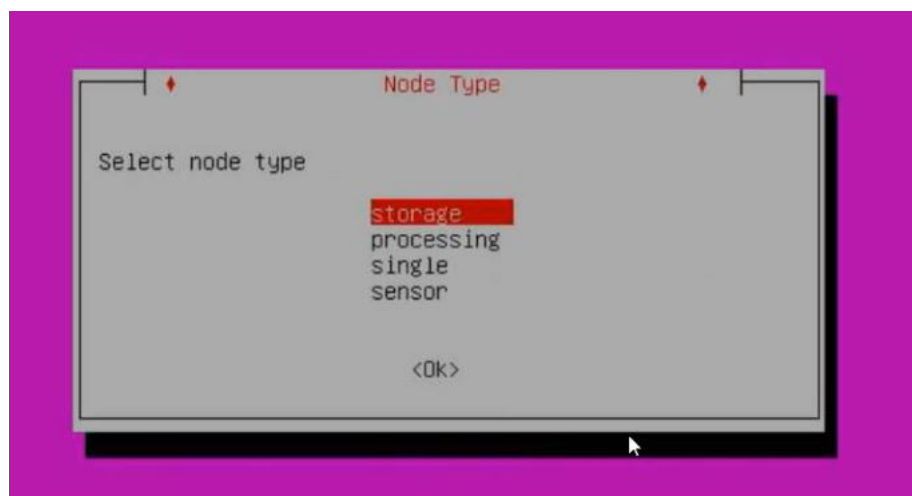
- 2) Se elige el Idioma Inglés:



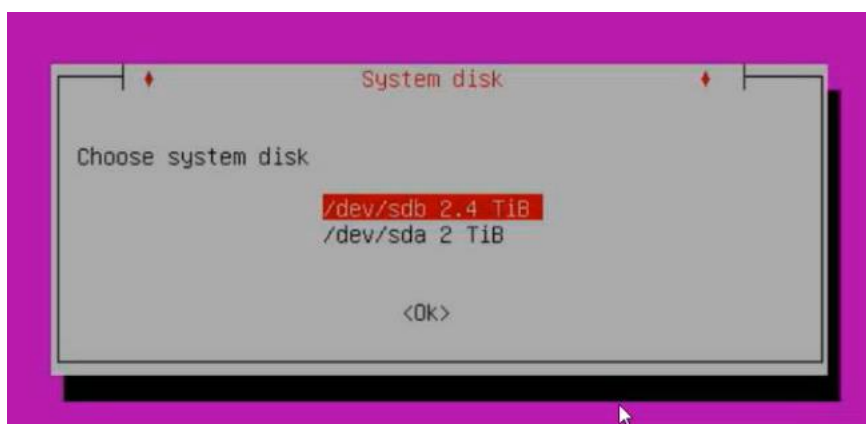
3) Se Acepta el License Agreement.



4) Se especifica el tipo de nodo a instalar, en este caso SINGLE (Central Node standalone):



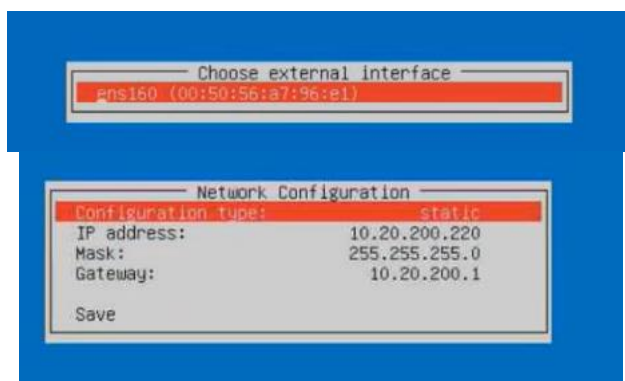
5) Se selecciona el disco de almacenamiento del sistema:



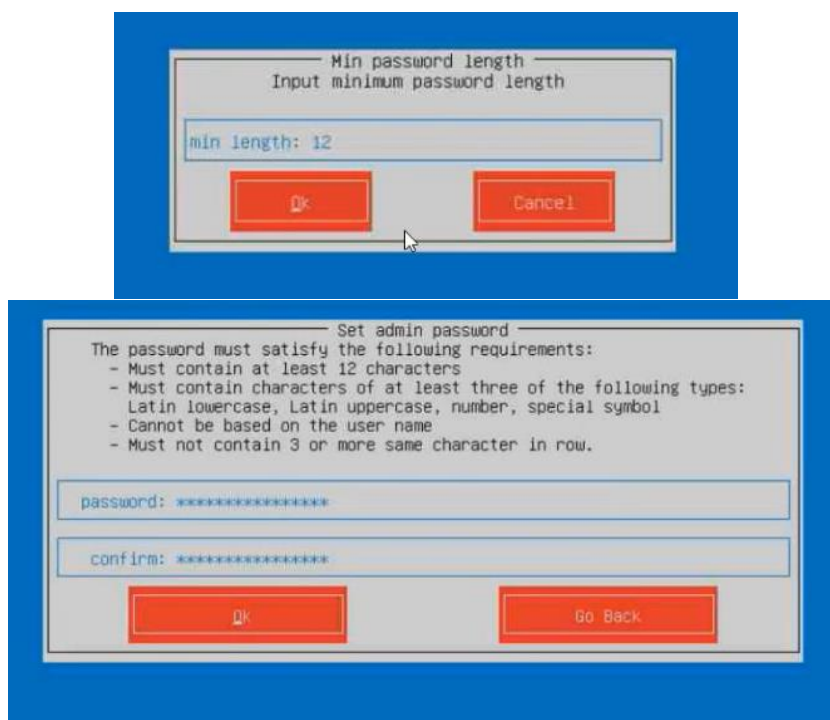
6) Se selecciona el disco separado para almacenar las TAA:



7) Se configura la interfaz de red:



8) Se configura la cuenta local "**admin**":



9) Se configuran los DNS del Central Node:


```
Configure at least one DNS server address
To set more addresses, separate them with 'enter'
To exit this configuration step, write an empty string and press 'enter'
10.20.110.3
10.20.110.5
-
```

10) Se configura el servidor de NTP:

```
Configure NTP server addresses.
Input one or more NTP server addresses, confirming each with an "Enter" key press.
To finish this configuration step, input an empty string.
10.20.110.3
-
```

11) Nos logueamos por única vez con la cuenta admin a la interfaz web de la consola de KATA administrada por el Central Node y realizamos la configuración final del nodo:

← → ↻ No es seguro <https://10.20.200.220:8443/katap/#/deployment>

**Kaspersky
Anti Targeted
Attack Platform**

⚙️ Server configuration



Server configuration

Specify values that Kaspersky Anti Targeted Attack Platform will use to determine the optimal server configuration. You will be able to change these values during operation. See [Calculations for the Central Node component](#) in Online Help.

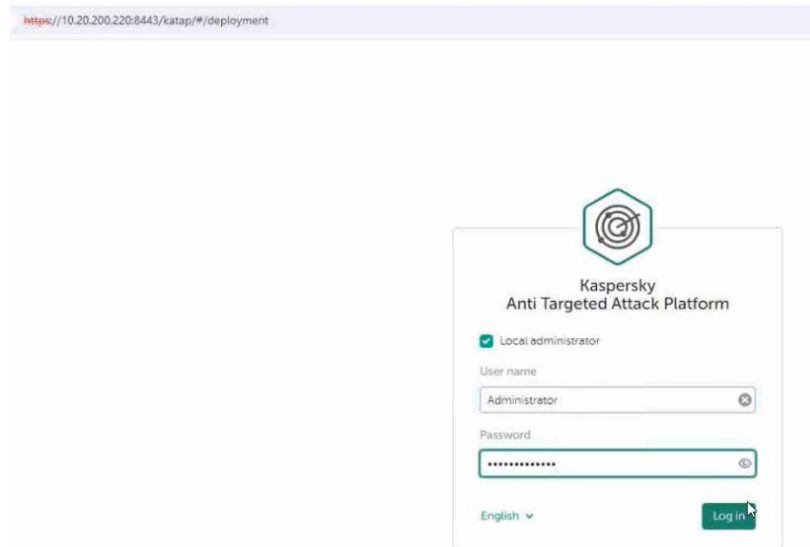
Number of Endpoint Agents*	<input type="text" value="1000"/>	<small>If you do not have a REDR license, enter 0</small>
Mail traffic, messages per second*	<input type="text" value="0"/>	<small>If you do not have a KATA license, enter 0</small>
SPAN traffic, Mbps*	<input type="text" value="7000"/>	<small>If you do not have a KATA license, enter 0</small>

Disk space

Specify the size of the events database and the Storage. Some disk space is already reserved for service information and the alerts database.

Events database, GB* 	<input type="text" value="1011"/>
Storage, GB* 	<input type="text" value="100"/>

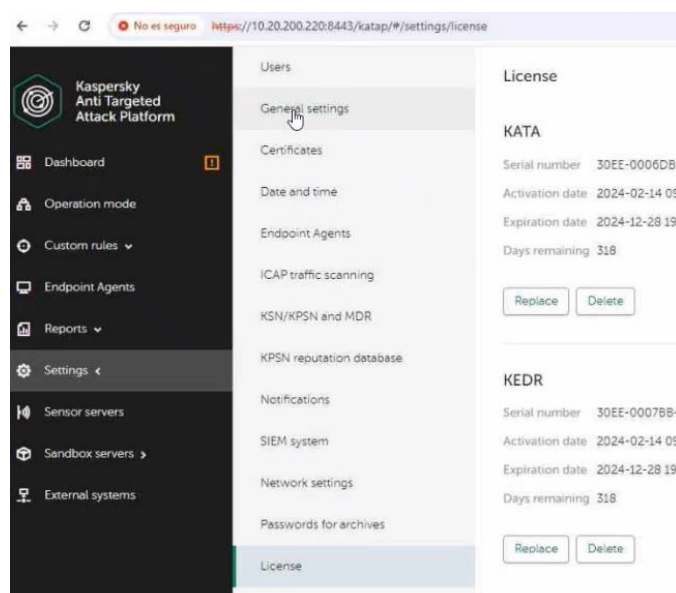
- 12) Finalmente, terminada la configuración se reinicia y podemos ingresar con la cuenta local **Administrator**, cuya password por defecto es **Administrator**.



- 13) Cambiamos la password por defecto de Administrator:



- 14) Se procede a adicionar las licencias de KATA y KEDR:



15) Habilitar el uso de KSN:

Participation in KSN/KPSN

The settings are applied to all the connected Central Nodes and Sensors.

Connection type: Not connected **KSN** KPSN

KSN Statement

KASPERSKY SECURITY NETWORK (KSN) STATEMENT

Kaspersky Security Network Statement (hereinafter "KSN Statement") relates to the computer program Kaspersky Anti Targeted Attack Platform 6.0 (hereinafter "Software").

KSN Statement along with the End User License Agreement for Software, in particular in the Section "Conditions regarding Data Processing" specifies the conditions, responsibilities and procedures relating to transmission and processing of the data, indicated in the KSN Statement. Carefully read the terms of the KSN Statement, as well as all documents referred to in the KSN Statement, before accepting it.

When the End User activates the using of the KSN, the End User is fully responsible for ensuring that the processing of personal data of Data Subjects is lawful, particularly, within the meaning of

☒ I agree to participate in KSN

☐ I do not agree to participate in KSN

Apply Cancel

KATA Sensor

1) Creación de la máquina virtual y validación de especificaciones para instalación del nodo con rol de sensor:

New Virtual Machine

✓ 1 Select a creation type
✓ 2 Select a name and folder
✓ 3 Select a compute resource
✓ 4 Select storage
✓ 5 Select compatibility
✓ 6 Select a guest OS
7 Customize hardware
8 Ready to complete

Customize hardware
Configure the virtual machine hardware

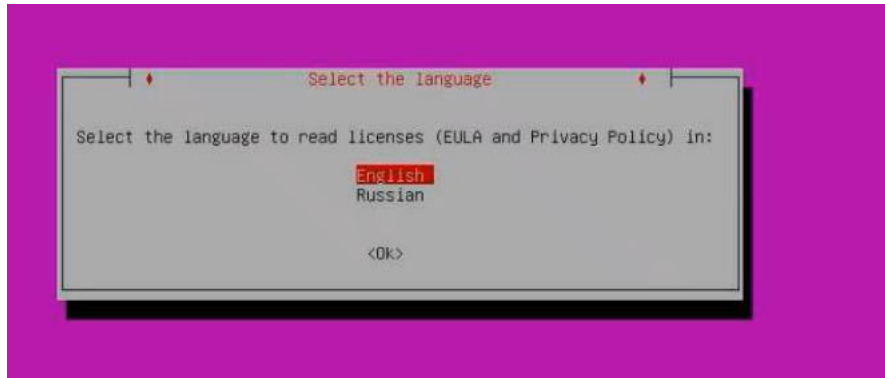
Virtual Hardware VM Options

ADD NEW DEVICE

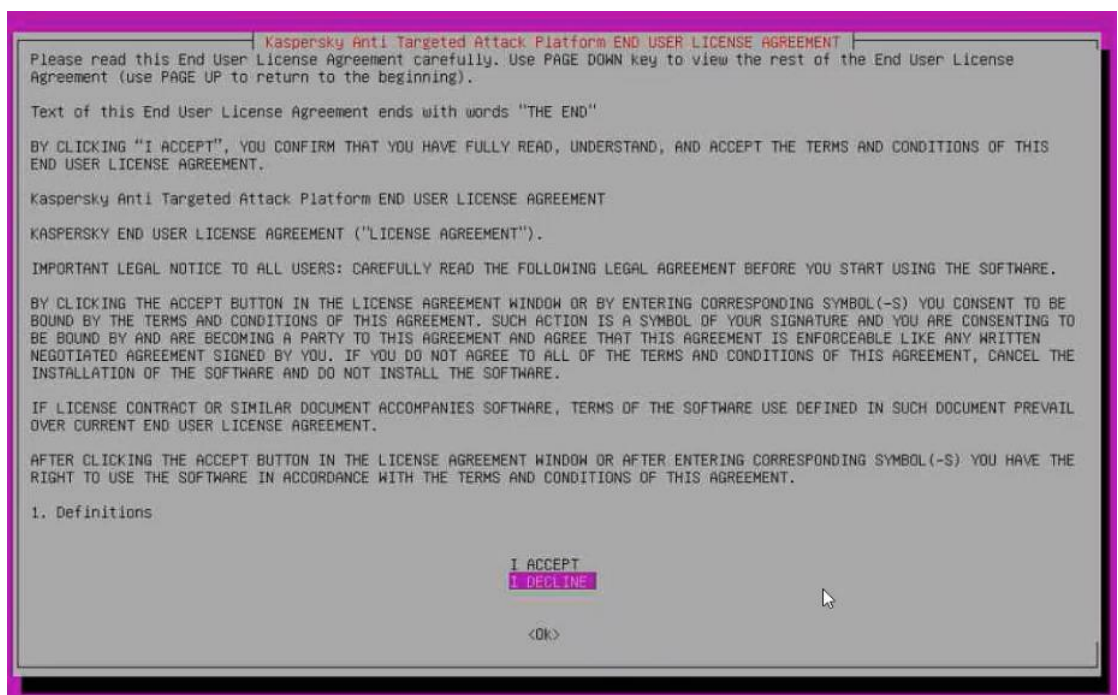
> CPU *	52	
> Memory *	128	GB
> New Hard disk *	500	GB
> New SCSI controller *	LSI Logic Parallel	
> New Network *	vm-virtualizacion-200	<input checked="" type="checkbox"/> Connect...
> New CD/DVD Drive *	Datastore ISO File	<input type="checkbox"/> Connect... (X)
> Video card *	Specify custom settings	
> Security Devices	Not Configured	
VMCI device		
New SATA Controller	New SATA Controller	
> Other	Additional Hardware	

CANCEL BACK NEXT

2) Elegimos idioma inglés:



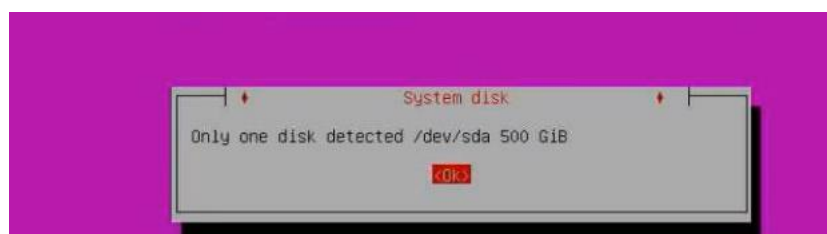
3) Aceptamos el License Agreement:



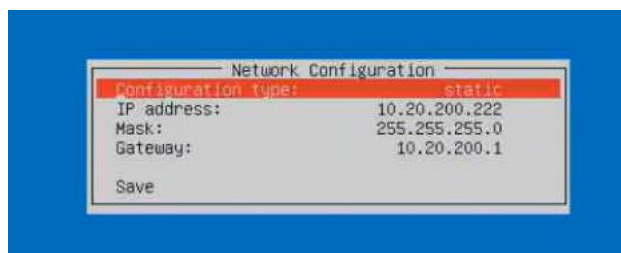
4) Elegimos el tipo de nodo a instalar, en este caso el Sensor:



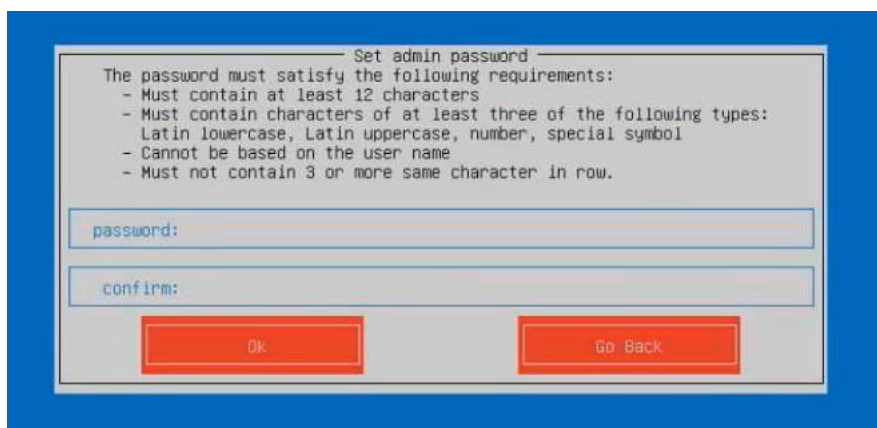
5) Elegimos el disco de instalación:



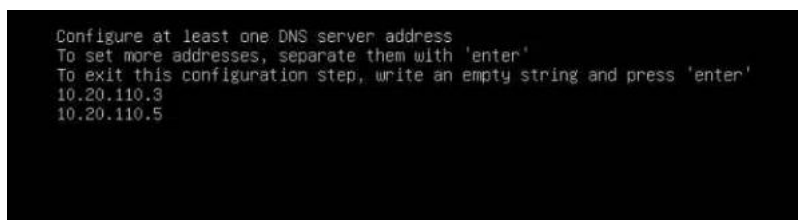
6) Configuramos la interfaz de red de administración:



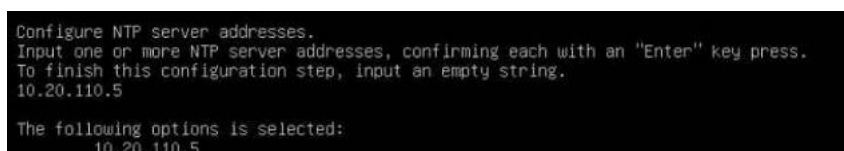
7) Se configura la contraseña para el usuario **admin**, que permitirá loguearse al nodo Sensor:



8) Se configuran los DNS:



9) Se configura el servidor NTP:



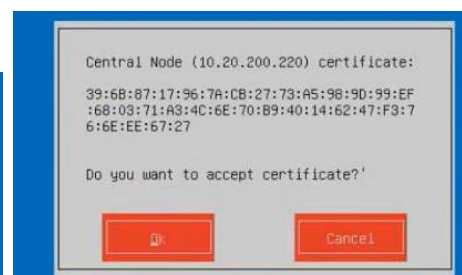
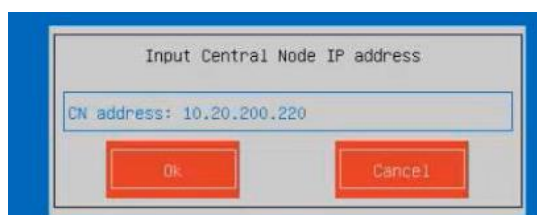
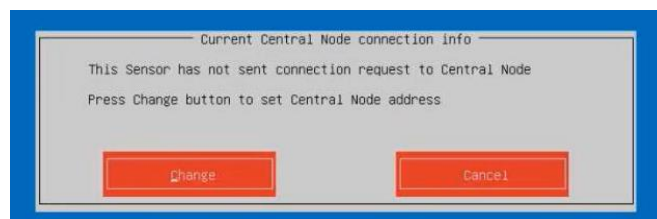
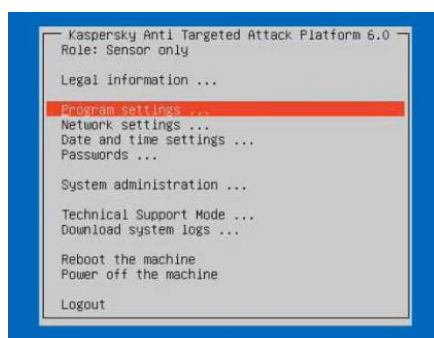
- 10) Una vez reiniciado el Sensor, ya podemos loguearnos en el servidor localmente:

```

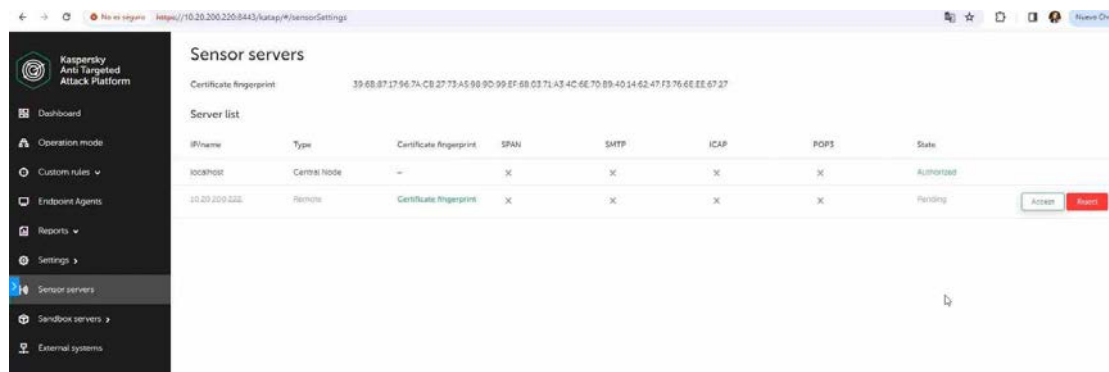
Ubuntu 22.04.2 LTS 1.srv.node1.node.dyn.katasensor tty1
1 login: admin
Password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-84-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage
  
```

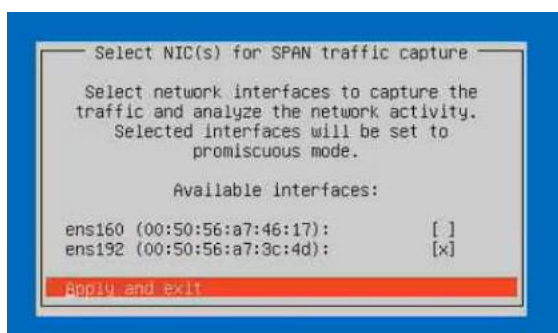
- 11) Aquí procedemos a integrar el Sensor con el Nodo Central o Central Node:



- 12) Del lado del Central Node aceptamos la solicitud y ya queda integrado con el Sensor:

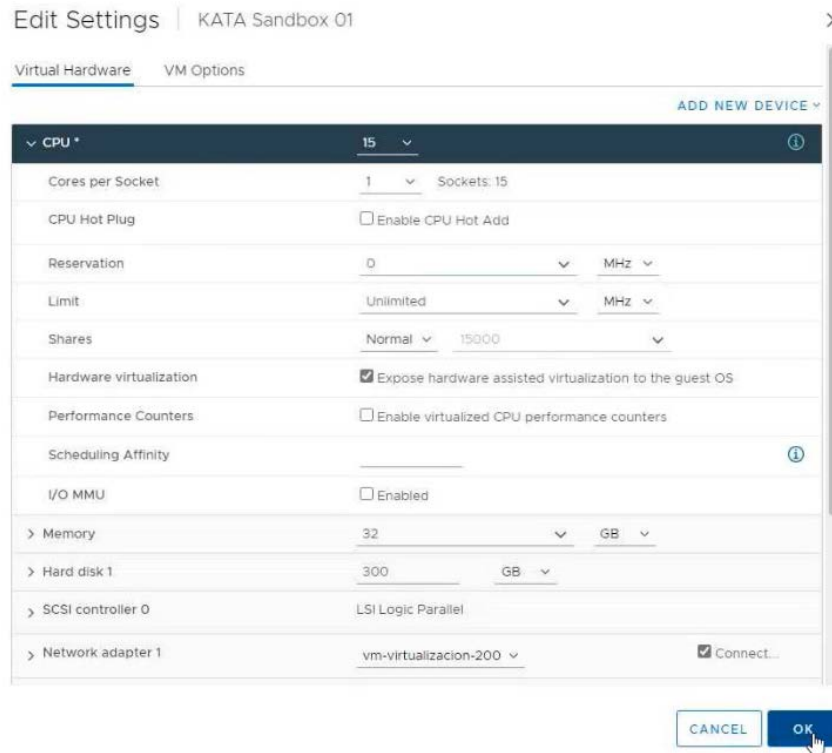


- 13) Finalmente, logueado en el nodo Sensor, dentro de Program Settings nos dirigimos a configurar la interfaz de recepción de tráfico vía SPAN:

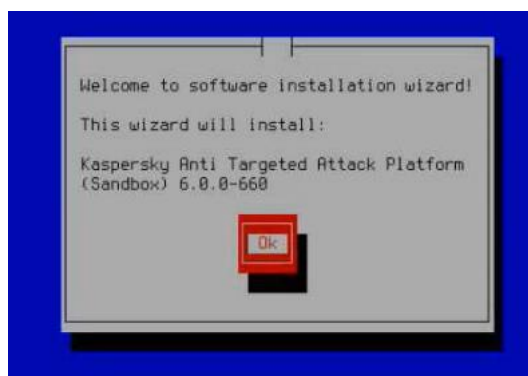


KATA Sandbox

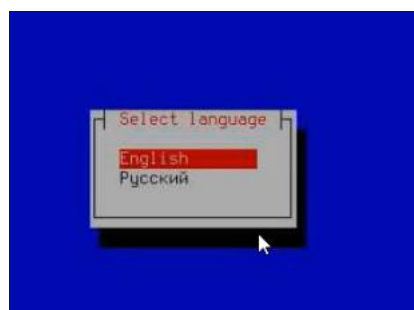
- 1) Se procede a crear la máquina virtual para desplegar el Sandbox mediante una ISO montada:



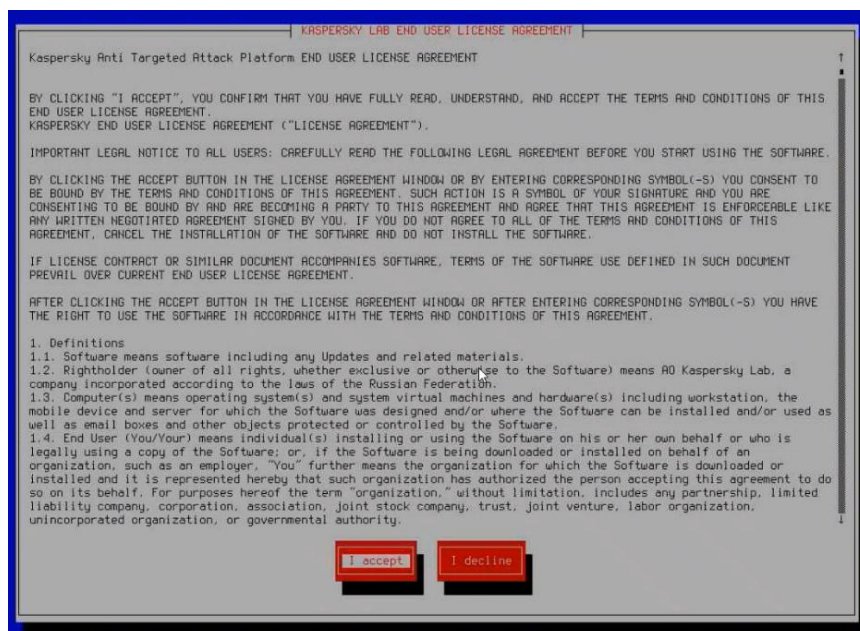
- 2) Iniciamos la instalación:



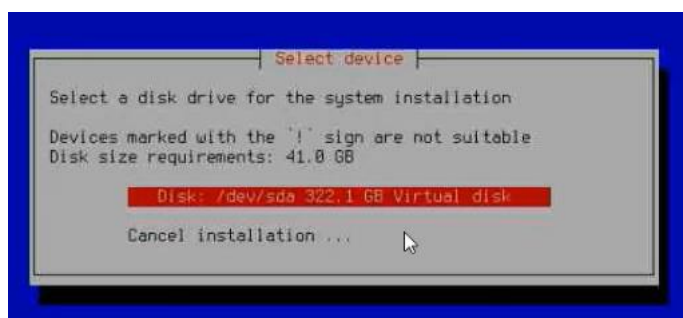
- 3) Escogemos el idioma inglés:



4) Aceptamos el License Agreement:



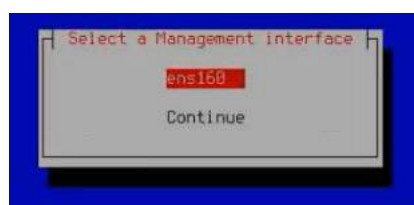
5) Seleccionamos el disco para su instalación:

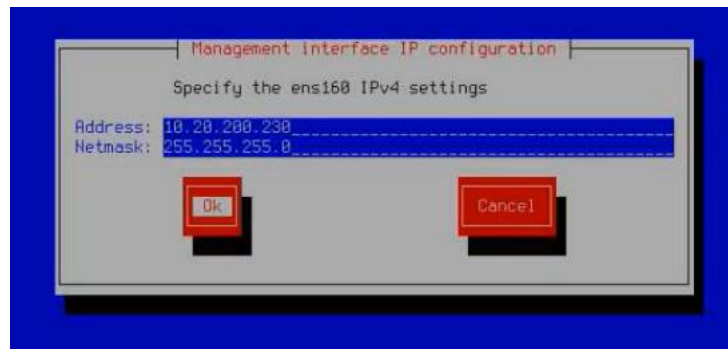


6) Configuramos un hostname para el Sandbox:

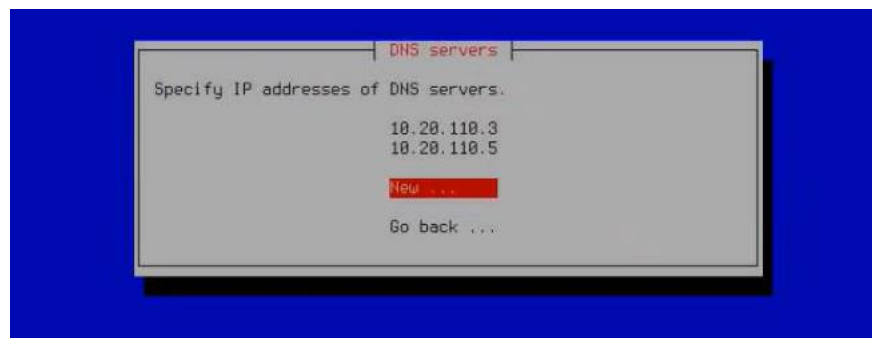


7) Configuramos la interfaz de red de administración:

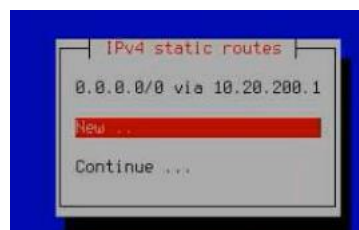




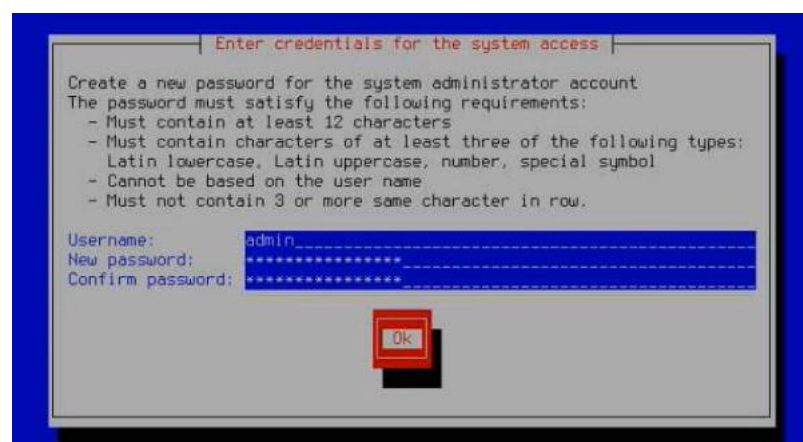
8) Configuramos los DNSs:



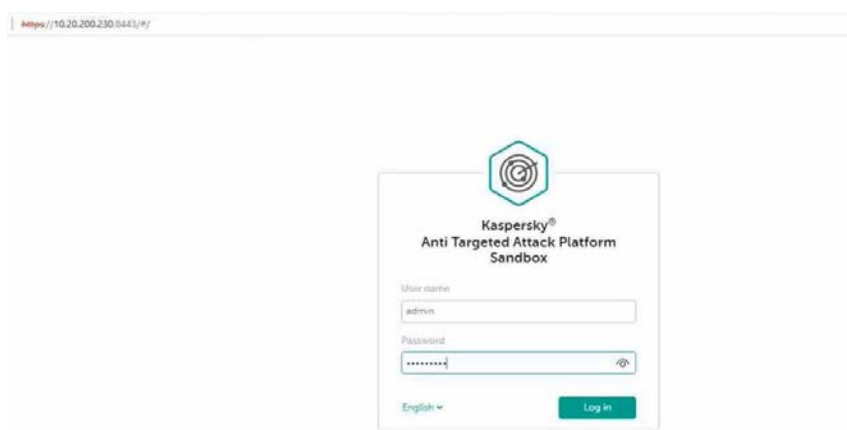
9) Configuramos el default route:



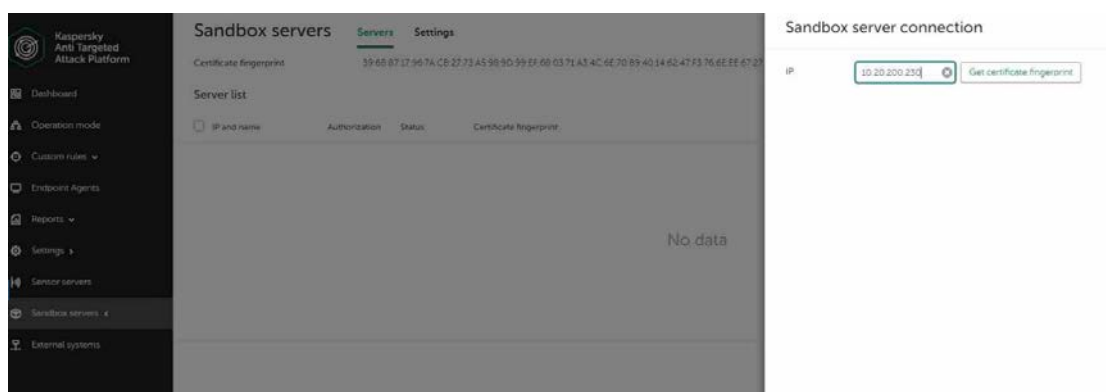
10) Configuramos la contraseña del usuario **admin**:



- 11) Una vez reiniciado el servidor de Sandbox, ya podemos loguearnos en su interfaz web:



- 12) Procedemos a configurar la integración con el Nodo Central de KATA, para esto, ingresamos primero a la consola web del nodo central y adicionamos la IP del recién creado Sandbox:



- 13) Acto seguido, desde la consola web del Sandbox, procedemos a aceptar la solicitud de integración completando el proceso:




14) Procedemos a configurar el servidor de NTP:

Date and time

Country

Time zone



Synchronization with NTP servers ☒ On

NTP servers

Date

15) Configuramos como fuente de las actualizaciones de base de datos al Nodo Central:

Database update

Last update

Update source

Central Node: 10.20.200.220

Proxy server ☐ Off

Address

Port

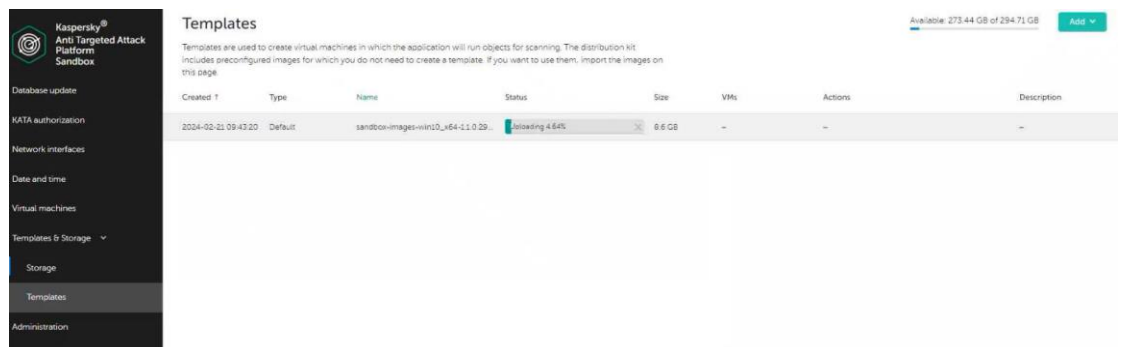
User name

Password

☐ Bypass proxy server for local addresses

✓ Saved successfully ✕

- 16) Se procede a cargar las imágenes ISO de las máquinas virtuales customizadas por Kaspersky dentro del Sandbox:



- 17) Por último, se debe configurar la interfaz de red de explotación en la sección de Network settings.

Integraciones finales

- 1) Procedemos a descargar el certificado del Nodo Central:



- 2) Luego, habilitamos el certificado cliente para doble validación y lo descargamos también:



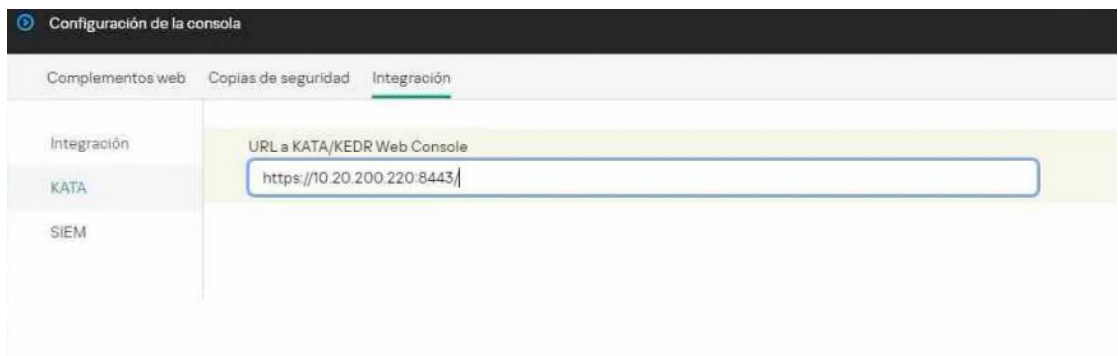
- 3) Importamos el certificado cliente y lo editamos mediante OPENSSL para poder adicionar una contraseña de encriptación:

```
admin@1.srv.node1.node.dyn.kata:~$ ls -lhrt
total 4.0K
-rw-rw-r-- 1 admin admin 2.7K Feb 21 15:11 KATA-cliente.pfx
admin@1.srv.node1.node.dyn.kata:~$ openssl pkcs12 -in KATA-cliente.pfx -out temp.pem -nodes
Enter Import Password:
admin@1.srv.node1.node.dyn.kata:~$ ls
KATA-cliente.pfx  temp.pem
admin@1.srv.node1.node.dyn.kata:~$ openssl pkcs12 -export -out KATA-cert-cliente.pfx -in temp.pem
Enter Export Password:
Verifying - Enter Export Password:
admin@1.srv.node1.node.dyn.kata:~$ ls -lhrt
total 12K
-rw-rw-r-- 1 admin admin 2.7K Feb 21 15:11 KATA-cliente.pfx
-rw-rw-r-- 1 admin admin 3.6K Feb 21 15:13 temp.pem
-rw-rw-r-- 1 admin admin 2.9K Feb 21 15:14 KATA-cert-cliente.pfx
admin@1.srv.node1.node.dyn.kata:~$
```

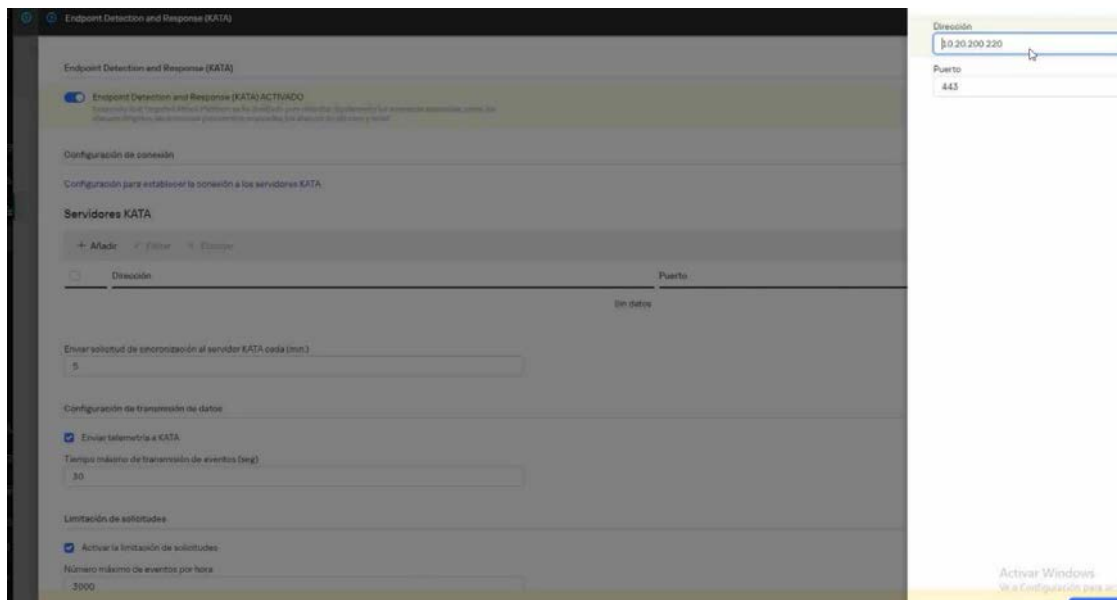
- 4) Volvemos a la consola web del Nodo Central y le reemplazamos el certificado cliente por el nuevo con contraseña:



- 5) A partir de aquí, empezamos a integrar con el Kaspersky Security Center (**KSC**) para habilitar el envío de telemetría desde los Endpoints usando el EDR como licenciamiento. Nos logueamos en el KSC y en Integración/KATA adicionamos la dirección del servicio web de KATA:



- 6) Luego nos dirigimos a la/las directivas de Kaspersky Endpoint Security dentro de la consola de KSC para poder configurar el servicio de EDR:

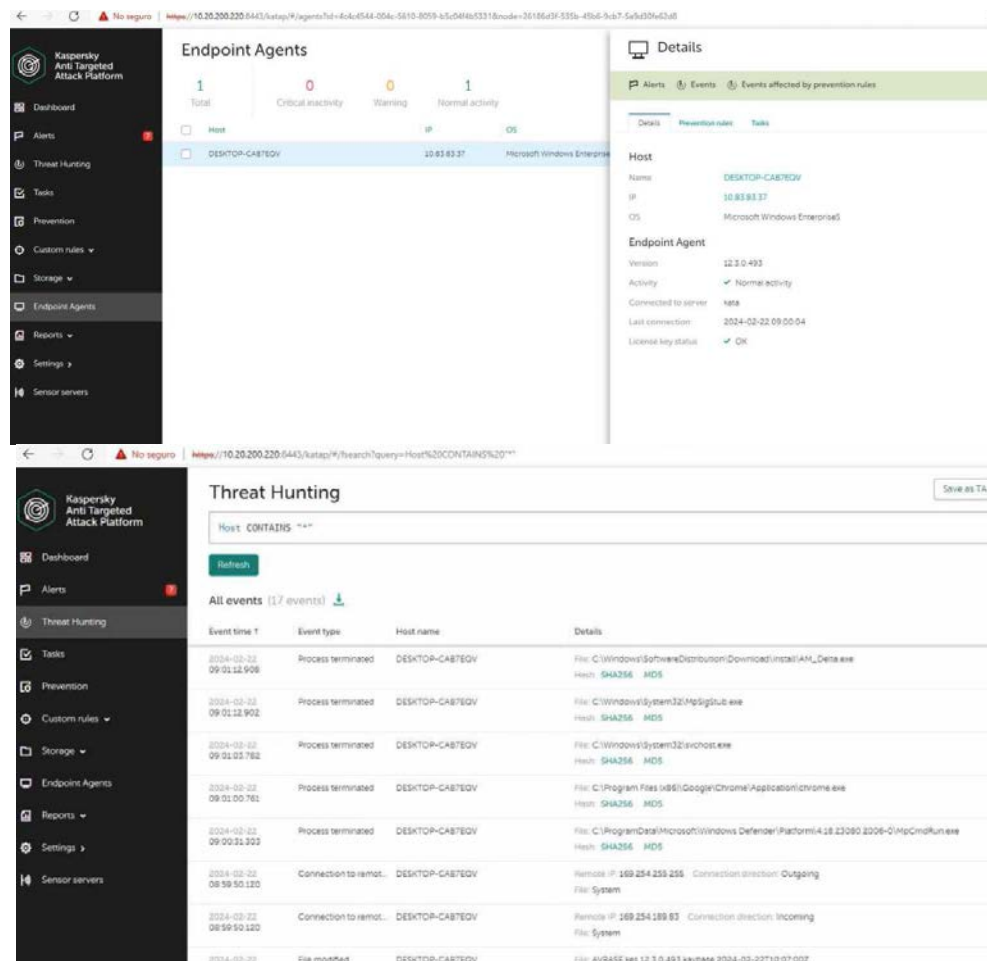


- 7) En la sección de Configuración para establecer la conexión a los servidores de KATA, vamos a colocar los certificados TLS del Nodo Central y el cliente que editamos:

- 8) Se procede a adicionar la licencia de KEDR dentro del repositorio del KSC:

- 9) Se genera la tarea de “Cambiar componentes de la aplicación” para habilitar el componente de KATA KEDR en las máquinas provistas por el cliente:

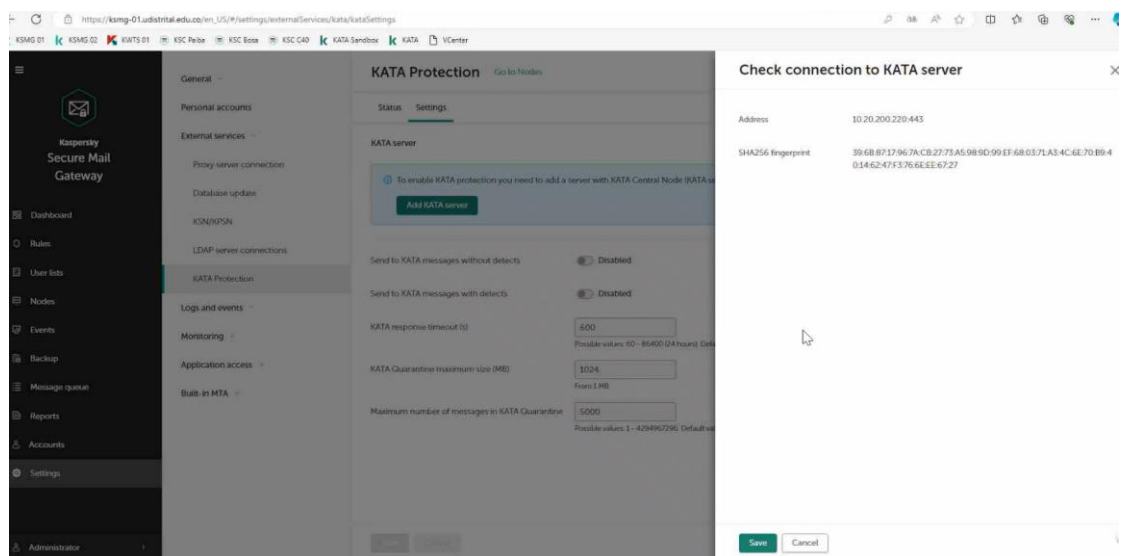
10) Se valida la conexión exitosa de un equipo de prueba:



The top screenshot shows the 'Endpoint Agents' section of the KATAP interface. It displays a list of agents with columns for Host, IP, and OS. A detailed view of an agent named 'DESKTOP-CAB7EDV' is shown on the right, including its IP (10.83.83.37), OS (Microsoft Windows Enterprise), version (12.3.0.493), activity (Normal activity), and connection status (Connected to server: OK).

The bottom screenshot shows the 'Threat Hunting' section. It displays a list of events with columns for Event time, Event type, Host name, and Details. The events listed include process terminations and connections to remote hosts.

11) Luego procedemos a integrar el Nodo Central con la aplicación KSMG, ingresando primero en la consola web del KSMG y luego aceptando la solicitud en la consola del Nodo Central (en External Systems):

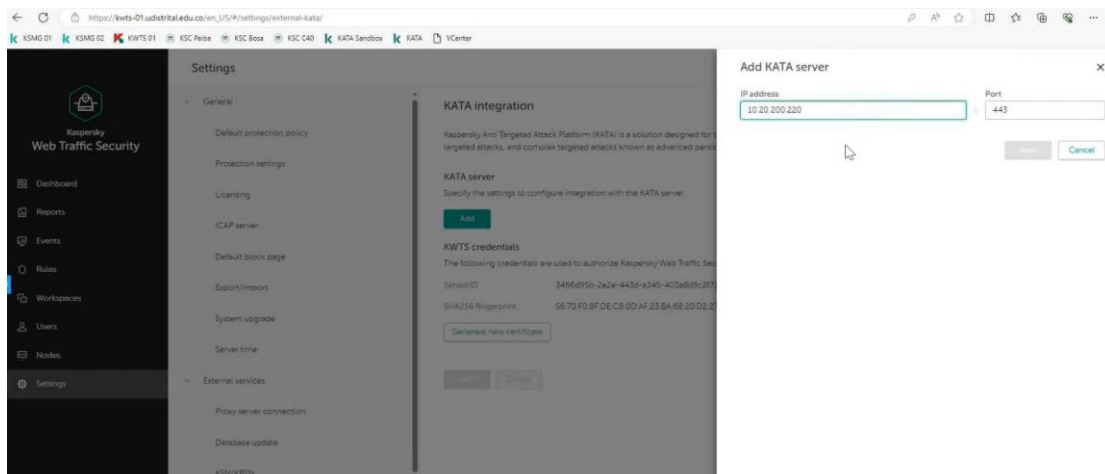


The top screenshot shows the KSMG interface. The 'KATA Protection' section is active, displaying settings for KATA server, including 'Send to KATA messages without detects' (Disabled), 'Send to KATA messages with detects' (Disabled), 'KATA response timeout (s)' (600), 'KATA quarantine maximum size (MB)' (1024), and 'Maximum number of messages in KATA Quarantine' (5000).

The bottom screenshot shows the 'Check connection to KATA server' dialog box. It displays the address (10.20.200.220:443) and the SHA256 fingerprint (39:6B:87:17:96:7A:CB:27:75:A5:98:9D:99:EF:68:03:71:A3:4C:6E:70:B9:4:0:14:62:47:F3:76:6E:EE:67:27).



12) Finalmente hacemos la integración con el producto KWTS, ingresando en primer lugar a la consola WEB de dicho producto y finalmente aceptando la solicitud dentro de la consola del Nodo Central (en External Systems):



4. Conclusión

No hubo grandes inconvenientes que pudieran detener el proceso de instalación y las posteriores integraciones. La solución se pudo implementar en su mayoría, faltando el despliegue de KEDR en todos los endpoints esperados. Parte de esto se debió a inconvenientes en la implementación de los otros dos productos que se desplegaron en conjunto sobre las mismas fechas **KWTS** y **KSMG**.

kaspersky

www.kaspersky.com/
www.securelist.com

© 2024 AO Kaspersky Lab.

All rights reserved. Registered trademarks and service marks are the property of their respective owner

The Kaspersky logo, consisting of the word "kaspersky" in a lowercase, bold, sans-serif font. The background of the entire page is a teal-to-green gradient with a large white abstract shape in the center.

INSTALACIÓN DE KASPERSKY SECURE MAIL GATEWAY

Índice

- 1. OBJETIVOS 3
- 2. PRODUCTOS 3
- 3. ESTRUCTURA 4
 - 3.1 Diagrama de tráfico 4
 - 3.2 Informaciones de los servidores 5
 - 3.3 Implementación de Kaspersky Secure Mail Gateway..... 6
- 4. CONCLUSIÓN..... 15

1. Objetivos

Documentar todas las configuraciones realizadas durante la fase de implementación del productor Kaspersky Secure Mail Gateway.

2. Productos

Kaspersky Secure Mail Gateway (KSMG): Kaspersky Secure Mail Gateway es un sistema de correo electrónico completamente integrado y también una solución de seguridad de correo, todo en un solo dispositivo virtual listo para usarse. Brinda una protección de correos electrónicos de última generación para todo tipo de amenazas conocidas y desconocidas, incluidos spam, phishing, correo electrónico empresarial comprometido (BEC) y todas las formas de adjuntos maliciosos.

3. Estructura

3.1

Diagrama tráfico entrante

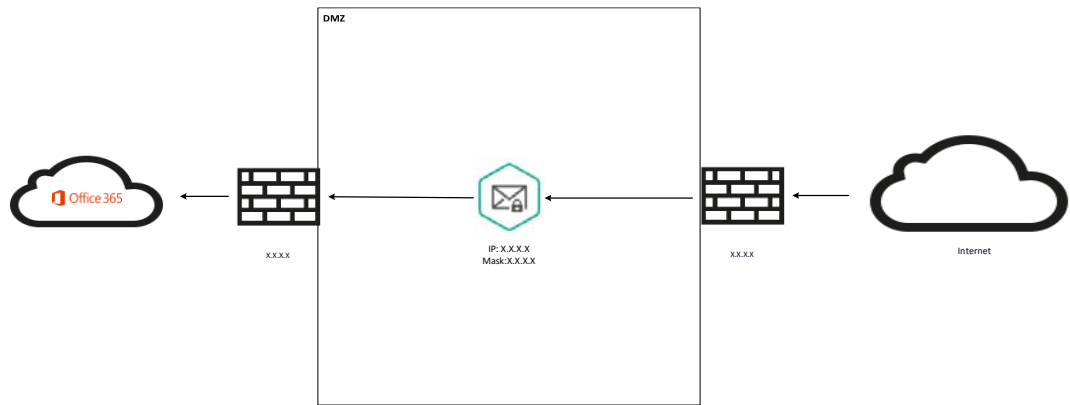
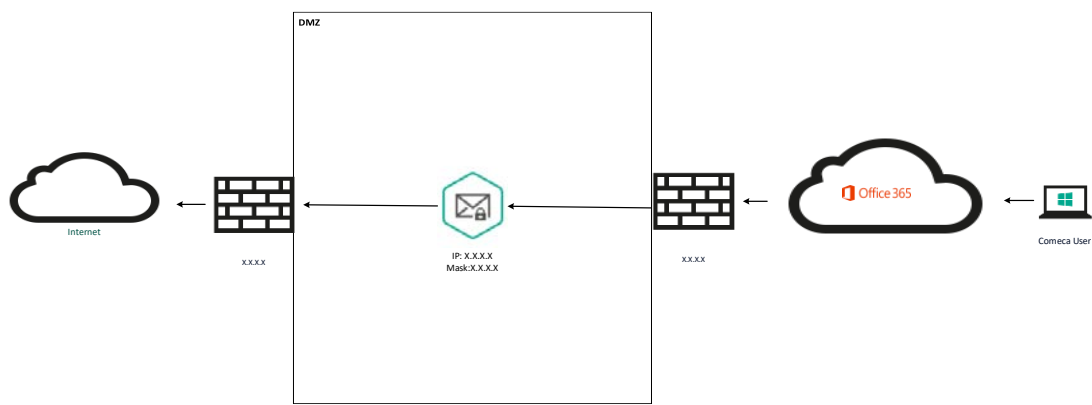


Diagrama tráfico saliente



3.2 Información de los servidores

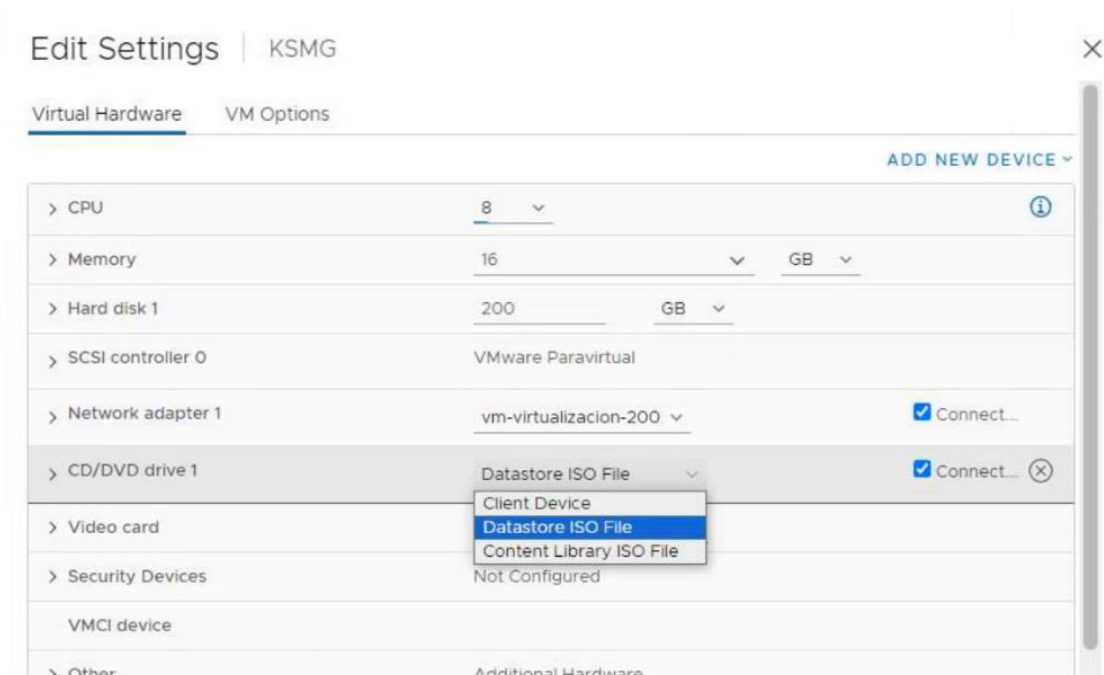
Abajo la descripción y función de los servidores.

NOMBRE	FUNCIÓN	DESCRIPCIÓN	IP
KSMG-01	Servidor de KSMG (Entrante)	Servidor de Kaspersky Secure Mail Gateway para correos entrantes.	10.20.200.225
KSMG-02	Servidor de KSMG (Saliente)	Servidor de Kaspersky Secure Mail Gateway para correos salientes.	10.20.200.226

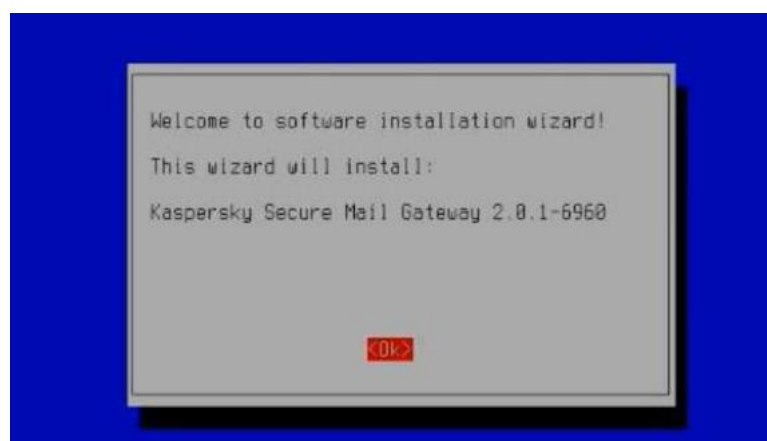
3.3 Implementación de Kaspersky Secure Mail Gateway

En esta sesión vamos a detallar el proceso de instalación de Kaspersky Secure Mail Gateway.

- 1) Validar la configuración de la máquina virtual antes del despliegue y montar la ISO para su instalación:



- 2) Se inicializa la instalación:

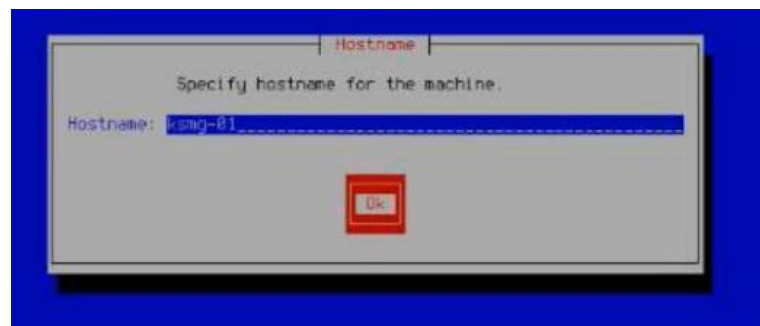


- 3) Se elige el Idioma Español y se Aceptan las bases y condiciones del producto.

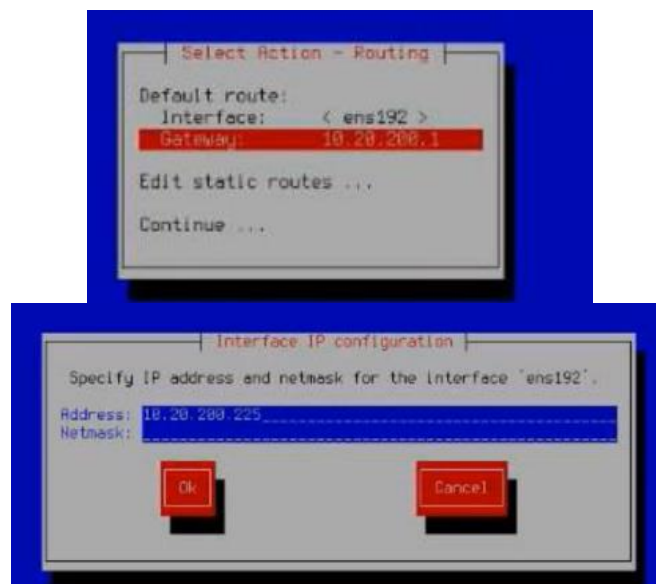
4) Se selecciona el disco de almacenamiento:



5) Se especifica el hostname:



6) Se configura la interfaz de red:



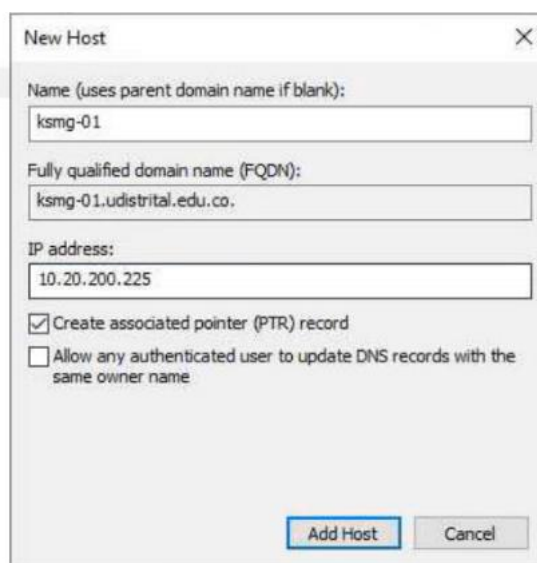
7) Se configura la cuenta de “**Administrator**”:



8) El servidor finaliza la instalación, reinicia el sistema operativo y procede a generar un fingerprint de conexión:




9) Generamos el registro DNS:



10) Se procede al login dentro de la interfaz web por primera vez:


https://10.20.200.225/en_US/



Kaspersky
Secure Mail Gateway

User name


Password

 Please do not use domain credentials for log in

11) Se procede a adicionar la licencia:

Licensing [Go to Nodes](#)

License key status Settings



Active license key

License type
Commercial

Serial number
BE2B772D-F02C-47C1-B25B-B91

Nodes

IP address:port	License key status
10.20.200.225.9045	The license is valid

12) Se configura el tiempo/ servidor NTP:

Date and time

Time zone

Country

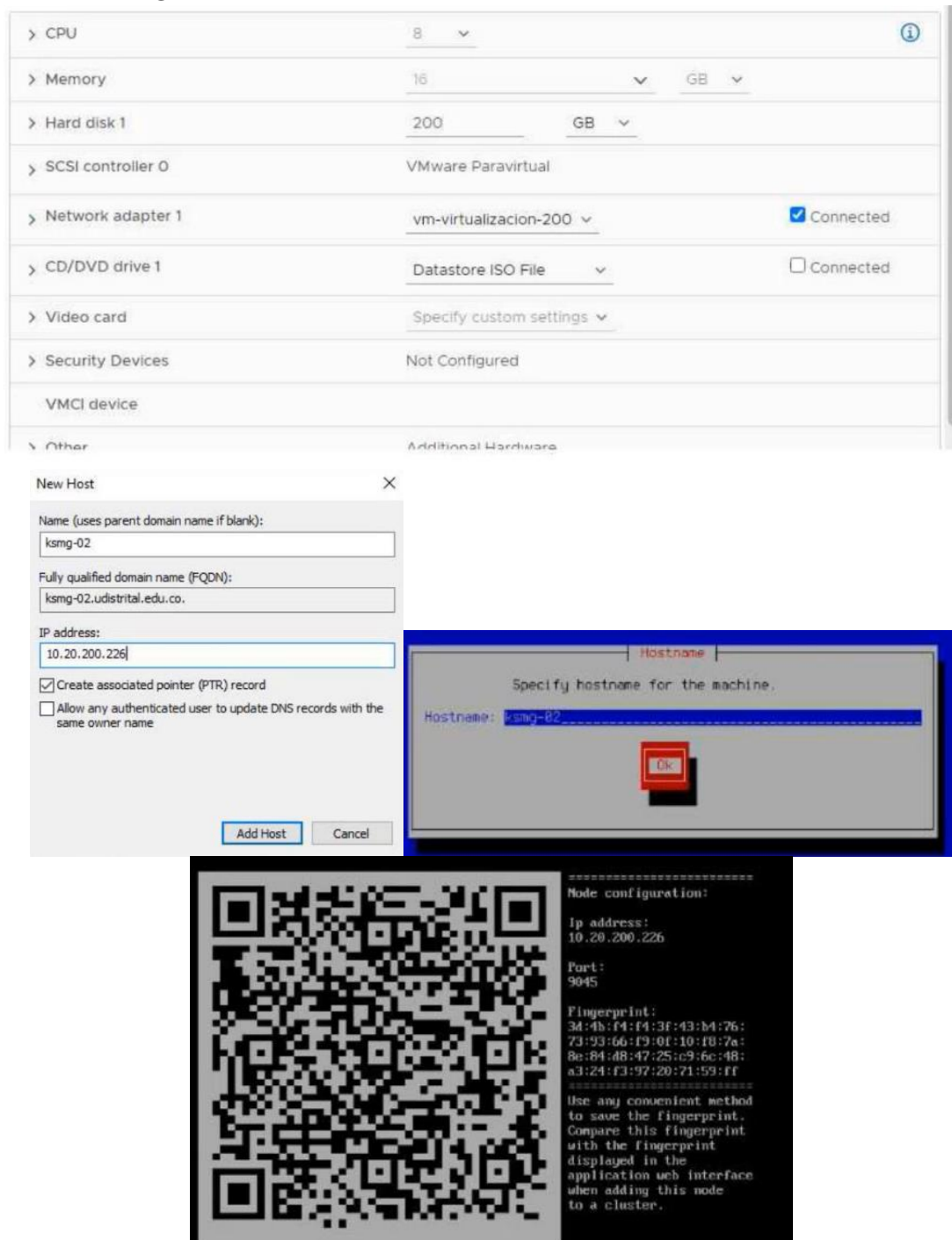
Time zone

Time synchronization

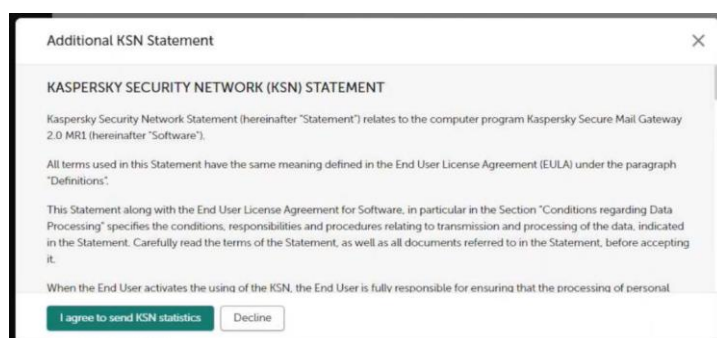
Synchronize with NTP server ☒ Enabled

NTP servers

13) Se repite el mismo proceso de los pasos 1 al 12 para el Nodo 2 de KSMG:



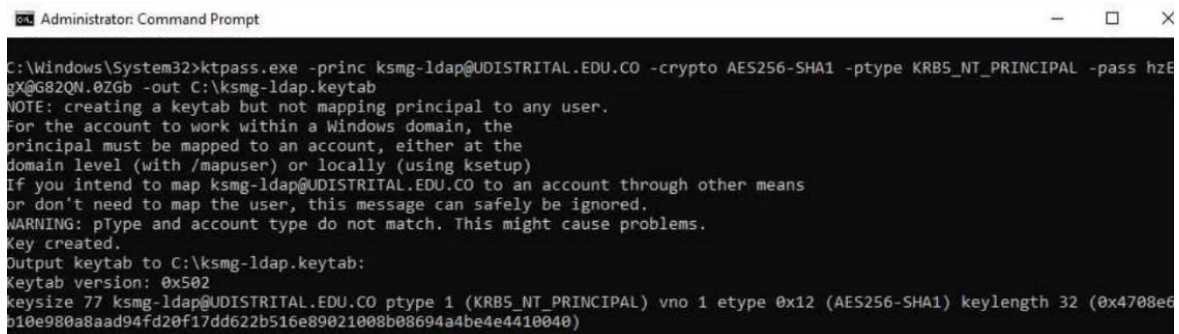
14) Habilitar el uso de KSN:



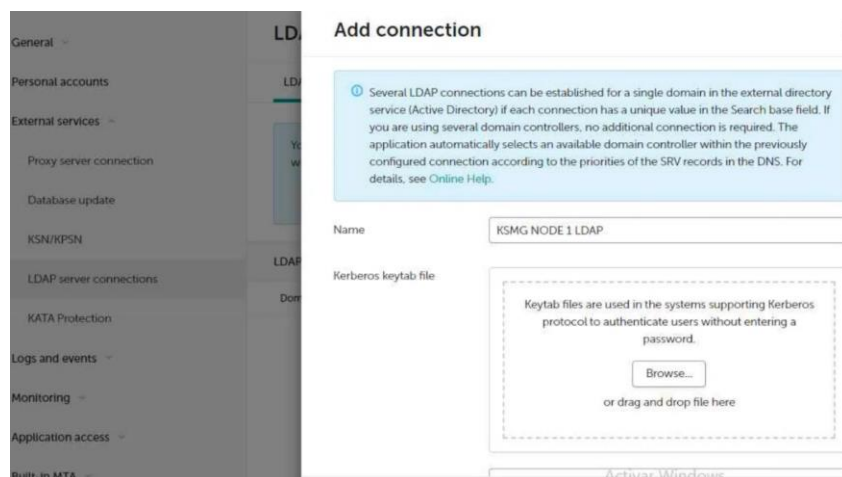
- 15) Generamos el usuario de Active Directory para integración mediante LDAP. Para esto se requiere generación de archivo KEYTAB mediante línea de comando:



- 16) Creación de Keytab:



- 17) Adicionar conexión para integración con LDAP, incluyendo el nuevo KEYTAB:



Entries in Kerberos keytab file

ksmg-ldap@UDISTRITALEDU.CO

Search base (Base DN)

dc=udistrital, dc=edu, dc=cd

LDAP users and groups

Attributes containing email addresses

proxyAddresses attribute

LDAP contact details

☐ Disabled

Attributes containing email addresses

mail and proxyAddresses attributes

18) Se confirma la correcta integración y sincronización con LDAP:

10.20.200.225:9045

Settings

Applied

Success 29/01/2024 15:35:44

Database information

Database update

Success 29/01/2024 15:32:50

Anti-Virus

Databases are up to date

Anti-Phishing

Databases are up to date

Anti-Spam

Databases are up to date

External services

KSN/KPSN status

No errors

LDAP status

KSMG NODE 1 LDAP:

Connection

29/01/2024 15:35:01

Data for rules match

29/01/2024 15:35:01

User accounts autofill

29/01/2024 15:35:01

19) Adicionamos un dominio con el cual el KSMG podrá trabajar, así como el servidor de correo con quien interactuará:

The screenshot shows the 'Domains' management interface on the left and the 'Edit domain' configuration panel on the right.

Domains Table:

Record	Domain type	Local domain	Protocol
udidrital.edu.co	Domain	<input checked="" type="checkbox"/> Enabled	SMTP

Edit domain configuration (udidrital.edu.co):

- General tab:**
 - Record type: Domain
 - Local domain: ☒ Yes
 - Email routing: ☒ Enabled
 - Protocol: SMTP
 - Host: smtp.office365.com
 - Port: 25
 - MX DNS Lookup: ☒ Enabled
 - TLS Encryption mode for outgoing mail: ☒ Use Attempt TLS Encryption
- DKIM records tab:** (Empty)

20) Se configura la información de conexión básica del servidor de KSMG dentro del propio dominio de la infraestructura donde opera:

Basic MTA Settings

The 'Basic MTA Settings' page contains the following configuration fields:

- Domain name:** udidrital.edu.co
- Hostname:**
 - ☐ Use FQDN of cluster nodes
 - ☒ Use specified hostname
 - ksmg-01.udidrital.edu.co
- Message size limit (bytes):** 20971520
- Trusted networks:**
 - 10.0.0.0/8 × 52.96.185.210 × 52.96.97.178 × 13.107.6.152/31 × 13.107.18.10/31 × 13.107.128.0/22 × 23.103.160.0/20 × 40.96.0.0/13 × 40.104.0.0/15 × 52.96.0.0/14 × 131.253.33.215/32 × 132.245.0.0/16 × 150.171.32.0/22 × 204.79.197.215/32 × 40.92.0.0/15 × 40.107.0.0/16 × 52.100.0.0/14 × 104.47.0.0/17 × 52.101.10.5 × 200.69.103.0/24 ×
- Email destination address:**
 - ☐ Send directly
 - ☒ Send through an edge gateway
 - : 25
 - ☐ Use MX lookup

- 21) Posterior a este punto, el cliente procede a realizar la integración mediante conector con Office365.

4. Conclusión

Durante el proceso final de integración con el servicio de Office 365 se presentaron problemas para la recepción de correos, posterior habilitación de los conectores, por lo que luego de varios intentos se decidió abrir el incidente con el Soporte MSA, número de incidente: INC000016236474 el cuál fue oficialmente cerrado el día 12/04/2024.

kaspersky

www.kaspersky.com/
www.securelist.com

© 2024 AO Kaspersky Lab.
All rights reserved. Registered trademarks and service marks are the property of their respective owner

kaspersky

INSTALACIÓN DE KASPERSKY WEB TRAFFIC SECURITY

Índice

- 1. OBJETIVOS 3
- 2. PRODUCTOS 3
- 3. ESTRUCTURA 4
 - 3.1 Diagrama de tráfico 4
 - 3.2 Informaciones de los servidores 5
 - 3.3 Implementación de Kaspersky Web Traffic Security 6
- 4. CONCLUSIÓN..... 14

1. Objetivos

Documentar todas las configuraciones realizadas durante la fase de implementación del productor Kaspersky Web Traffic Security.

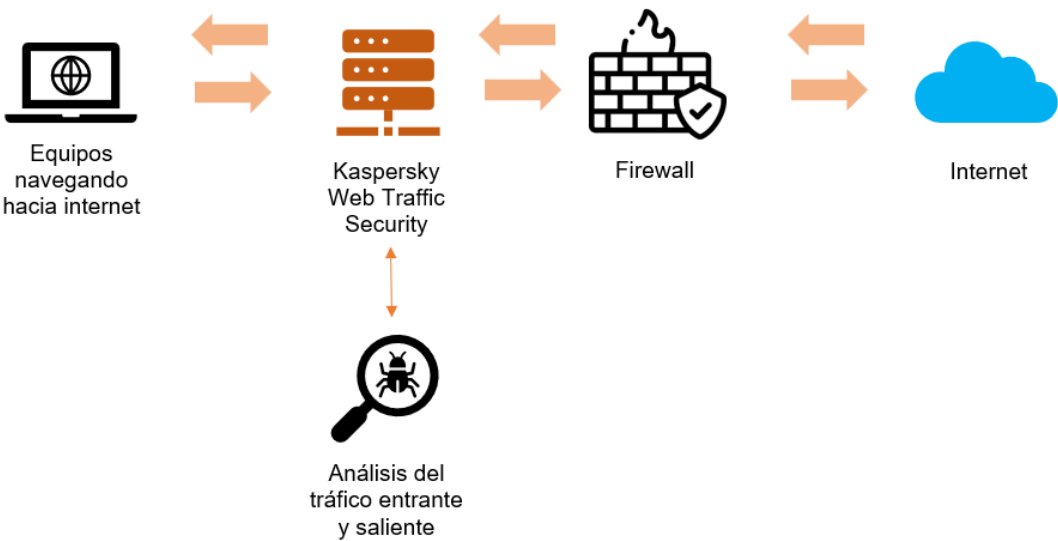
2. Productos

Kaspersky Web Traffic Security: (en adelante también referido como "la aplicación" o "KWTS") es una solución diseñada para proteger el tráfico HTTP, HTTPS y FTP que pasa a través de un servidor proxy.

La aplicación protege a los usuarios de una red corporativa al acceder a recursos web. Por ejemplo, elimina malware y otras amenazas del flujo de datos que entra a la red corporativa a través de los protocolos HTTP(S) y FTP, bloquea sitios web infectados y de phishing, y controla el acceso a recursos web basado en categorías de recursos web y tipos de contenido.

3. Estructura

3.1 Diagrama de tráfico



3.2 Información de los servidores

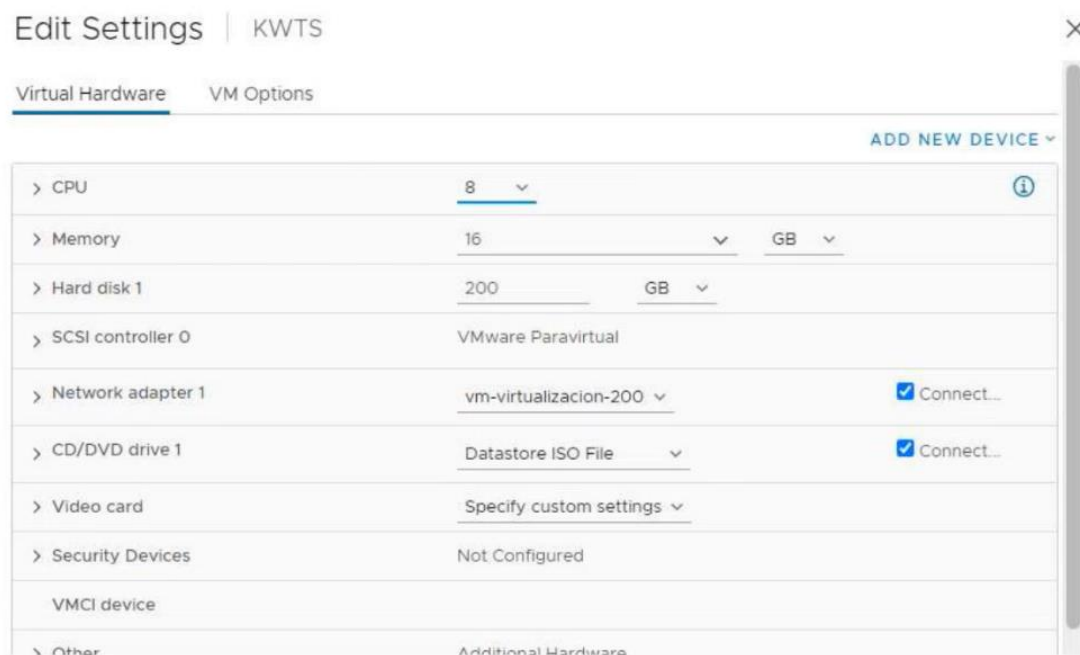
Abajo la descripción y función de los servidores.

NOMBRE	FUNCIÓN	DESCRIPCIÓN	IP
KWTS-01	Servidor de KWTS	Servidor de Kaspersky Web Traffic Security par análisis y detección de amenazas en tráfico HTTP, HTTPS y FTP	10.20.200.228

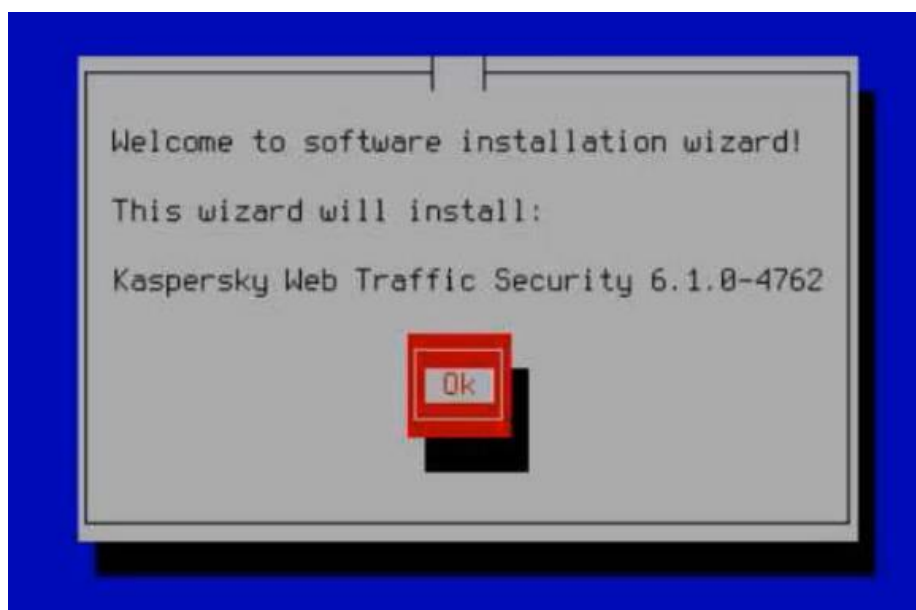
3.3 Implementación de Kaspersky Web Traffic Security

En esta sesión vamos a detallar el proceso de instalación de Kaspersky Web Traffic Security.

- 1) Validar la configuración de la máquina virtual antes del despliegue y montar la ISO para su instalación:



- 2) Se inicializa la instalación:



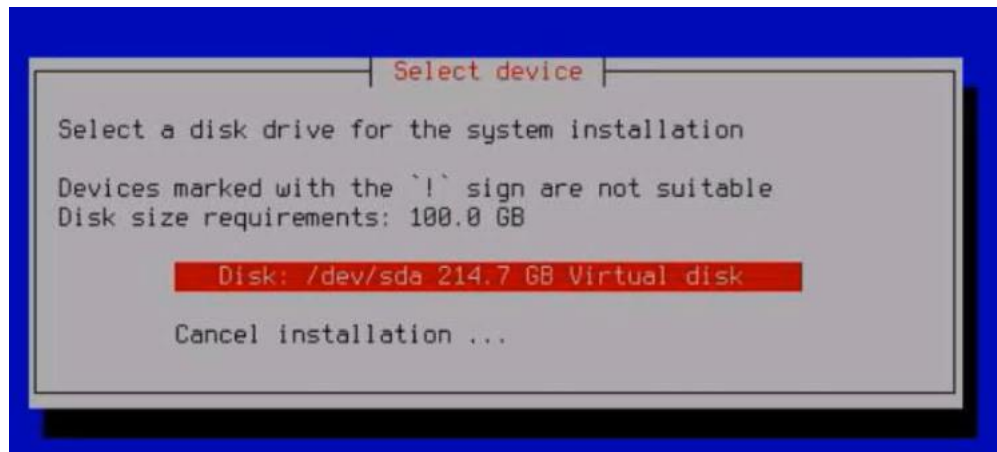
3) Se elige el Idioma Español.



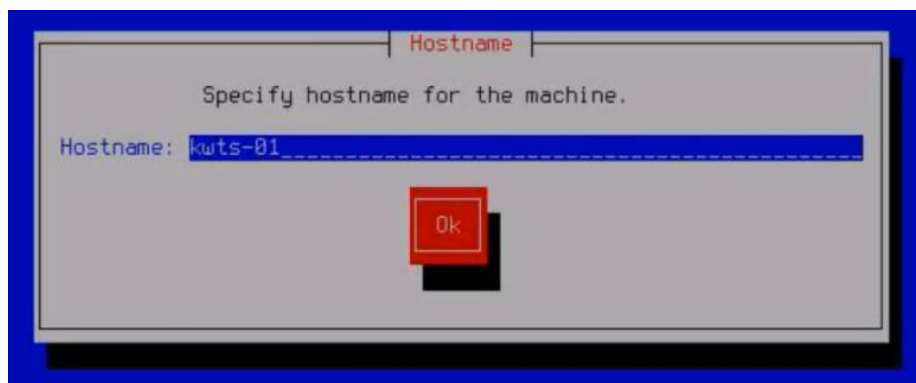
4) Se Acepta el License Agreement.



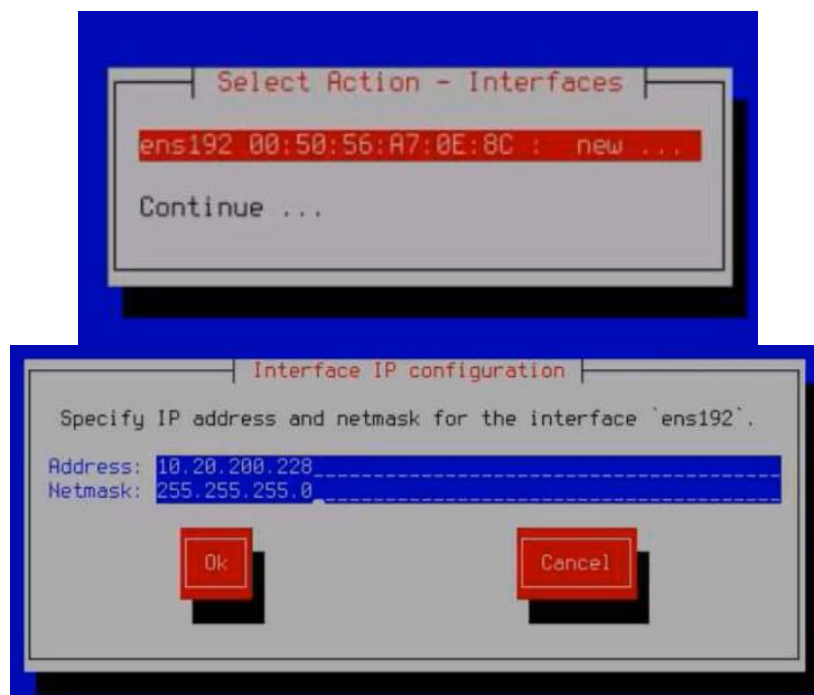
5) Se selecciona el disco de almacenamiento:

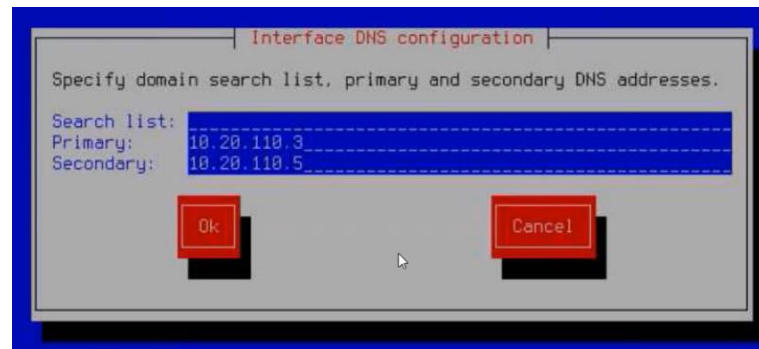


6) Se especifica el hostname:



7) Se configura la interfaz de red:

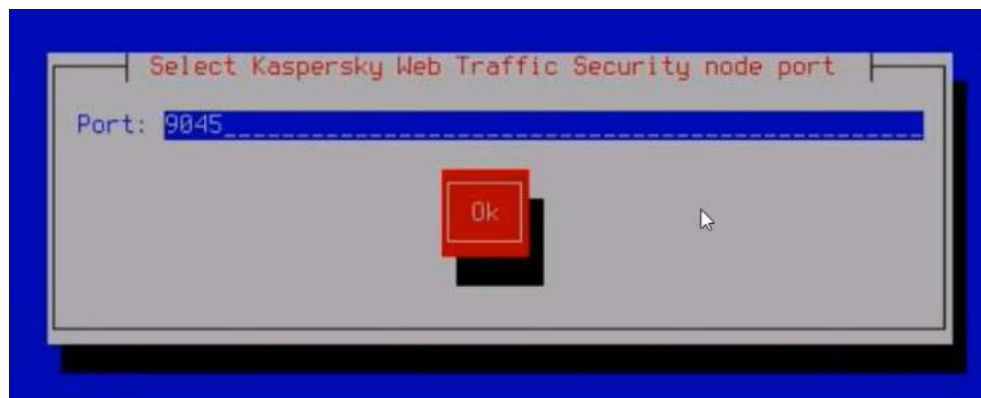




8) Se configura la cuenta de “**Administrator**”:



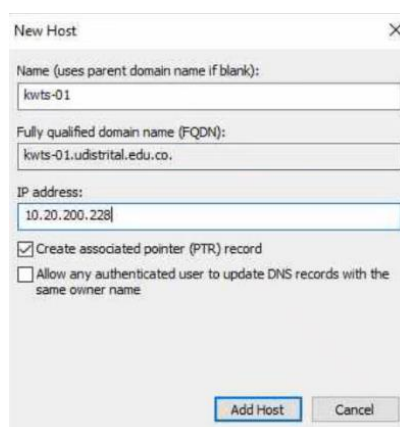
9) Se configura el puerto (Por defecto):



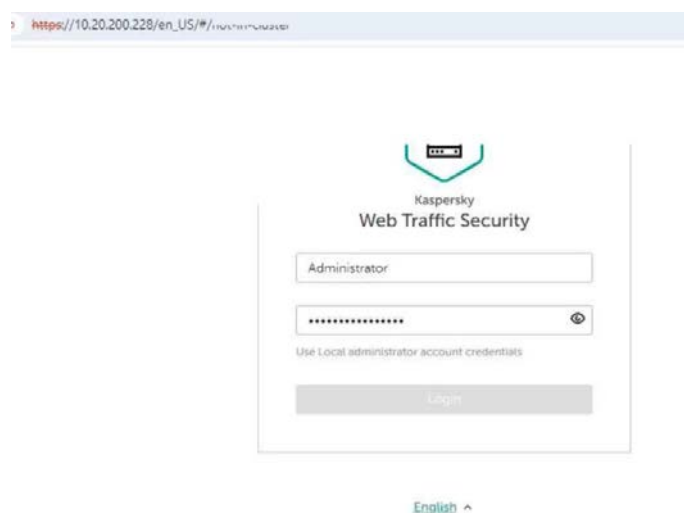
- 10) El servidor finaliza la instalación, reinicia el sistema operativo y procede a generar un fingerprint de conexión:



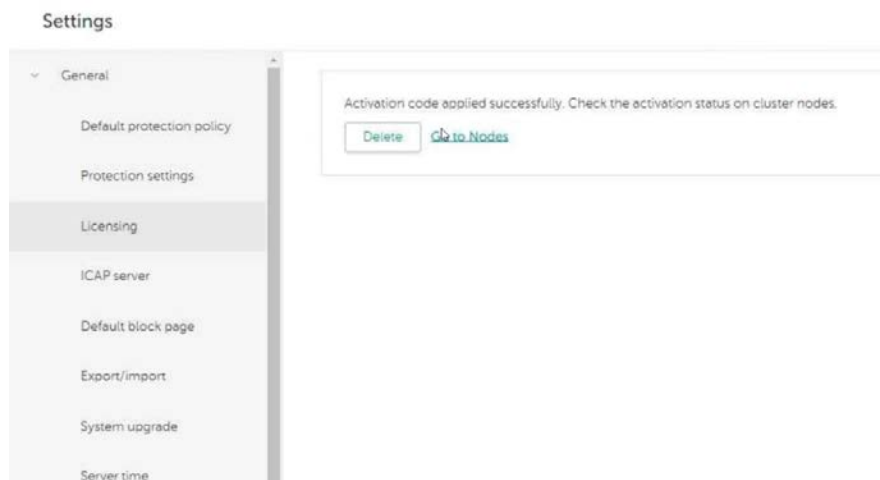
- 11) Generamos el registro DNS:



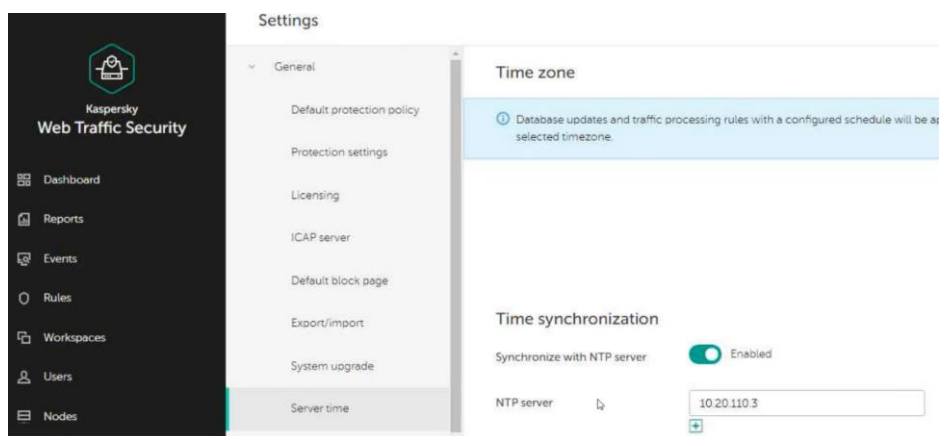
- 12) Se procede al login dentro de la interfaz web por primera vez:



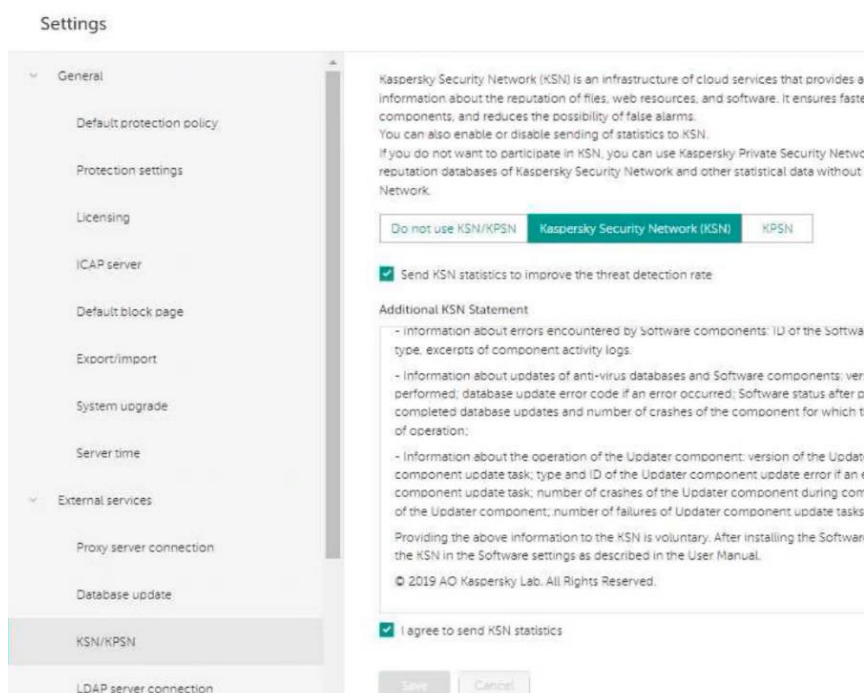
13) Se procede a adicionar la licencia:



14) Se configura el tiempo/ servidor NTP:



15) Habilitar el uso de KSN:



- 16) Generamos el usuario de Active Directory para integración mediante LDAP. Para esto se requiere generación de archivo KEYTAB mediante línea de comando:



- 17) Creación de Keytab:

```
C:\Windows\System32>ktutil.exe /crypto AES256-SHA1 /ptype KR85_NT_PRINCIPAL /out C:\kwts-ldap.keytab /princ kwts-ldap-user@UDISTRITAL.EDU.CO /pass Lb3M*w,3Qk1*ic*
NOTE: creating a keytab but not mapping principal to any user.
For the account to work within a Windows domain, the
principal must be mapped to an account, either at the
domain level (with /mapuser) or locally (using ksetup)
If you intend to map kwts-ldap-user@UDISTRITAL.EDU.CO to an account through other means
or don't need to map the user, this message can safely be ignored.
WARNING: pType and account type do not match. This might cause problems.
Key created.
Output keytab to C:\kwts-ldap.keytab:
Keytab version: 0x502
keysize 82 kwts-ldap-user@UDISTRITAL.EDU.CO ptype 1 (KR85_NT_PRINCIPAL) vno 1 etype 0x12 (AES256-SHA1) keylength 32 (0xd4de118e466e43ed99cc6f4fce3726680dae41ce9053ae5cb845d0dc7eab66be)
```

- 18) Adicionar conexión para integración con LDAP, incluyendo el nuevo KEYTAB:

Edit connection

×

Name

KWTS node 01 integration ldap

Keytab file

A keytab file is a file containing pairs of unique user names (principals) and encrypted keys, derived from the Kerberos password. Keytab files are used in various remote systems supporting Kerberos to authenticate users without entering a password.

kwts-ldap.keytab

Replace

Entries in keytab file:

kwts-ldap-user@UDISTRITAL.EDU.CO

Search base (Base DN)

dc=udistrital, dc=edu, dc=co

Save

Cancel

- 19) Se confirma la correcta integración y sincronización con LDAP

LDAP cache status

KWTS node 01 integration ldap:

Connection	Data for rules matching	User accounts autofill
29/01/2024 15:23:07	29/01/2024 15:23:07	29/01/2024 15:23:07

- 20) En este paso se genera un nuevo archivo de keytab y se añade en la sección de Single Sign On mediante KERBEROS. (Punto que actualmente se encuentra sujeto a revisión mediante ticket de Soporte por problemas durante la configuración).

4. Conclusión

El proceso de implementación fue rápido y sin inconvenientes hasta el punto de integración mediante Kerberos para evitar que pida contraseña ante la navegación a los usuarios, el problema es que llegado a este punto luego de varios intentos se necesito derivar el caso a soporte y actualmente sigue vigente el caso bajo el número: **INC000016178166**.

kaspersky

www.kaspersky.com/
www.securelist.com

© 2024 AO Kaspersky Lab.

All rights reserved. Registered trademarks and service marks are the property of their respective owner

INFORME DE INSTALACIÓN DE LA SOLUCIÓN PARA PROTECCIÓN DE AMENAZAS A LA RED KASPERSKY ANTI-TARGETED ATTACK

Instalación, configuración, licenciamiento y puesta en marcha de la solución Kaspersky
Anti-targeted Attack para la protección de amenazas a la Red para la Universidad
Distrital Francisco José de Caldas.

06 DE MARZO DE 2024

INFOCOMUNICACIONES

Autopista Medellín Km 3.5 vía Siberia – TTCB – OFC C4 / C5



INSTALACION, CONFIGURACIÓN, LICENCIAMIENTO Y PUESTA EN MARCHA DE LA SOLUCIÓN KASPERSKY ANTI-TARGETED ATTACK PARA LA PROTECCIÓN DE AMENAZAS A LA RED PARA LA UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS.

Informe de instalación de la solución para protección de amenazas a la red Kaspersky Anti-targeted Attack para la universidad distrital Francisco Jose de Caldas.

El siguiente informe consigna las actividades que se llevaron a cabo desde el pasado 29 de enero de 2024 con el objetivo de dar alcance a la Implementación de la solución para protección contra amenazas de red Kaspersky Anti-Targeted Attack para la universidad distrital Francisco Jose de Caldas.

Información del Cliente	
Nombre de la Empresa	Universidad Distrital Francisco Jose de Caldas
Nombre del Contacto	Martha Cecilia Valdés Cruz – Líder Red de Datos UDNET
Correo Electronico	udnet@udistrital.edu.co
Teléfono de Contacto	6013239300 ext 1307

TABLA DE CONTENIDO.

1.	Objeto del Contrato.....	5
2.	Objetivo General	5
3.	Instalación y Configuración de Kaspersky Security for Mail Gateway (KSMG).....	5
4.	Instalación y Configuración de Kaspersky Web Traffic Security (KWTS).....	9
5.	Instalación y configuración Kaspersky Anti – Targeted Attack Platform (KATA) – NODO CENTRAL.	13
6.	Instalación y configuración Kaspersky Anti – Targeted Attack Platform (KATA) – SENSOR.....	15
7.	Instalación y configuración Kaspersky Anti – Targeted Attack Platform (KATA) – SANDBOX.	18
8.	Instalación y configuración Kaspersky Anti – Targeted Attack Platform (KATA) – EDR EXPERT.....	21
9.	Diagrama de red (arquitectura actual) de instalación para los componentes de la solución para detección, prevención y respuesta de red (NDR) de ataques de red con la solución Kaspersky Anti-targeted Attack Platform KATA.....	25
10.	Tareas Programadas y Ejecutadas.	26

INDICE DE TABLAS.

Tabla 1	Licenciamiento Kaspersky Componente red	5
Tabla 2	Accesos a Plataforma KSMG Instalada	6
Tabla 3	Roles para KSMG instalado en Cluster	6
Tabla 4	Accesos a Plataforma KWTS Instalada	9
Tabla 5	Accesos a Plataforma KATA-CN Instalada	13
Tabla 6	Accesos a Plataforma KATA-SENSOR Instalada	16

Tabla 7 Accesos a Plataforma KATA-SANDBOX Instalada.....	18
Tabla 8 Accesos a Consolas KCS Instaladas.....	21

TABLA DE ILUSTRACIONES.

Ilustración 1 - Interfaz de acceso Plataforma KSMG 01	6
Ilustración 2 – Dashboard principal KSMG 01	7
Ilustración 3 - Licenciamiento Plataforma KSMG	7
Ilustración 4 – Integración plataforma KSMG 01 con KATA	8
Ilustración 5 - Integración plataforma KSMG 01 con KATA	8
Ilustración 6 – Actualización bases de datos plataforma KSMG 01.....	8
Ilustración 7- versión Instalada actualizada de la plataforma KSMG 01.....	9
Ilustración 8 – Interfaz de Acceso a la plataforma KWTS	10
Ilustración 9 - Licenciamiento Plataforma KWTS	10
Ilustración 10 - Dashboard principal KWTS	11
Ilustración 11 - Actualización bases de datos plataforma KWTS.....	11
Ilustración 12 - Integración plataforma KWTS con KATA	12
Ilustración 13 - Integración plataforma KWTS con KATA	12
Ilustración 14 - versión Instalada actualizada de la plataforma KWTS.....	12
Ilustración 15 - Interfaz de Acceso a la plataforma KATA-CN.....	13
Ilustración 16 - Dashboard principal KWTS	14
Ilustración 17 - Licenciamiento Plataforma KATA-CN Y EDR EXPERT	14
Ilustración 18 - Integración plataforma KATA con SENSOR.....	15
Ilustración 19 – Versión instalada actualizada de la plataforma KATA-CN.....	15

Ilustración 20 Interfaz de Acceso a la plataforma KATA (SENSOR).....	16
Ilustración 21 - Dashboard principal KATA (SENSOR).....	16
Ilustración 22 - Integración plataforma KATA(SENSOR) con KATA.....	17
Ilustración 23 - Integración plataforma KATA(SENSOR) con KATA.....	17
Ilustración 24 - Versión instalada actualizada de la plataforma KATA(SENSOR).18	
Ilustración 25 - Interfaz de Acceso a la plataforma KATA (SANDBOX).....	19
Ilustración 26 - Dashboard principal KATA (SANDBOX).....	19
Ilustración 27 - Integración plataforma KATA(SANDBOX) con KATA.....	19
Ilustración 28 - Integración plataforma KATA(SENSOR) con KATA.....	20
Ilustración 29 - Actualización bases de datos plataforma KATA(SANDBOX)	20
Ilustración 30 - Versión instalada actualizada de la plataforma KATA(SANDBOX 20	
Ilustración 31 - Interfaz de Acceso a la plataforma KATA (EDR EXPERT).....	21
Ilustración 32 - Dashboard principal KATA (EDR EXPERT).....	22
Ilustración 33 - Dashboard principal KATA (EDR EXPERT).....	22
Ilustración 34 - Licenciamiento Plataforma KATA-CN Y EDR EXPERT	23
Ilustración 35 - Licenciamiento Plataforma KATA (EDR EXPERT).....	23
Ilustración 36 - Licenciamiento Plataforma KATA (EDR EXPERT) - Endpoint	24
Ilustración 37 - Integración plataforma KATA(EDR EXPERT) con KATA	24
Ilustración 38 - Versión instalada actualizada de la plataforma KATA(EDR EXPERT) – Agente EDR	24
Ilustración 39 – Topología de red para todos los componentes de la plataforma KATA.....	25

1. Objeto del Contrato

Componente 1

Adquirir, instalar, configurar y puesta en correcto funcionamiento de una solución tecnológica para equipos servidores físicos y virtuales pc, portátiles y máquinas virtuales propiedad de la Universidad Distrital Francisco José de Caldas, que permita la detección, prevención y respuesta de red contra ciberamenazas, incluyendo soporte técnico 7x24 (update y Upgrade).

2. Objetivo General

Realizar la instalación de las soluciones Kaspersky Anti-targeted Attack Platform para asegurar la detección, prevención y respuesta de red (NDR) para la protección correcta de los datos que hacen parte del parque informático de la Universidad Distrital Francisco José de Caldas, a continuación, se enumeran y describen las licencias adquiridas por la universidad distrital y que hace parte de este informe de instalación del despliegue adquirido y de los componentes que componen la solución.

ITEM	Descripción de la Licencias	Cantidad
1	Licencias de Kaspersky Anti-targeted Attack EDR Agent	400
2	Licencias Kaspersky Anti-targeted attack Platform	1
3	Entrenamiento KATA Security Analyst	5

Tabla 1 Licenciamiento Kaspersky Componente red

3. Instalación y Configuración de Kaspersky Security for Mail Gateway (KSMG).

Kaspersky Security for Mail Gateway en adelante **KSMG** es una solución de protección contra las amenazas que comúnmente están dirigidas al correo electrónico fabricada y soportada por las tecnologías de Kaspersky, la solución ha sido desplegada en la plataforma de hiperconvergencia con la que cuenta la Universidad Distrital para alojar todos sus servidores críticos de operación, la solución actúa como una puerta de enlace (Gateway) para la recepción y entrega de correos basada en la configuración de un conector que se hace presente en Office 365 servidor de correo de la Universidad Distrital.

En las imágenes a continuación se puede observar el acceso a la plataforma y direcciones donde están alojados los servicios en este caso el de KSMG, más adelante en este informe se podrá visualizar la topología de red final y el flujo de tráfico, e integración con el nodo central KATA.

PLATAFORMA	URL de Acceso	Acceso	Usuario
KSMG-01	https://10.20.200.225/en_US/#/	HTTP	Administrator
KSMG-02	https://10.20.200.226/en_US/#/	HTTP	Administrator
KSMG (SSH)	ssh://10.20.200.226	SSH	Administrator

Tabla 2 Accesos a Plataforma KSMG Instalada

Descripción del rol de cada servidor desplegado.

La solución KSMG ha sido desplegada en modo Clúster por lo cual se relacionan 2 IP para la solución ya que están dos máquinas virtuales instaladas y configuradas con el licenciamiento y direccionamiento correspondientes.

NOMBRE	FUNCIÓN	DESCRIPCIÓN	IP
KSMG-01	Servidor de KSMG (Entrante)	Servidor de Kaspersky Secure Mail Gateway para correos entrantes.	10.20.200.225
KSMG-02	Servidor de KSMG (Saliente)	Servidor de Kaspersky Secure Mail Gateway para correos salientes.	10.20.200.226

Tabla 3 Roles para KSMG instalado en Cluster

KSMG 01

Imagen KSMG 01 – Acceso (10.20.200.225 y Administrator)

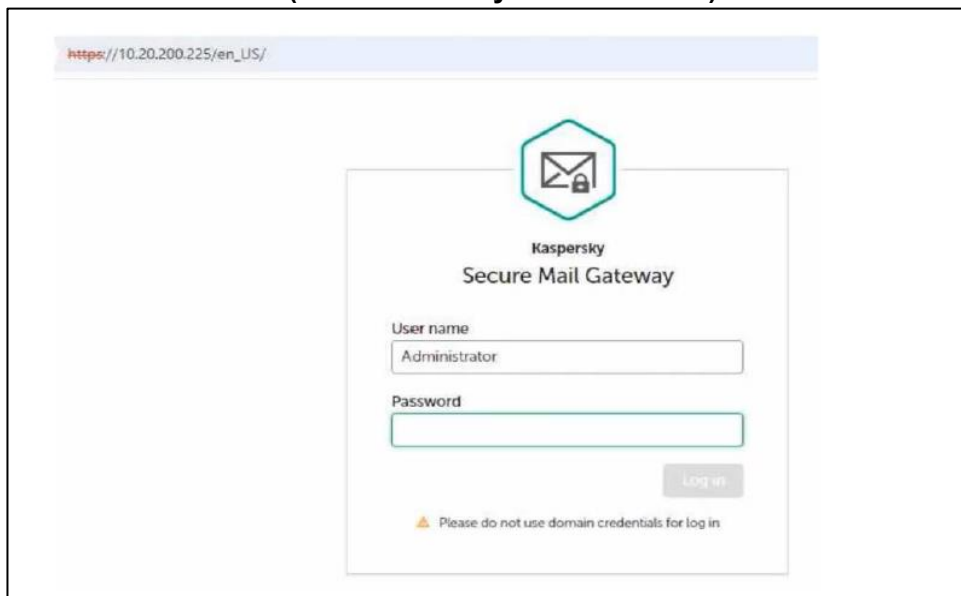


Ilustración 1 - Interfaz de acceso Plataforma KSMG 01

Imagen KSMG – Dashboard

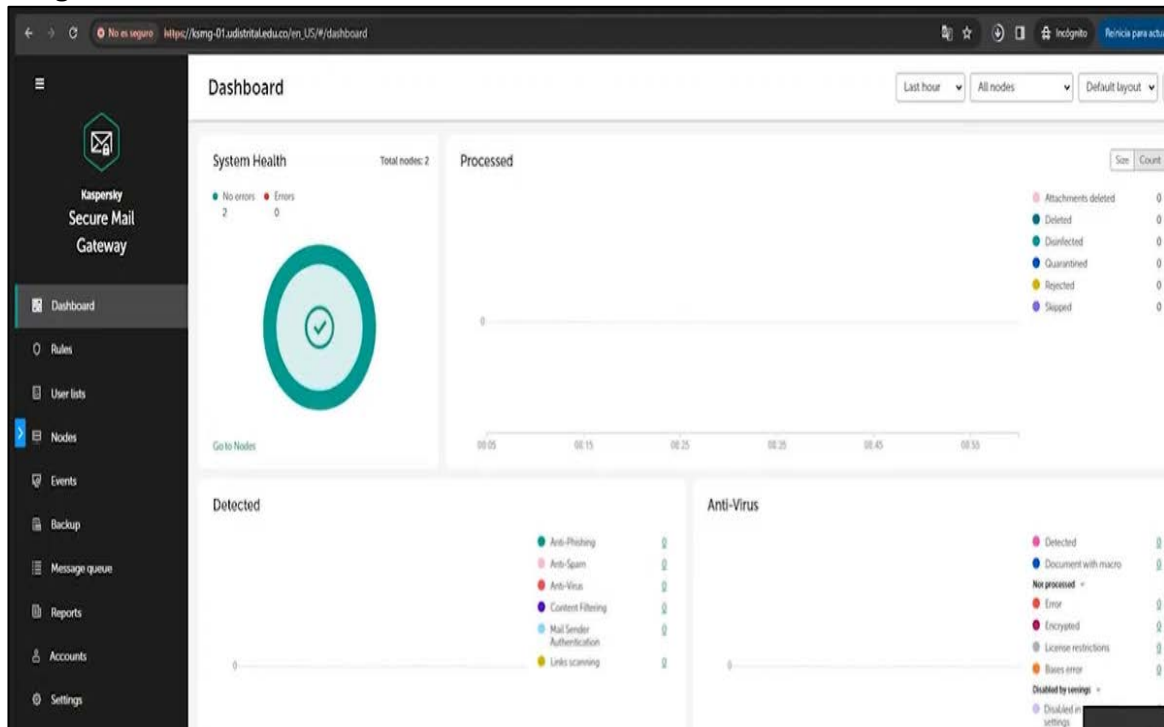


Ilustración 2 – Dashboard principal KSMG 01

Imagen KSMG – Licenciamiento

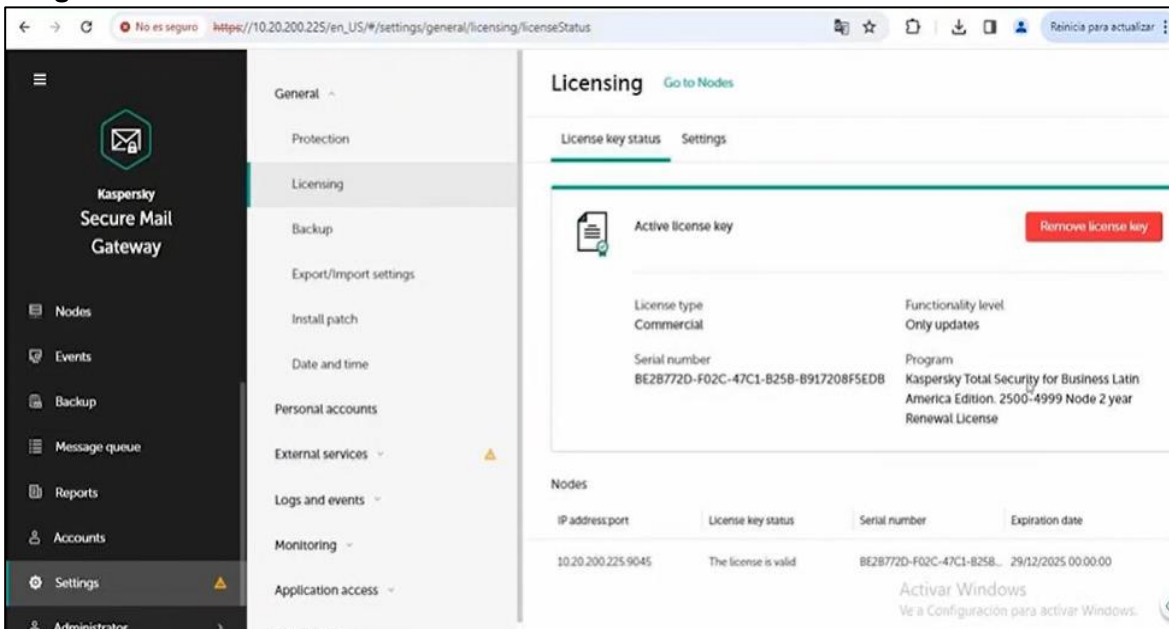


Ilustración 3 - Licenciamiento Plataforma KSMG

Imagen KSMG – Integración KATA

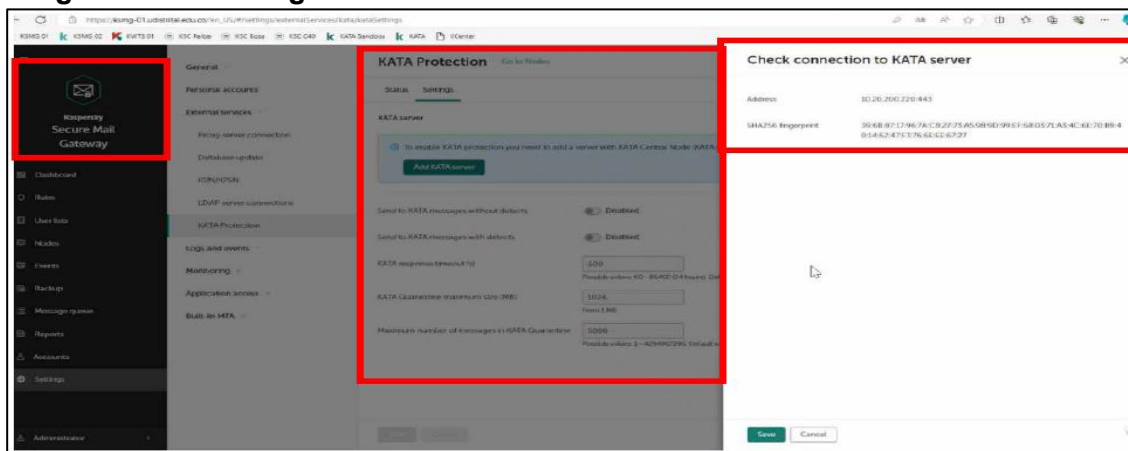


Ilustración 4 – Integración plataforma KSMG 01 con KATA



Ilustración 5 - Integración plataforma KSMG 01 con KATA

Imagen KSMG – Actualización Bases de Datos.

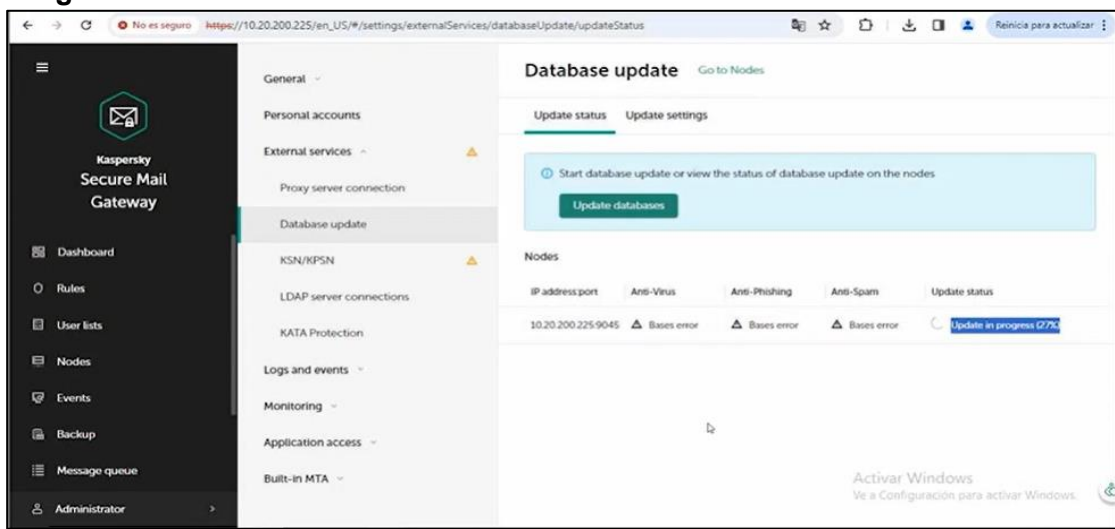


Ilustración 6 – Actualización bases de datos plataforma KSMG 01

Imagen KSMG – Versión



Ilustración 7- Versión Instalada actualizada de la plataforma KSMG 01

El Servidor **KSMG 02** se desplegó con la misma configuración de **KSMG 01** por lo tanto aplican las mismas imágenes registradas anteriormente.

4. Instalación y Configuración de Kaspersky Web Traffic Security (KWTS).

Kaspersky Web Traffic Security adelante **KWTS** es una solución de protección contra las amenazas que comúnmente están dirigidas al entorno y operación de la navegación de los usuarios en internet y tráfico mediante navegadores de internet utilizados en los equipos de la Universidad Distrital

En las imágenes a continuación se puede observar el acceso a la plataforma y direcciones donde están alojados los servicios en este caso el de KWTS, más adelante en este informe se podrá visualizar la topología de red final y el flujo de tráfico, e integración con el nodo central KATA.

PLATAFORMA	URL de Acceso	Acceso	Usuario
KWTS	https://10.20.200.228/en_US/#/	HTTP	Administrator
KWTS	ssh://10.20.200.228	ssh	Administrator

Tabla 4 Accesos a Plataforma KWTS Instalada

Imagen KWTS – Acceso (10.20.200.228 y Administrator)

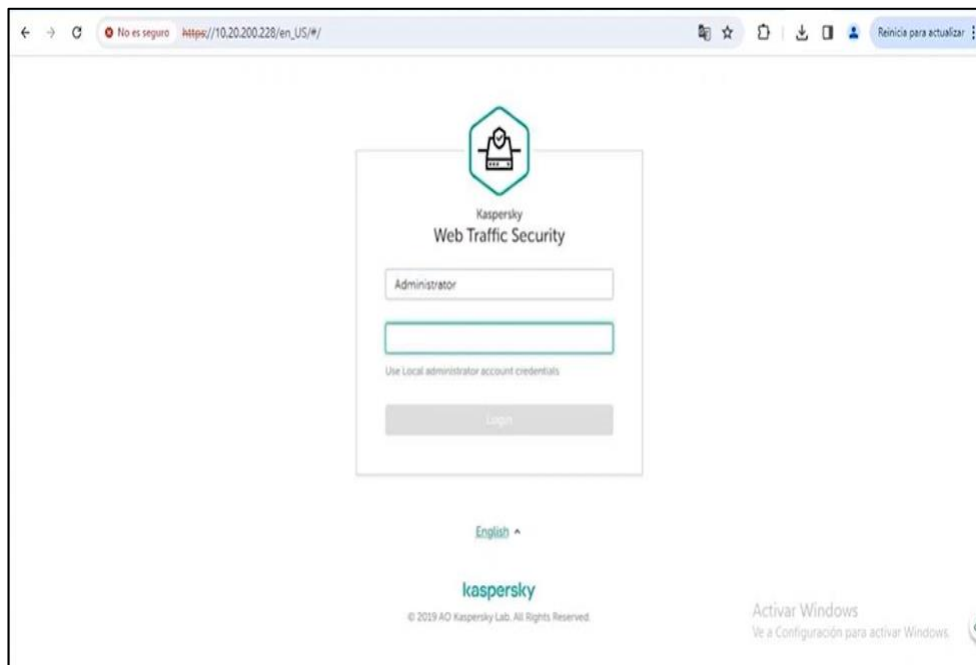


Ilustración 8 – Interfaz de Acceso a la plataforma KWTS

Imagen KWTS – Licenciamiento

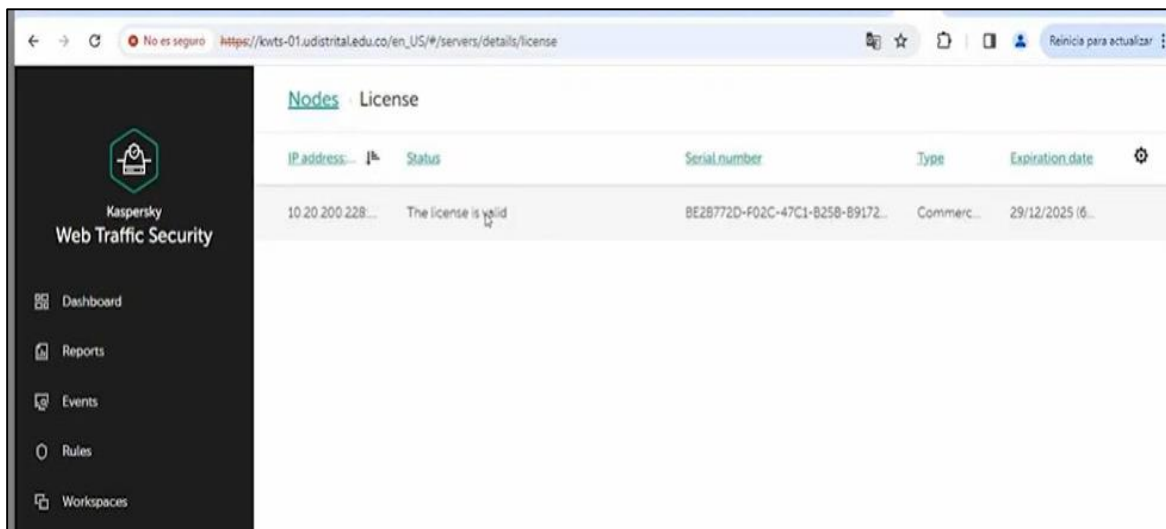


Ilustración 9 - Licenciamiento Plataforma KWTS

Imagen KWTS – Dashboard

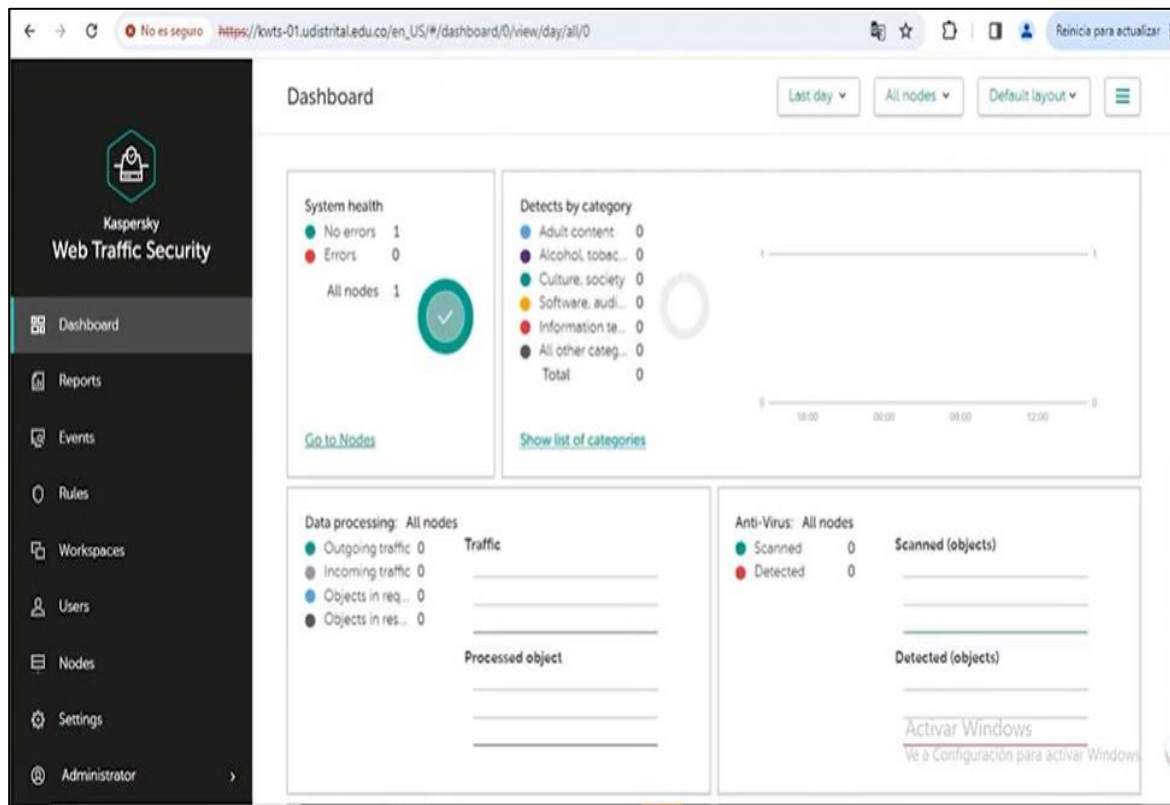


Ilustración 10 - Dashboard principal KWTS

Imagen KWTS – Actualización Bases de Datos.

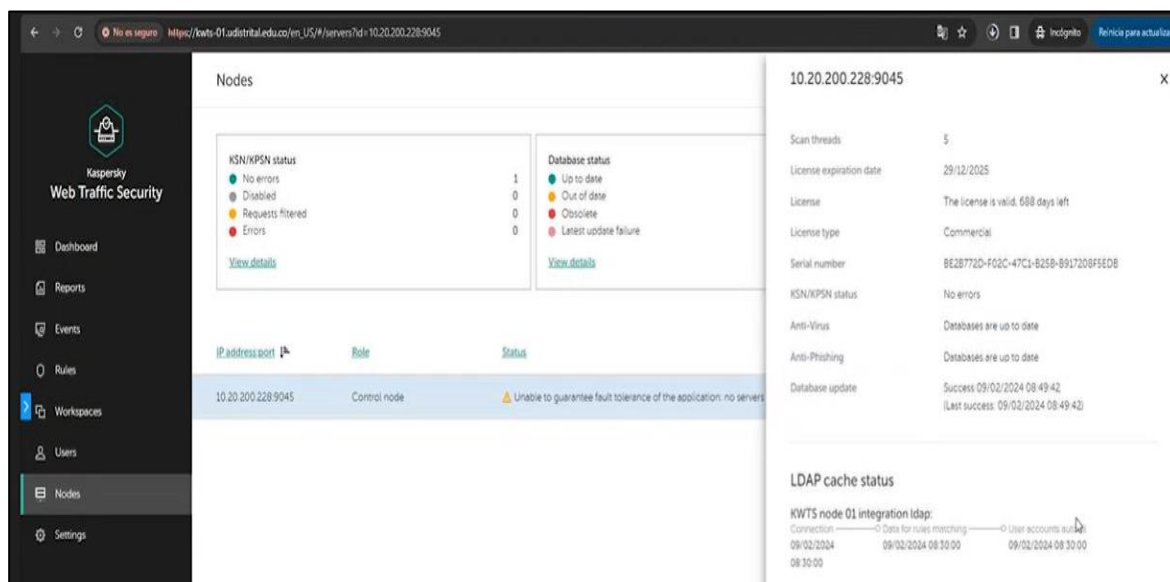


Ilustración 11 - Actualización bases de datos plataforma KWTS

Imagen KWTS – Integración KATA

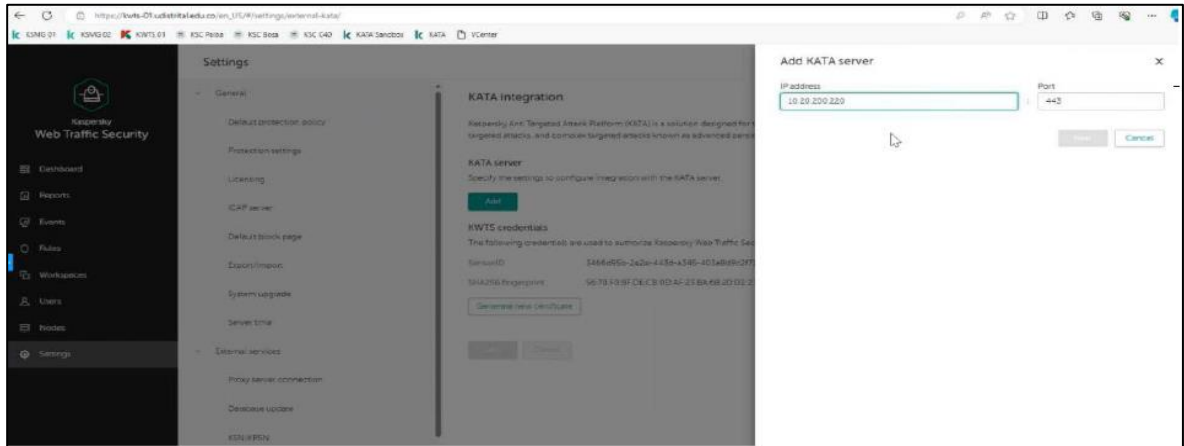


Ilustración 12 - Integración plataforma KWTS con KATA

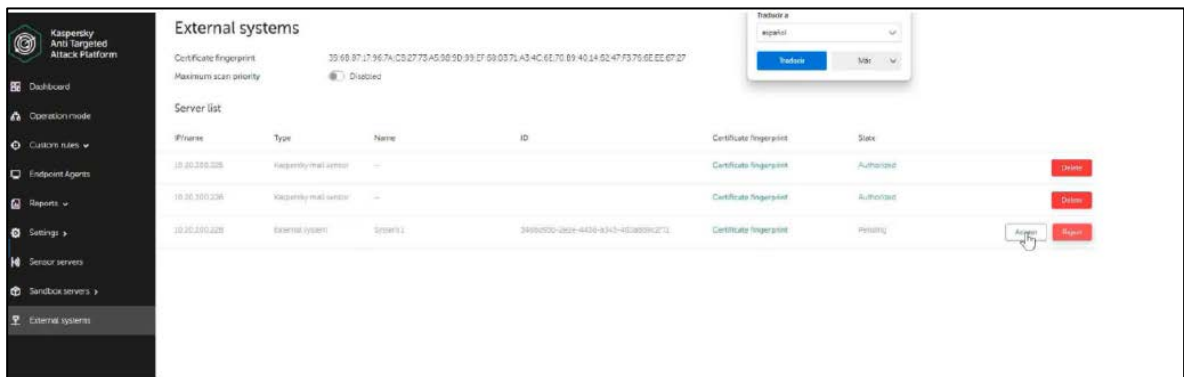


Ilustración 13 - Integración plataforma KWTS con KATA

Imagen KWTS – Versión

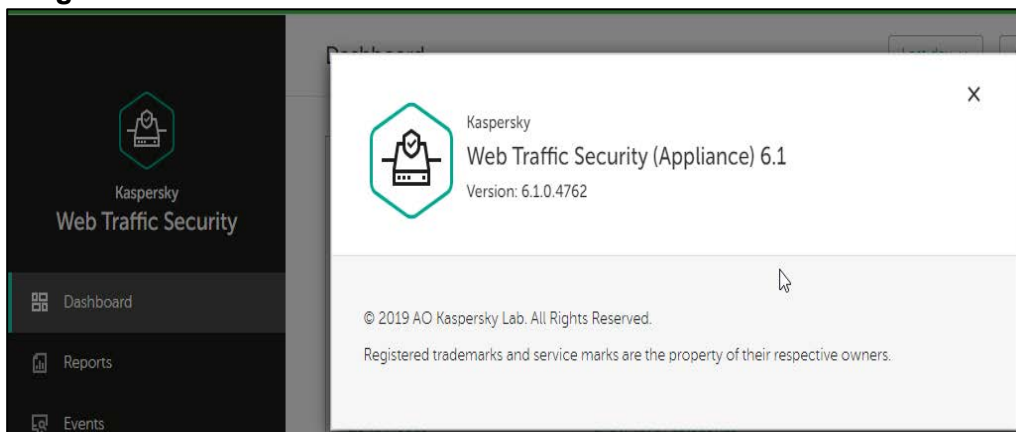


Ilustración 14 - versión Instalada actualizada de la plataforma KWTS

5. Instalación y configuración Kaspersky Anti – Targeted Attack Platform (KATA) – NODO CENTRAL.

Kaspersky Anti-targeted Attack Platform en adelante **KATA** es una solución de protección contra las amenazas que están presentes en el tráfico de red, está compuesta por un NODO CENTRAL que se encarga de realizar el análisis de toda la información recibida con su motor antimalware y que a su vez recibe información de plataformas adicionales como SENSORES de red, herramientas de seguridad como SANDBOX, KWTS, KSMG, Endpoints, de tal manera que al recibir y tratar dicha información con telemetría enriquecida podrá hacer frente a las amenazas y comportamientos maliciosos que se presenten en la red y en los equipos de la Universidad Distrital Francisco Jose de Caldas.

En las imágenes a continuación se puede observar el acceso a la plataforma y direcciones donde están alojados los servicios en este caso el nodo Central de KATA, más adelante en este informe se podrá visualizar la topología de red final y el flujo de tráfico.

PLATAFORMA	URL de Acceso	Acceso	Usuario
KATA-CN	https://10.20.200.220/en_US/#/	HTTP	Admin - plataformas
KATA-CN	ssh://10.20.200.220	SSH	admin

Tabla 5 Accesos a Plataforma KATA-CN Instalada

Imagen KATA (Nodo Central) – Acceso (10.20.200.220 y Plataformas)

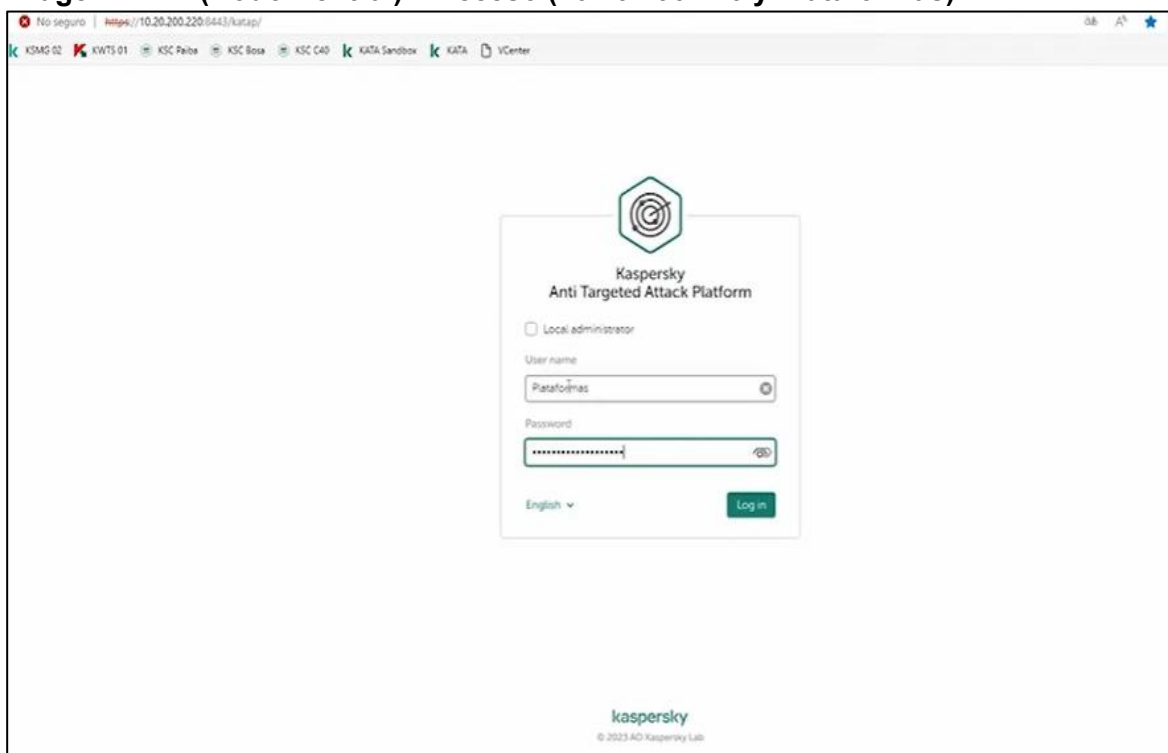


Ilustración 15 - Interfaz de Acceso a la plataforma KATA-CN

Imagen KATA (Nodo Central) – Dashboard

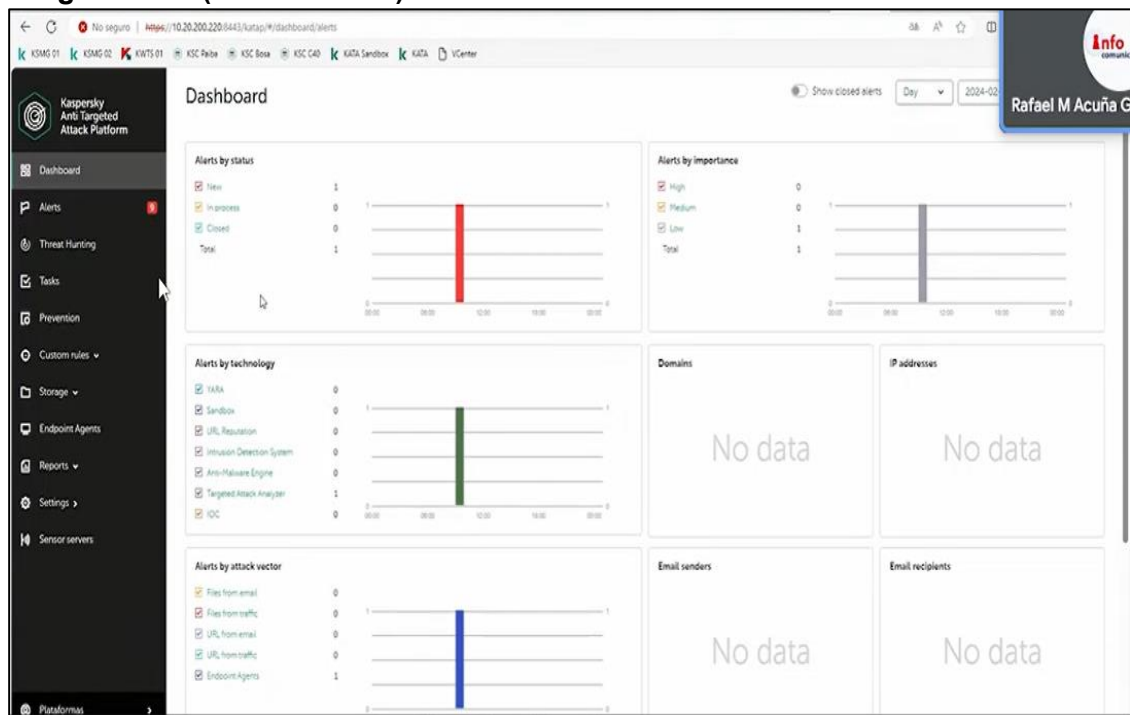


Ilustración 16 - Dashboard principal KWTS

Imagen KATA (Nodo Central) – Licenciamiento

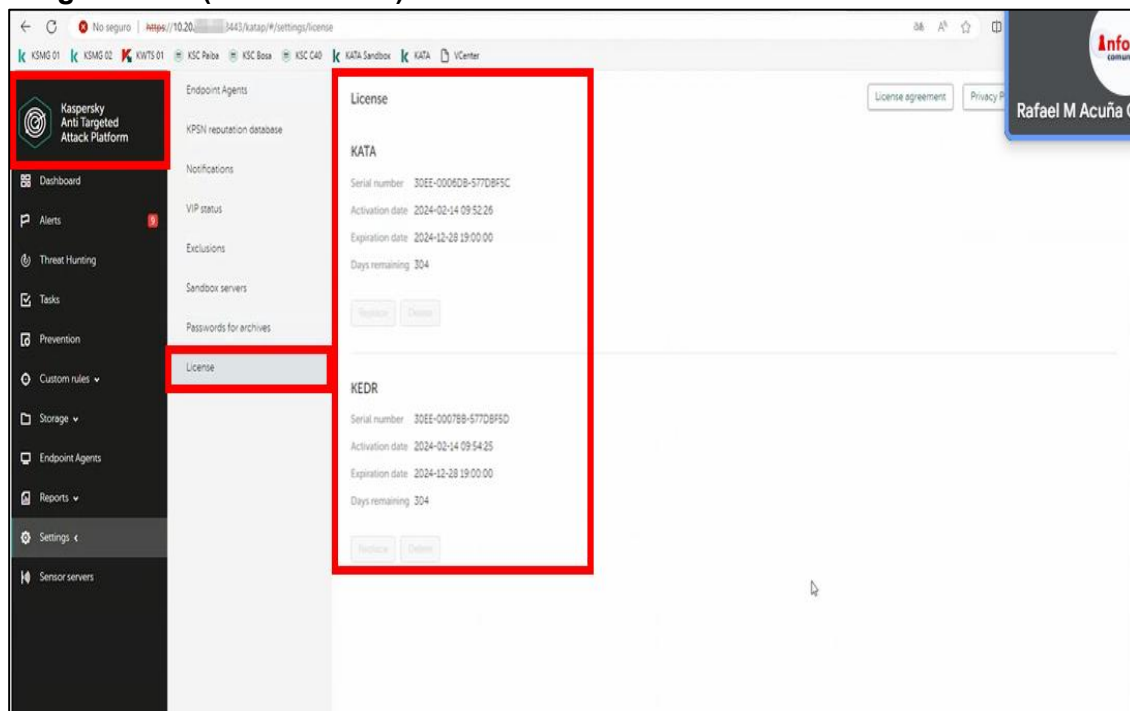


Ilustración 17 - Licenciamiento Plataforma KATA-CN Y EDR EXPERT

Imagen KATA (Nodo Central) – Integración KATA

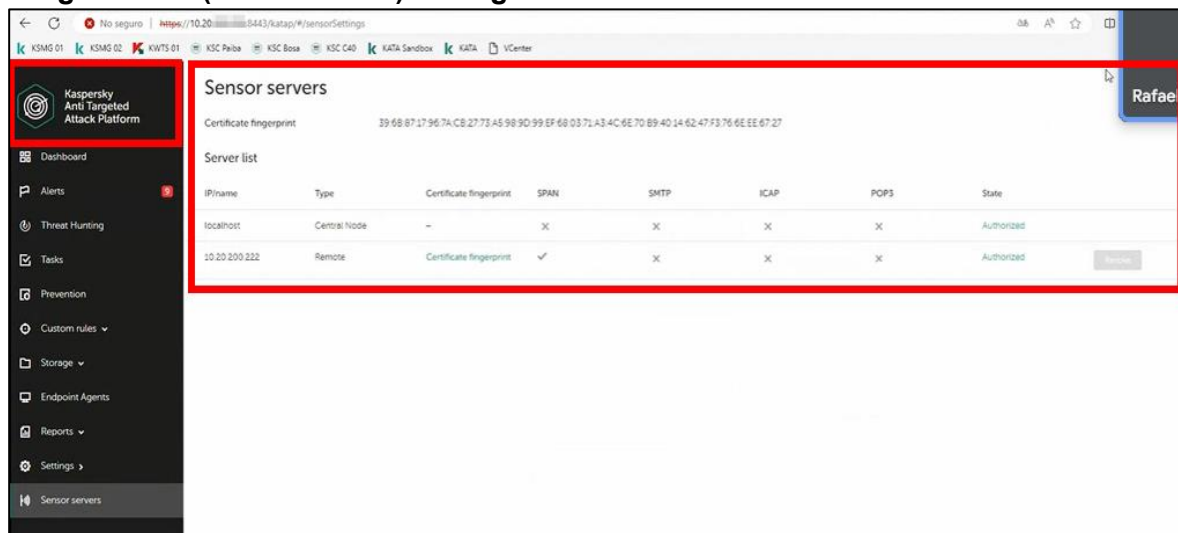


Ilustración 18 - Integración plataforma KATA con SENSOR

Imagen KATA (Nodo Central) – Versión

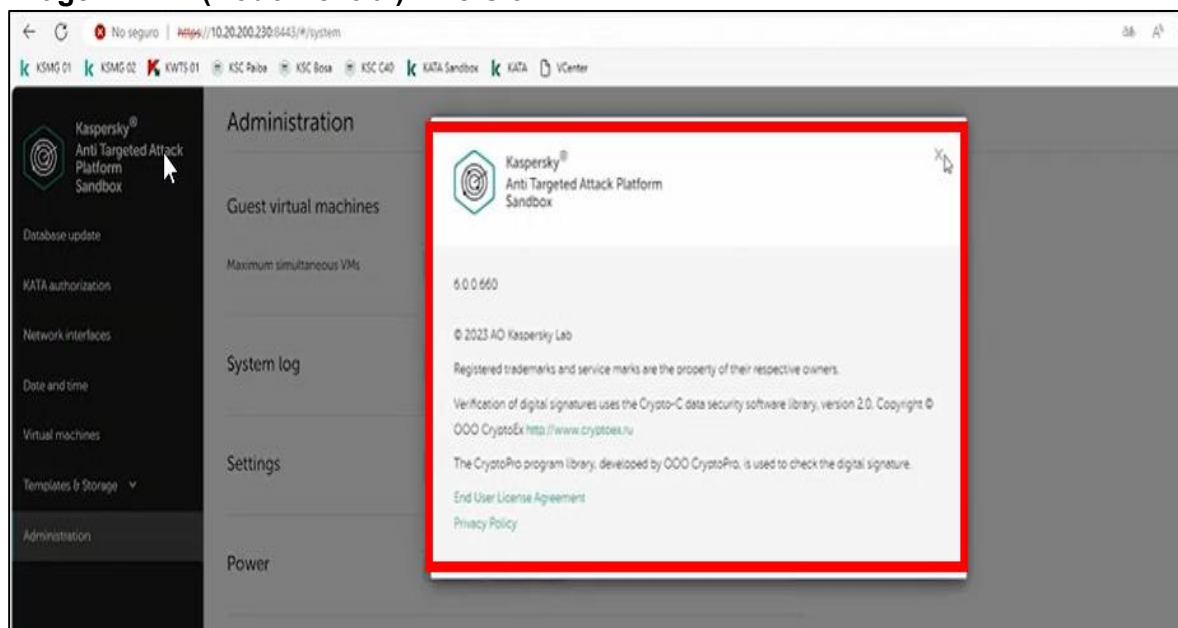


Ilustración 19 – Versión instalada actualizada de la plataforma KATA-CN

6. Instalación y configuración Kaspersky Anti – Targeted Attack Platform (KATA) – SENSOR.

Kaspersky Anti-targeted Attack Platform en adelante **KATA** es una solución de protección contra las amenazas que están presentes en el tráfico de red, está compuesta por un NODO CENTRAL que se encarga de realizar el análisis de toda la información recibida con

su motor antimalware y que a su vez recibe información de plataformas adicionales como SENSORES de red, herramientas de seguridad como SANDBOX, KWTS, KSMG, Endpoints, de tal manera que al recibir y tratar dicha información con telemetría enriquecida podrá hacer frente a las amenazas y comportamientos maliciosos que se presenten en la red y en los equipos de la Universidad Distrital Francisco Jose de Caldas.

En las imágenes a continuación se puede observar el acceso a la plataforma y direcciones donde están alojados los servicios en este caso el SENSOR de KATA, más adelante en este informe se podrá visualizar la topología de red final y el flujo de tráfico.

PLATAFORMA	URL de Acceso	Acceso	Usuario
KATA-SENSOR	ssh://10.20.200.222	SSH	admin

Tabla 6 Accesos a Plataforma KATA-SENSOR Instalada

Imagen KATA (Sensor) – Acceso (10.20.200.222 y admin)

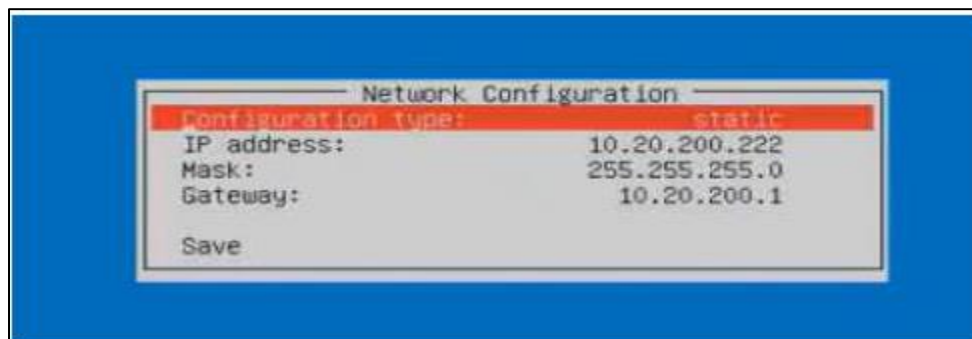


Ilustración 20 Interfaz de Acceso a la plataforma KATA (SENSOR)

Imagen KATA (Sensor) – Dashboard



Ilustración 21 - Dashboard principal KATA (SENSOR)

Imagen KATA (Sensor) – Integración KATA

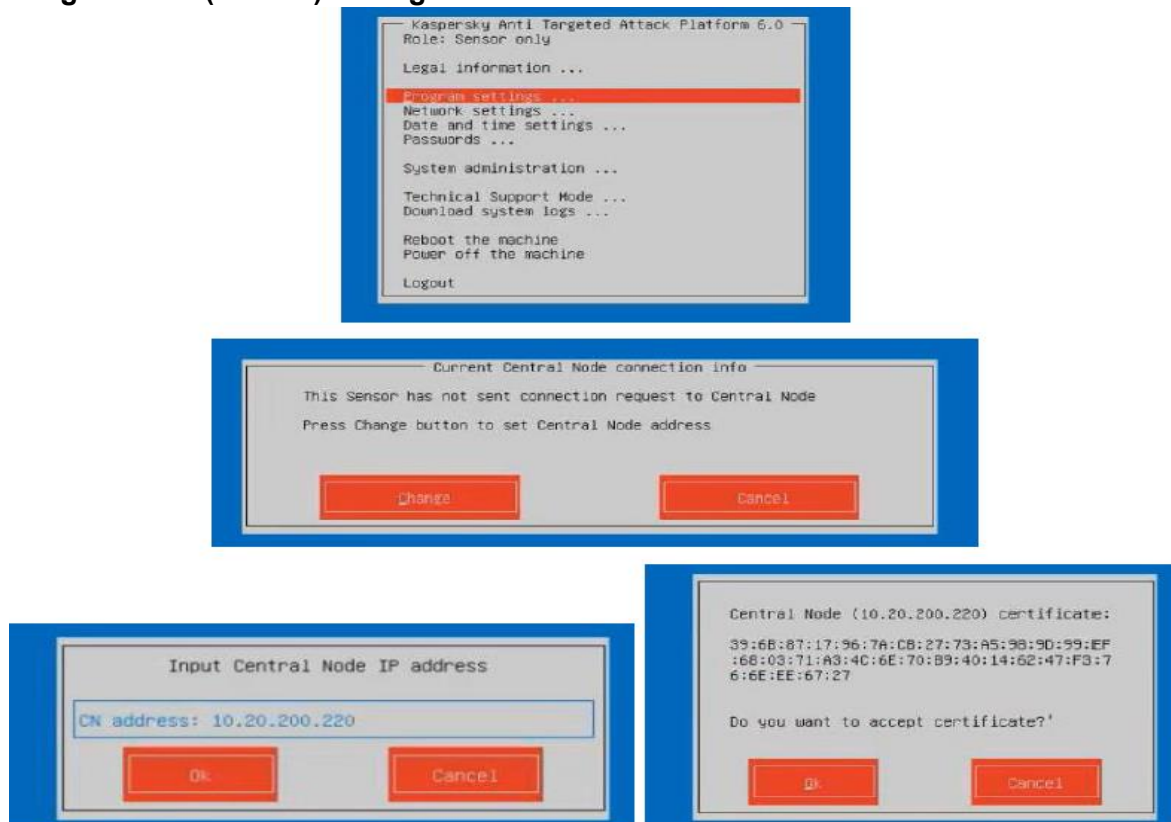


Ilustración 22 - Integración plataforma KATA(SENSOR) con KATA

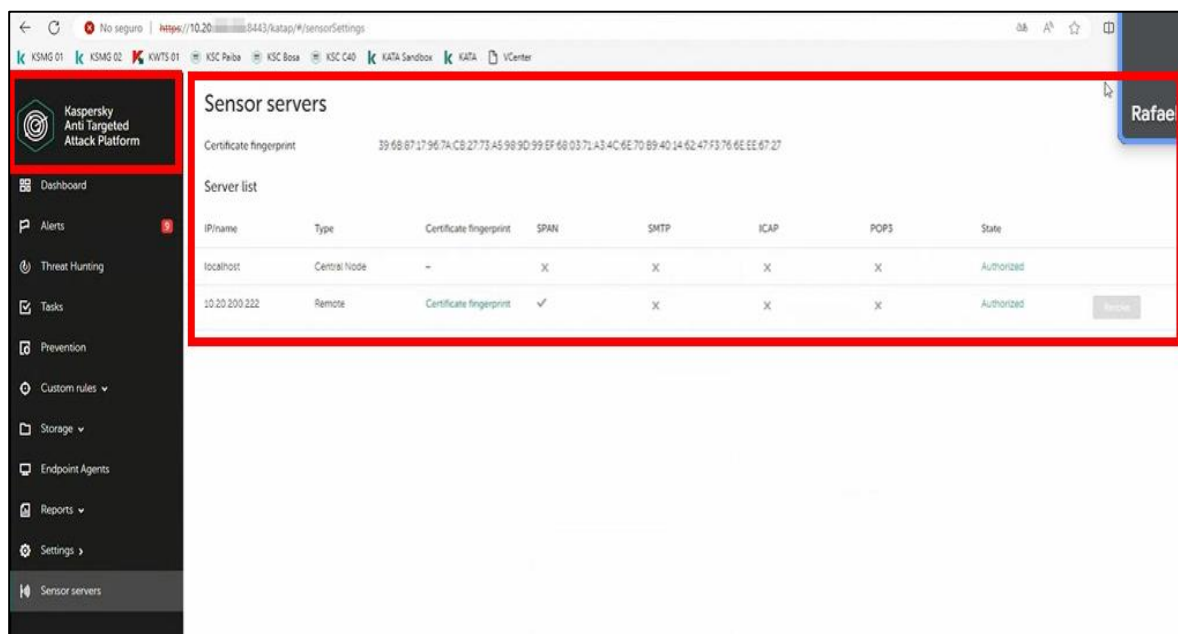


Ilustración 23 - Integración plataforma KATA(SENSOR) con KATA

Imagen KATA (Sensor) – Versión

```

Ubuntu 22.04.2 LTS 1.srv.node1.node.dyn.katasensor tty1
1 login: admin
Password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-84-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
  
```

Ilustración 24 - Versión instalada actualizada de la plataforma KATA(SENSOR)

7. Instalación y configuración Kaspersky Anti – Targeted Attack Platform (KATA) – SANDBOX.

Kaspersky Anti-targeted Attack Platform en adelante **KATA** es una solución de protección contra las amenazas que están presentes en el tráfico de red, está compuesta por un NODO CENTRAL que se encarga de realizar el análisis de toda la información recibida con su motor antimalware y que a su vez recibe información de plataformas adicionales como SENSORES de red, herramientas de seguridad como SANDBOX, KWTS, KSMG, Endpoints, de tal manera que al recibir y tratar dicha información con telemetría enriquecida podrá hacer frente a las amenazas y comportamientos maliciosos que se presenten en la red y en los equipos de la Universidad Distrital Francisco Jose de Caldas.

En las imágenes a continuación se puede observar el acceso a la plataforma y direcciones donde están alojados los servicios en este caso el SANDBOX de KATA, más adelante en este informe se podrá visualizar la topología de red final y el flujo de tráfico.

PLATAFORMA	URL de Acceso	Acceso	Usuario
KATA-SANDBOX	https://10.20.200.230/en_US/#/	HTTP	admin
KATA-SANDBOX	ssh://10.20.200.230	SSH	admin

Tabla 7 Accesos a Plataforma KATA-SANDBOX Instalada

Imagen KATA (Sandbox) – Acceso (10.20.200.230 y admin)

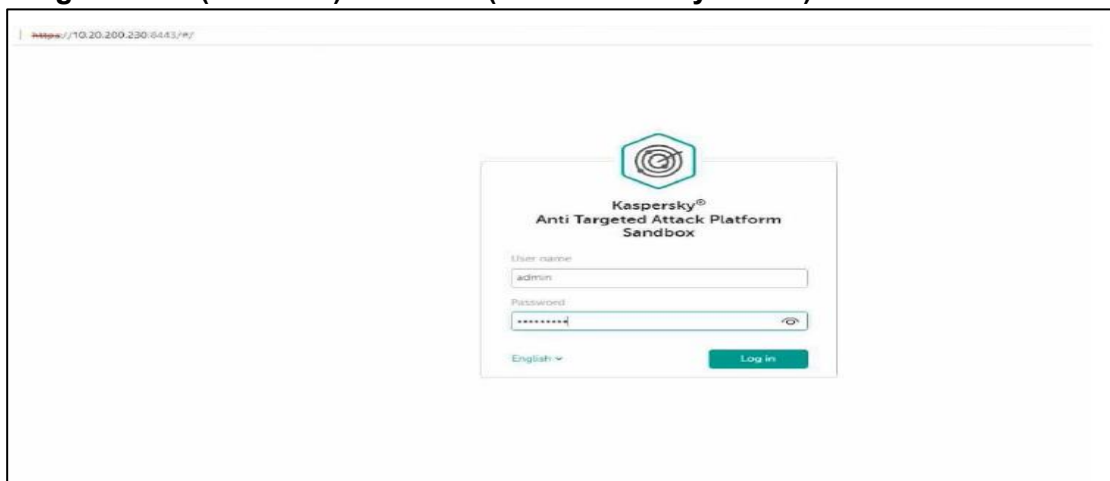


Ilustración 25 - Interfaz de Acceso a la plataforma KATA (SANDBOX)

Imagen KATA (Sandbox) – Dashboard

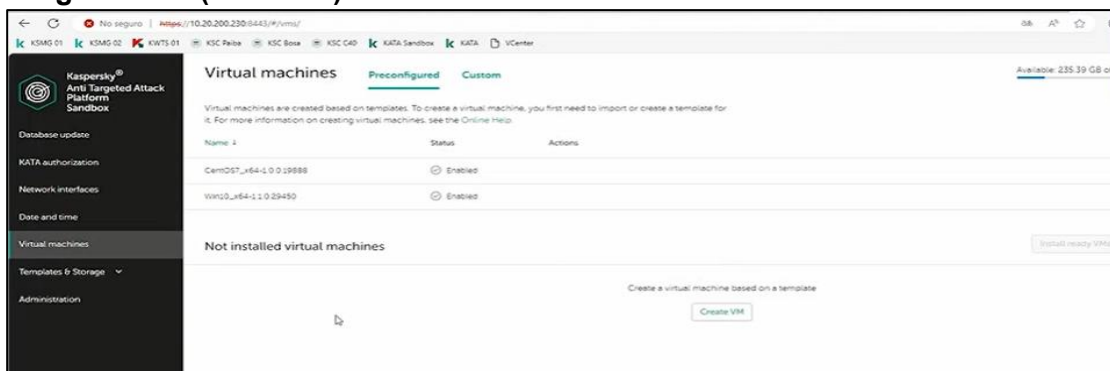


Ilustración 26 - Dashboard principal KATA (SANDBOX)

Imagen KATA (Sandbox) – Integración KATA

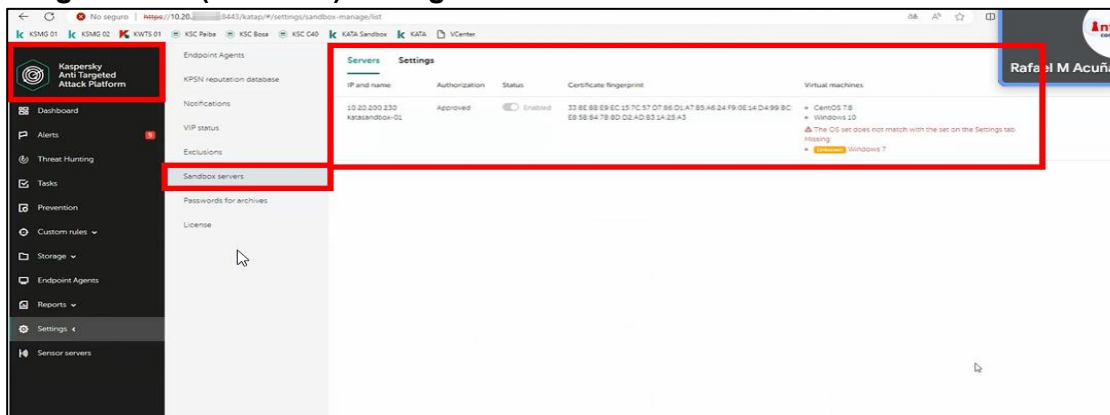


Ilustración 27 - Integración plataforma KATA(SANDBOX) con KATA

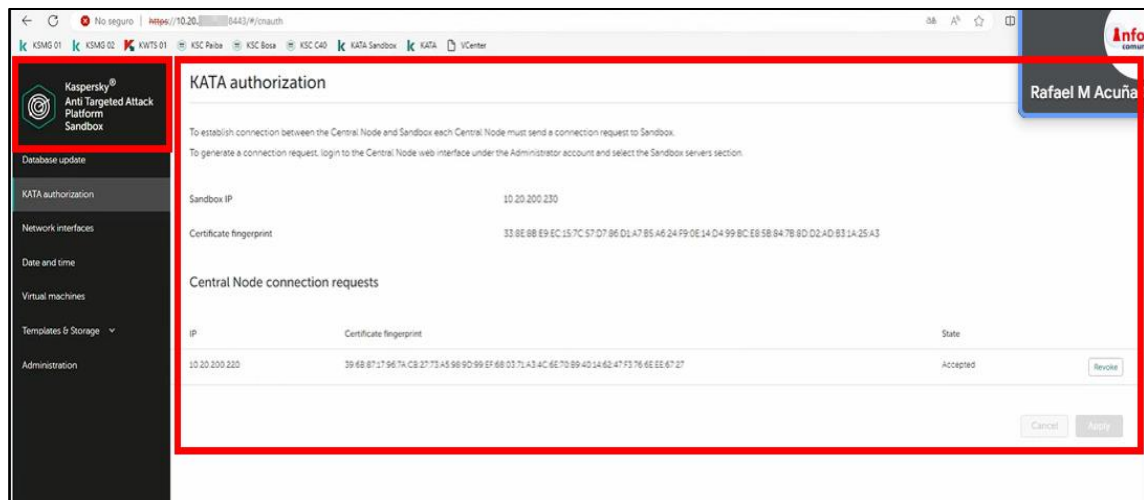


Ilustración 28 - Integración plataforma KATA(SENSOR) con KATA

Imagen KATA (Sandbox) – Actualización Bases de Datos

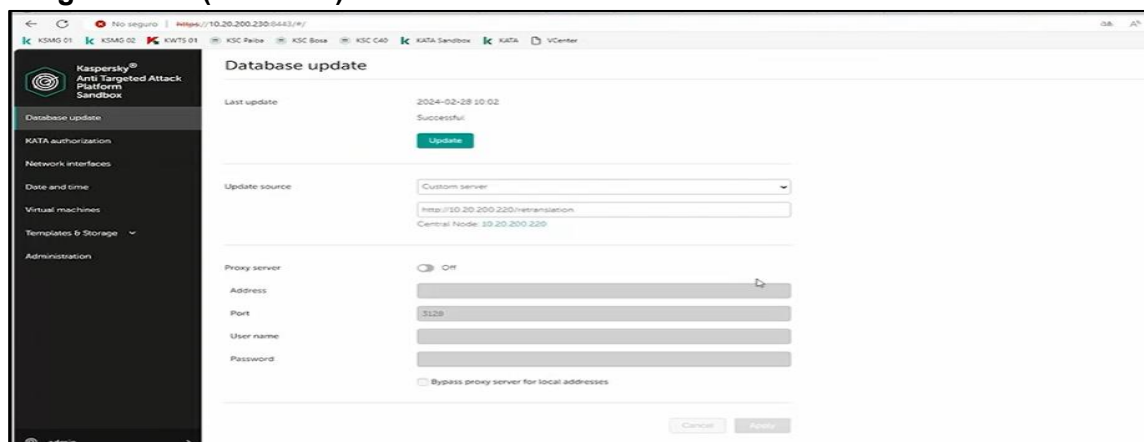


Ilustración 29 - Actualización bases de datos plataforma KATA(SANDBOX)

Imagen KATA (Sandbox) - Versión

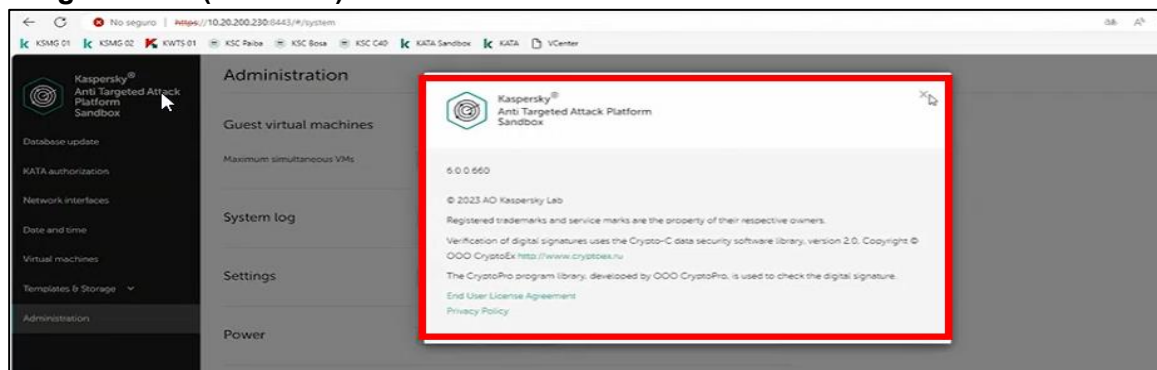


Ilustración 30 - Versión instalada actualizada de la plataforma KATA(SANDBOX)

8. Instalación y configuración Kaspersky Anti – Targeted Attack Platform (KATA) – EDR EXPERT.

Kaspersky Anti-targeted Attack Platform en adelante **KATA** es una solución de protección contra las amenazas que están presentes en el tráfico de red, está compuesta por un NODO CENTRAL que se encarga de realizar el análisis de toda la información recibida con su motor antimalware y que a su vez recibe información de plataformas adicionales como SENSORES de red, herramientas de seguridad como SANDBOX, KWTS, KSMG, Endpoints, de tal manera que al recibir y tratar dicha información con telemetría enriquecida podrá hacer frente a las amenazas y comportamientos maliciosos que se presenten en la red y en los equipos de la Universidad Distrital Francisco Jose de Caldas.

En las imágenes a continuación se puede observar el acceso a la plataforma y direcciones donde están alojados los servicios en este caso los agentes de EDR EXPERT de KATA, los cuales son desplegados y administrados desde cada consola de administración Kaspersky KSC y visualizados en la sección endpoints del nodo central en KATA más adelante en este informe se podrá visualizar la topología de red final y el flujo de tráfico.

PLATAFORMA	URL de Acceso	Acceso	Usuario
KSC-BOSA	https://10.60.24.2/en_US/#/	HTTP	Administrator
KSC-CALLE40	https://10.20.110.10/en_US/#/	HTTP	Administrator
KSC-PAIBA	https://10.40.42.2	HTTP	Administrator
KATA-CN	https://10.20.200.220/en_US/#/	HTTP	Plataformas

Tabla 8 Accesos a Consolas KCS Instaladas

Imagen KATA (EDR-Expert) – Acceso (10.20.200.220 / Administrator)

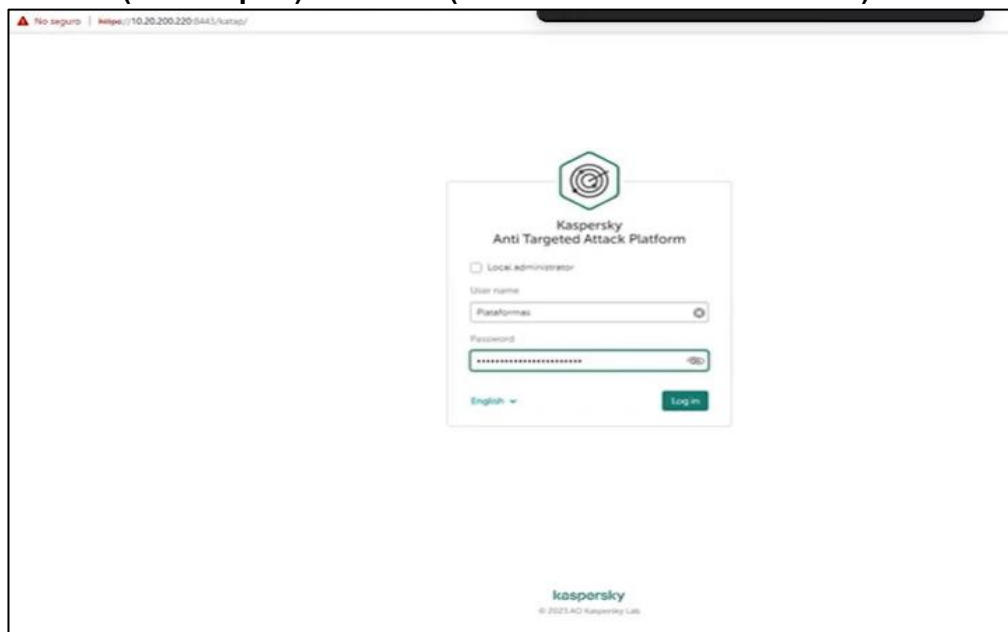


Ilustración 31 - Interfaz de Acceso a la plataforma KATA (EDR EXPERT)

Imagen KATA (EDR-Expert) – Dashboard

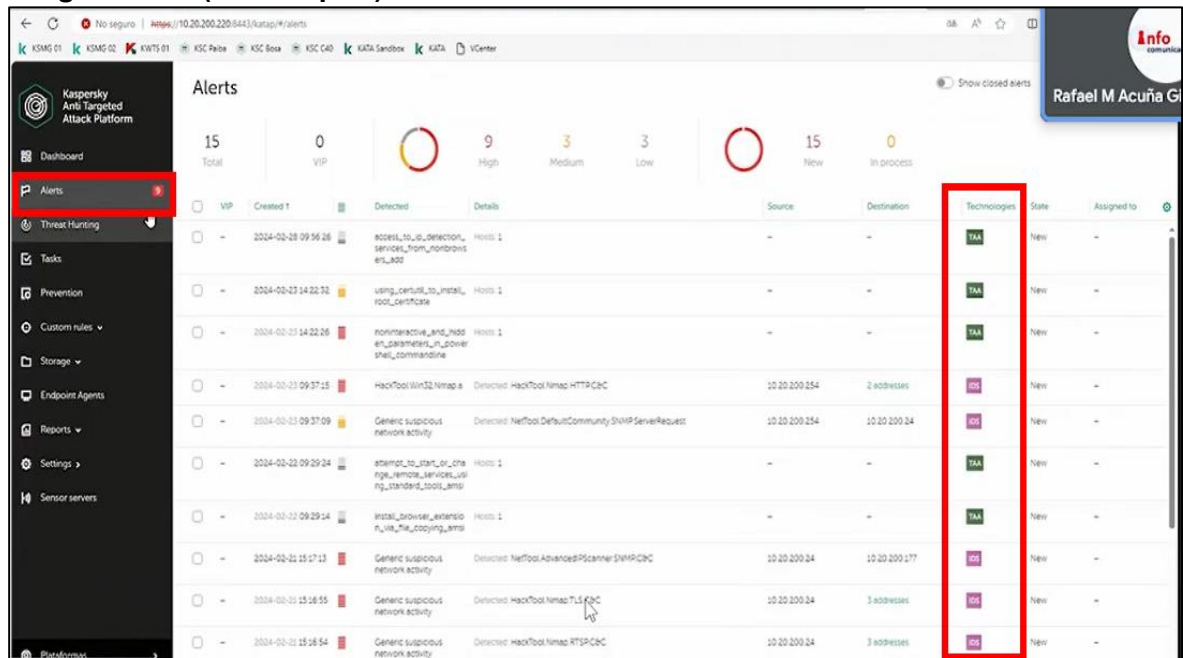


Ilustración 32 - Dashboard principal KATA (EDR EXPERT)

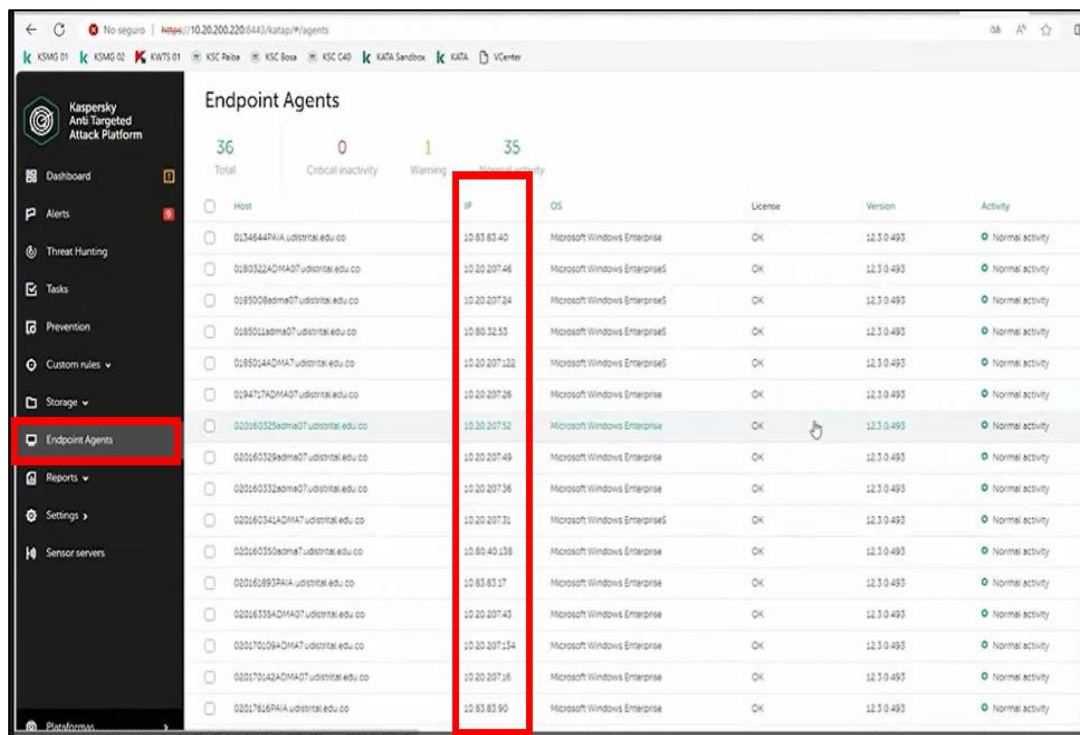


Ilustración 33 - Dashboard principal KATA (EDR EXPERT)

Imagen KATA (EDR-Expert) – Licenciamiento

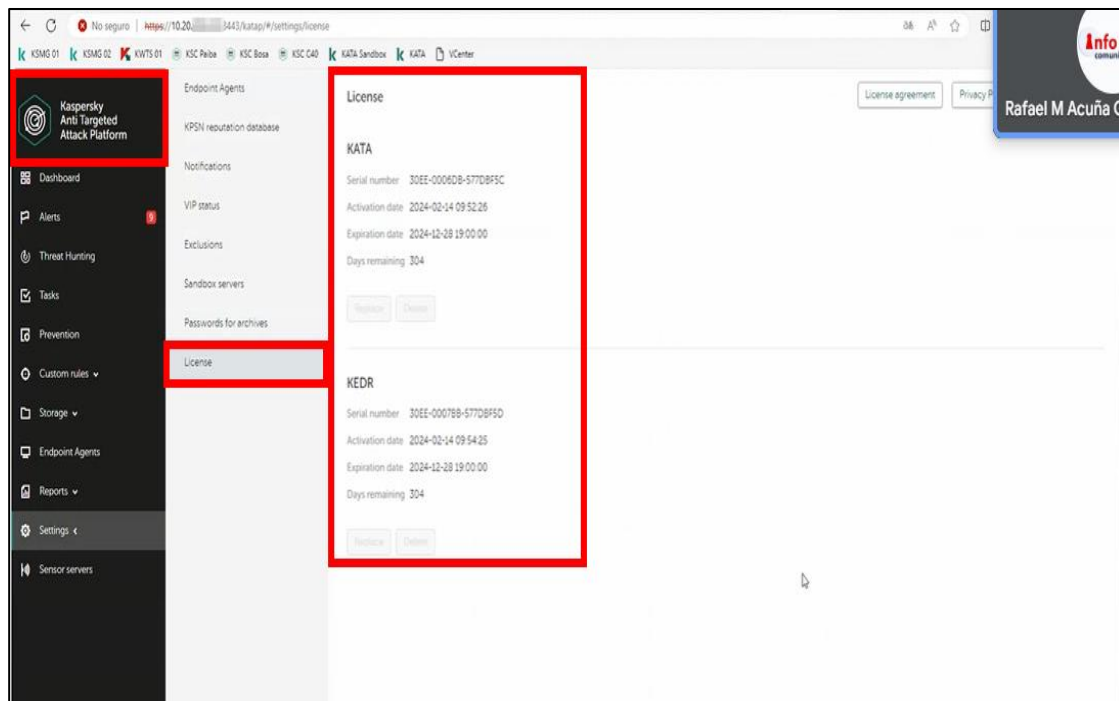


Ilustración 34 - Licenciamiento Plataforma KATA-CN Y EDR EXPERT

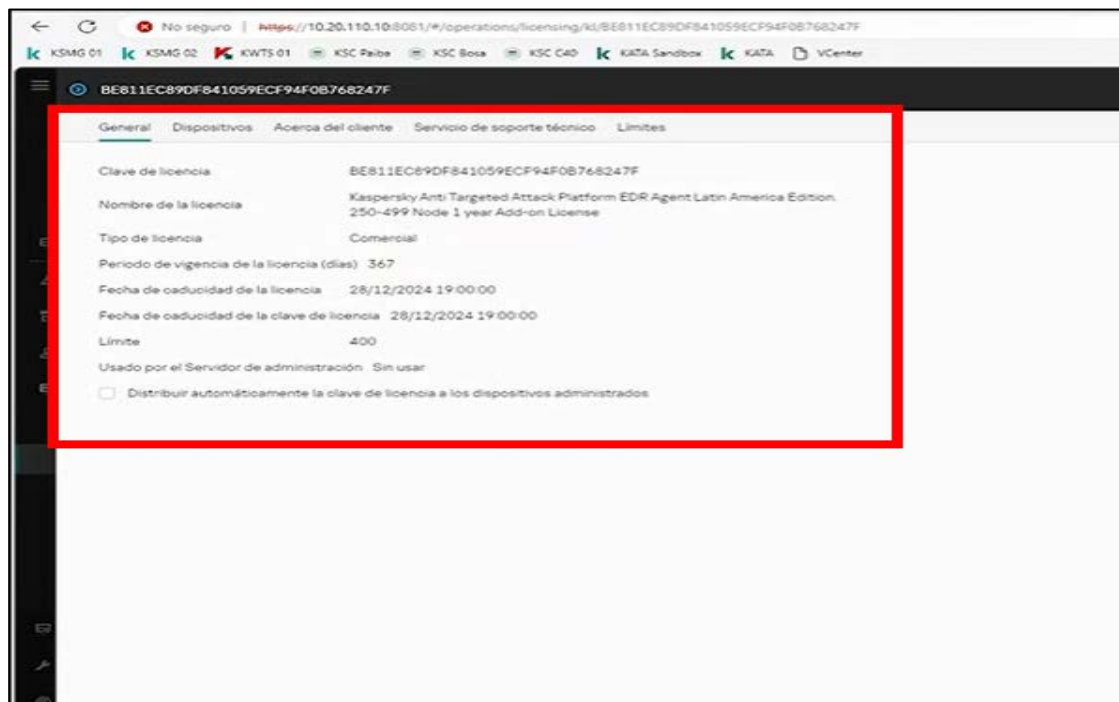


Ilustración 35 - Licenciamiento Plataforma KATA (EDR EXPERT)

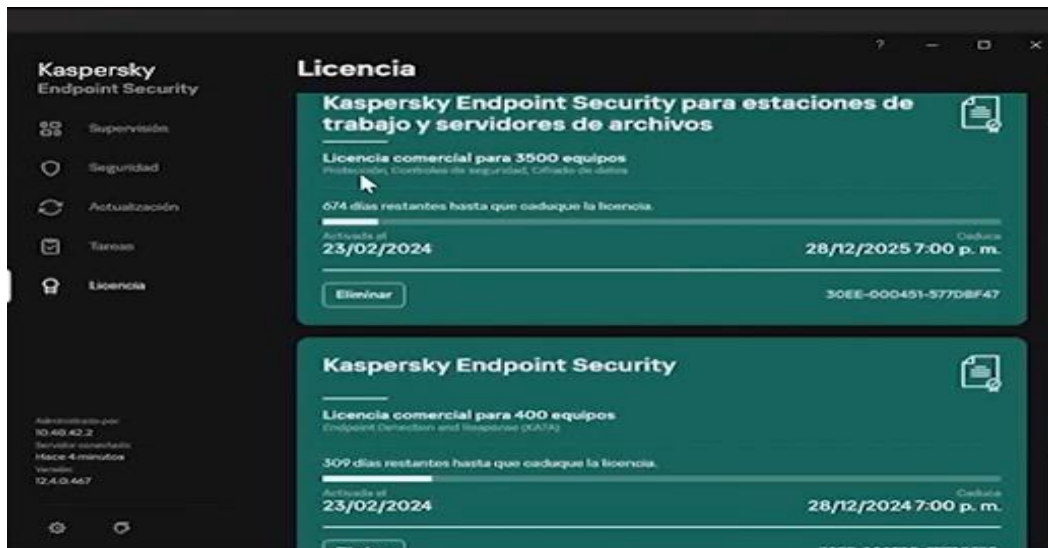


Ilustración 36 - Licenciamiento Plataforma KATA (EDR EXPERT) - Endpoint

Imagen KATA (EDR-Expert) – Integración KATA

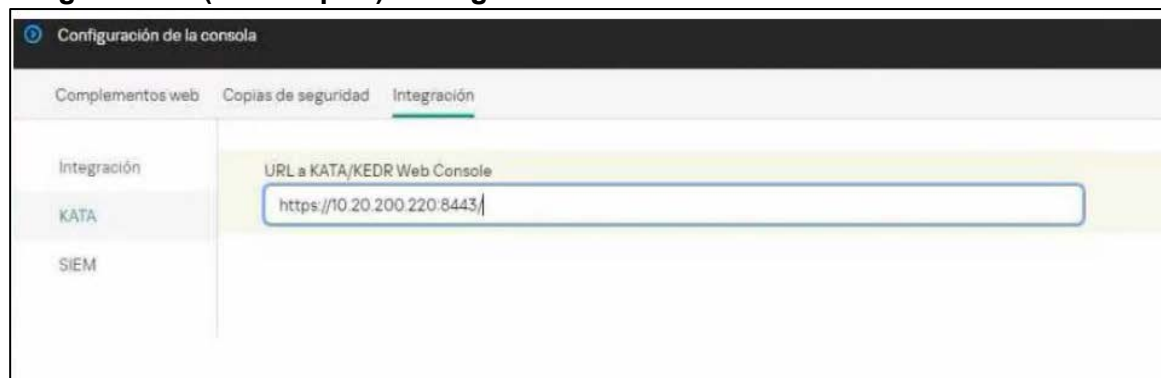


Ilustración 37 - Integración plataforma KATA(EDR EXPERT) con KATA

Imagen KATA (EDR-Expert) – Versión

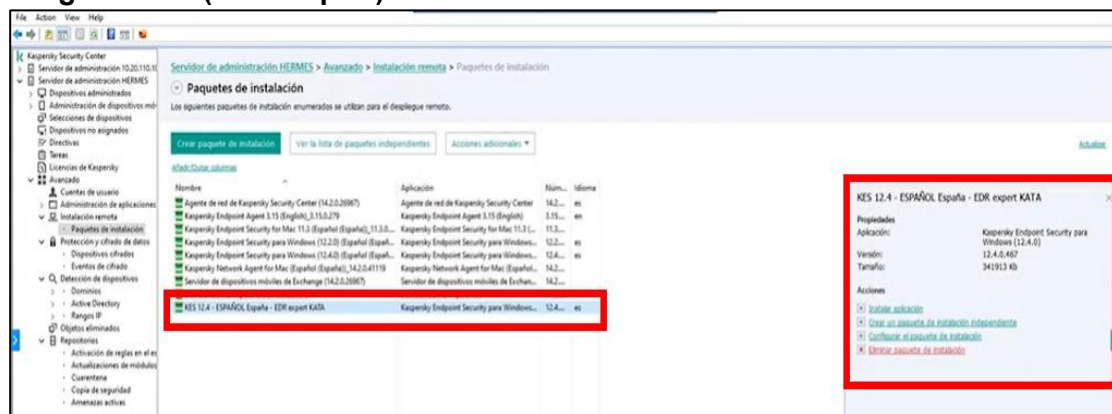


Ilustración 38 - Versión instalada actualizada de la plataforma KATA(EDR EXPERT) – Agente EDR

9. Diagrama de red (arquitectura actual) de instalación para los componentes de la solución para detección, prevención y respuesta de red (NDR) de ataques de red con la solución Kaspersky Anti-targeted Attack Platform KATA.

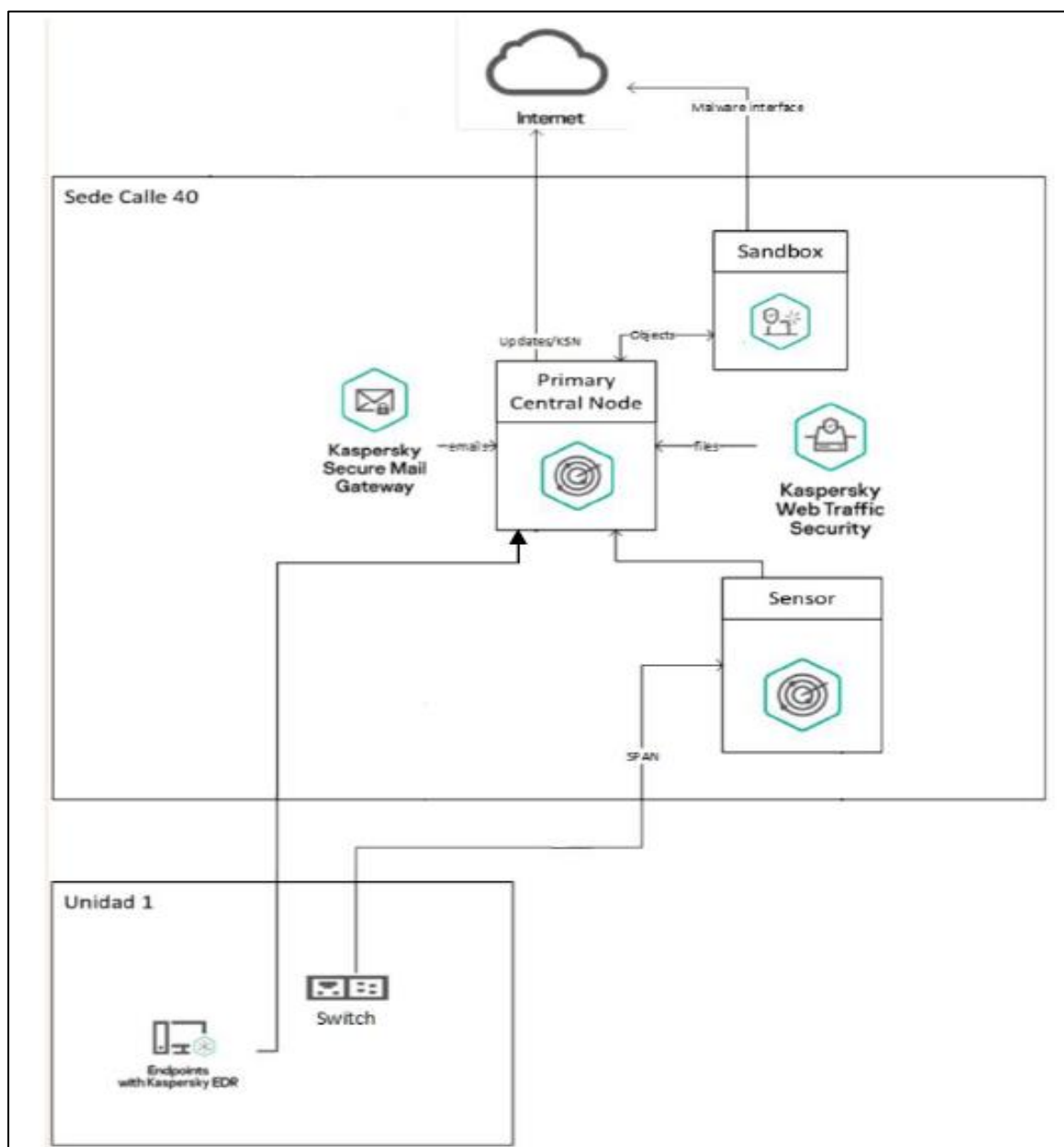


Ilustración 39 – Topología de red para todos los componentes de la plataforma KATA


10. Tareas Programadas y Ejecutadas.

- Descarga de instaladores para los componentes de protección que integran la solución KATA (KSMG – KWTS – KATA - SANDBOX).
- Revisión de requerimientos para instalación y despliegue de soluciones en el entorno de virtualización asignado por la universidad distrital francisco José de caldas
- Configuración de cada componente con base en su funcionamiento de protección genérica y principal.
- Integración de Soluciones instaladas vía API con el nodo Central de KATA (Ver imagen de Topología de la Solución)
- Creación y configuración de los paquetes de instalación Endpoint en los que se realiza la adición de componentes (EDR-EXPERTO) en cada una de las consolas Kaspersky que administran los equipos de la Universidad Distrital Francisco Jose de Caldas.
- Creación y despliegue de tareas de instalación de los componentes de protección con versiones actualizadas previamente en la creación de paquetes de instalación, labor realizada en cada consola de administración Kaspersky.
- Configuración de la conexión de los equipos con el componente de EDR-EXPERTO instalado para que reporten la información necesaria al nodo central de KATA.
- Se ha realizado transferencia de conocimiento en cada sesión a los participantes de la instalación y administración de la solución indicando las nuevas funcionalidades, así como el modo de operación y ejecución.
- Se realizaron dos sesiones de transferencia de conocimiento como preparación al curso de KATA Security Analyst estas sesiones se desarrollaron con una intensidad cada una de 2 horas y fueron impartidas por el líder de la instalación designado por Kaspersky.
- Se realizo también el entrenamiento especializado para el KATA Security Analyst en el cual participo el personal designado por la universidad distrital francisco José de

caldas, con una intensidad de 8 horas y entrega de certificado de asistencia al mismo.

- Se anexa a este informe de implementación los entregados por la fábrica Kaspersky ya que ellos se encargaron de la primera etapa de implementación de las soluciones de protección y detección de amenazas en la red, y que sirven de complemento con detalles de la instalación realizada, los nombres de los documentos se relacionan a continuación:
 - ✓ **Documentación_Implementación_KATA.pdf**
 - ✓ **Documentación_Implementación_KSMG.pdf**
 - ✓ **Documentación_Implementación_KWTS.pdf**
- Todos los componentes de la solución se entregaron instalados y en completo funcionamiento, comprobado en el envío y recepción de datos para el análisis de cada uno, así como la aprobación de los ingenieros encargados de la instalación por parte de la Universidad Distrital.

Elaboró.



Rafael Mariano Acuña Giraldo
Gerente de Soporte TI
Infocomunicaciones S.A.S

Revisó.



Juan Sebastian Gil Bolaños
Área de Plataformas Red de Datos UDNET
Universidad Distrital Francisco José de Caldas

SOFTWARE DE SEGURIDAD ANTIVIRUS.

Renovación y upgrade licenciamiento Kaspersky EDR Optimum y Kaspersky TOTAL Security para la Universidad Distrital Francisco José de Caldas.

06 DE MARZO DE 2024

INFOCOMUNICACIONES

Autopista Medellín Km 3.5 vía Siberia – TTCB – OFC C4 / C5



**RENOVACIÓN Y UPGRADE LICENCIAMIENTO KASPERSKY EDR OPTIMUM Y
KASPERSKY TOTAL SECURITY PARA LA UNIVERSIDAD DISTRITAL
FRANCISCO JOSE DE CALDAS.**

Informe de renovación y upgrade licenciamiento Kaspersky EDR Optimum y Kaspersky TOTAL Security para la universidad distrital Francisco Jose de Caldas.

El siguiente informe consigna las actividades que se llevaron a cabo desde el pasado 29 de diciembre de 2023 con el objetivo de dar alcance a la renovación y upgrade del licenciamiento adquirido por la universidad en lo que corresponde a Kaspersky EDR Optimum y Kaspersky TOTAL Security.

Información del Cliente	
Nombre de la Empresa	Universidad Distrital Francisco Jose de Caldas
Nombre del Contacto	Martha Cecilia Valdés Cruz – Líder Red de Datos UDNET
Correo Electronico	udnet@udistrital.edu.co
Teléfono de Contacto	6013239300 ext 1307



TABLA DE CONTENIDO.

1.	Objeto del Contrato.....	4
2.	Objetivo General	4
3.	Renovación y upgrade de licenciamiento Kaspersky EDR Optimum y Kaspersky TOTAL Security Consola Sede Calle 40.....	4
4.	Renovación y upgrade de licenciamiento Kaspersky EDR Optimum y Kaspersky TOTAL Security Consola Sede Bosa.....	8
5.	Renovación y upgrade de licenciamiento Kaspersky EDR Optimum y TOTAL Security Consola Sede Paiba.	11
6.	Tareas Programadas y Ejecutadas.	14

TABLA DE ILUSTRACIONES.

Ilustración 1	Licencia KEDRO instalada en la consola Hermes	5
Ilustración 2	Tarea despliegue licencia KEDRO en la consola HERMES.....	5
Ilustración 3	Licencia Kaspersky TOTAL instalada en la consola HERMES	6
Ilustración 4	Tarea despliegue licencia Kaspersky TOTAL en la consola HERMES	6
Ilustración 5	Licencia Kaspersky Hybrid Cloud instalada en la consola HERMES	7
Ilustración 6	Tarea de despliegue Licencia Kaspersky Hybrid Cloud en la consola HERMES	7
Ilustración 7	Licencia KEDRO instalada en la consola GOKU	8
Ilustración 8	Tarea de despliegue Licencia KEDRO en la consola GOKU	8
Ilustración 9	Licencia Kaspersky TOTAL instalada en la consola GOKU	9
Ilustración 10	Tarea de despliegue Licencia Kaspersky TOTAL en la consola GOKU	9

Ilustración 11 Licencia Kaspersky Hybrid Cloud – Server- instalada en la consola GOKU	10
Ilustración 12 Tarea de despliegue Licencia Kaspersky Hybrid Cloud Desktop- en la consola GOKU	10
Ilustración 13 Licencia KEDRO instalada en la consola CONSOLAKASAB.....	11
Ilustración 14 Tarea de despliegue Licencia KEDRO en la consola CONSOLAKASAB	11
Ilustración 15 Licencia Kaspersky TOTAL instalada en la consola CONSOLAKASAB .	12
Ilustración 16 Tarea de despliegue Licencia Kaspersky TOTAL en la consola CONSOLAKASAB.....	12
Ilustración 17 Licencia Kaspersky Hybrid Cloud Server- instalada en la consola CONSOLAKASAB.....	13
Ilustración 18 Tarea de despliegue Licencia Kaspersky Hybrid Cloud en la consola CONSOLAKASAB.....	13

1. Objeto del Contrato

Componente 2

Adquirir, instalar, configurar y puesta en correcto funcionamiento de una solución de seguridad antivirus para equipos servidores físicos y virtuales pc, portátiles y máquinas virtuales propiedad de la Universidad Distrital Francisco José de Caldas, incluyendo soporte técnico 7x24 y actualizaciones (update y upgrade)

2. Objetivo General

Realizar la renovación del licenciamiento de las soluciones Kaspersky para asegurar la protección correcta de los datos que hacen parte del parque informático de la Universidad Distrital Francisco José de Caldas, a continuación, se enumeran y describen las licencias adquiridas por la Universidad Distrital y que hace parte de este informe de renovación y upgrade de licenciamiento adquirido.

ITEM	Descripción de la Licencias	Cantidad
1	Licencias de Kaspersky Endpoint Detection and Response Optimum Add-on	2841
2	Licencias Kaspersky Total Security for Business	3500
3	Licencias Kaspersky Hybrid Cloud Security, Server	30
4	Licencias Kaspersky Hybrid Cloud Security, Desktop	200

3. Renovación y upgrade de licenciamiento Kaspersky EDR Optimum y Kaspersky TOTAL Security Consola Sede Calle 40.

En la sede de la Calle 40 mas exactamente en el servidor con Hostname **HERMES**, dirección IP Interna 10.x.x.x, se procedió a realizar la renovación de licenciamiento para la solución actualmente instalada que es Kaspersky Endpoint Security and Response OPTIMUM en adelante **KEDRO**, las imágenes a continuación evidencian la adición correcta de la licencia al contenedor de la consola de Kaspersky Security Center así como su fecha de vencimiento según periodo contratado y cantidad de dispositivos que puede proteger.

Servidor de administración HERMES > Licencias de Kaspersky

Licencias de Kaspersky
 Guardar los detalles de la licencia en el Servidor de administración, activar las aplicaciones de Kaspersky en dispositivos y ver informes sobre licencias de dispositivos.

[Añadir código de activación o archivo clave](#) [Distribuir automáticamente la clave de licencia a los dispositivos administrados](#) [Acciones adicionales](#) [Actualizar](#)

[Añadir/Quitar columnas](#)

Aplicación	Número	Límite	Periodo de vigencia de l...	Fecha de caducidad de l...	Cód...	Usa...
Kaspersky Endpoint D...	30EE-000879-577DBF58	2841	732	Sunday, December 28, 2...	Arch...	Sin u...
Kaspersky Endpoint D...	08D033F1F7A647DF88F...	3400	32	Sunday, October 12, 202...	Cód...	Sin u...
Kaspersky Endpoint D...	08D033F1F7A647DF88F...	3400	45	Thursday, September 14...	Cód...	Sin u...
Kaspersky Endpoint D...	66DD29DE40124728A80...	3400	9	Thursday, December 21...	Cód...	Sin u...
Kaspersky Endpoint D...	2A16-000451-577D195F	3400	9	Thursday, December 21...	Arch...	Sin u...
Kaspersky Endpoint D...	346C-000451-577C6DDE	3400	32	Monday, December 11...	Arch...	Sin u...
Kaspersky Endpoint D...	2A16-000879-577D1960	3400	9	Thursday, December 21...	Arch...	Sin u...
Kaspersky Endpoint D...	2A16-0003F9-577D195E	3400	9	Thursday, December 21...	Arch...	Sin u...
Kaspersky Endpoint S...	368BAE74C8CA4149BA9...	3400	1097	Friday, December 8, 202...	Cód...	Sin u...
Kaspersky Endpoint S...	2D5E-000451-5762437B	3400	1097	Friday, December 8, 202...	Arch...	Sin u...

30EE-000879-577DBF58

Propiedades

Aplicación: Kaspersky Endpoint Detection and Response Optimum Add-on Latin America Edition, 2500-4999 Node 2 year Add-on License

Tipo: Comercial

Periodo de vigencia de la licencia (días): 732

La clave de licencia caduca el: Sunday, December 28, 2025 7:00:00 PM

Fecha de caducidad de la licencia: Sunday, December 28, 2025 7:00:00 PM

Número máximo de dispositivos: 2841

Dispositivos que usan la clave como activa: 0

Dispositivos que usan la clave como de reserva: 0

Usado por el Servidor de administración: Sin usar

Acciones

[Exportar archivo clave](#)

[Ver propiedades de la clave de licencia](#)

[Eliminar clave de licencia](#)

Ilustración 1 Licencia KEDRO instalada en la consola Hermes

El Despliegue de esta licencia es automático por defecto sin embargo para forzar una aplicación más rápida del licenciamiento en los equipos se realizó la creación y ejecución de una tarea de despliegue de la licencia como se ve en la imagen a continuación.

Servidor de administración HERMES > Tareas

Tareas
[Nueva tarea](#) [Importar tarea desde archivo](#) [Actualizar](#)

[Añadir/Quitar columnas](#)

Nombre	Aplicación	Tipo de tarea	Estado	En ej...	Se co...	Fallo	Com...	Grupo
Actualizar								
Actualizar MAC	Kaspersky End...	Actualizar		0	0	0	0	Dispositivos adminis
Instalar actualización	Kaspersky End...	Actualizar	Fallo	0	0	33	0	Dispositivos adminis
Administrar dispositivos								
Reiniciar Equipos	Agente de red ...	Administrar dispositivos	Se completó c...	0	1	0	0	Tareas para dispositi
Análisis								
Análisis MAC	Kaspersky End...	Análisis		0	0	0	0	Dispositivos adminis
Análisis antimalware								
Análisis antimalware Windows	Kaspersky End...	Análisis antimalware	En pausa	43	87	3	0	Dispositivos adminis
Análisis de Antimalware	Kaspersky End...	Análisis antimalware	En ejecución (...)	1	10	0	0	Tareas para dispositi
Añadir clave								
Agregar clave EDR	Kaspersky End...	Añadir clave	Fallo	0	132	1	0	Tareas para dispositi
Añadir clave EDR 2025	Kaspersky End...	Añadir clave	En ejecución (...)	0	0	0	0	Tareas para dispositi
Buscar vulnerabilidades y actualizaciones requeridas								
Buscar vulnerabilidades y actualización...	Agente de red ...	Buscar vulnerabilidades ...	En ejecución (...)	8	139	2	0	Dispositivos adminis
Copia de seguridad de los datos del Servid...	Servidor de ad...	Copia de seguridad de l...	Se completó c...	0	1	0	0	Tareas para dispositi
Descargar actualizaciones en el repositorio del Servidor de administración	Servidor de ad...	Descargar actualización...	Se completó c...	0	1	0	0	Tareas para dispositi
Desconocido								
Activation of Application EDR	Desconocido	Desconocido		0	0	0	0	Tareas para dispositi

Añadir clave (EDR) 2025

Tipo de tarea: Añadir clave

Aplicación: Kaspersky Endpoint Security para Windows (12.2.0)

Grupo: Tareas para dispositivos específicos

Estadísticas de ejecución en dispositivos

Pendiente en 138 dispositivos

Programado en 13 dispositivos

[Ver resultados](#)

[Configurar tarea](#)

[Exportar tarea a archivo](#)

[Eliminar tarea](#)

[Detener](#)

Ilustración 2 Tarea despliegue licencia KEDRO en la consola HERMES

Se realiza adición de la licencia que corresponde a Kaspersky Total Security en el contenedor de licencias de la consola de Kaspersky Security Center para despliegue automático a los equipos administrados en esta.

Servidor de administración HERMES > Licencias de Kaspersky

Licencias de Kaspersky

Guardar los detalles de la licencia en el Servidor de administración, activar las aplicaciones de Kaspersky en dispositivos y ver informes sobre licencias de dispositivos.

[Añadir código de activación o archivo clave](#) [Distribuir automáticamente la clave de licencia a los dispositivos administrados](#) [Acciones adicionales](#) [Actualizar](#)

[Añadir/Quitar columnas](#)

Aplicación	Número	Límite	Periodo de vigencia de l...	Fecha de caducidad de l...	Códi...	Usad...
Kaspersky Endpoint D...	30EE-000879-577DBF58	2841	732	Sunday, December 28, 2...	Arch...	Sin u...
Kaspersky Endpoint D...	083D02C2CFC44032841...	3400	32	Sunday, October 15, 202...	Códi...	Sin u...
Kaspersky Endpoint D...	08DD3F1F7A647DFB8F...	3400	45	Thursday, September 14...	Códi...	Sin u...
Kaspersky Endpoint D...	66DD29E40124728A80...	3400	9	Thursday, December 21...	Códi...	Sin u...
Kaspersky Endpoint D...	2A16-000451-577D195F	3400	9	Thursday, December 21...	Arch...	Sin u...
Kaspersky Endpoint D...	345C-000451-577C6DDE	3400	32	Monday, December 11, ...	Arch...	Sin u...
Kaspersky Endpoint D...	2A16-000879-577D1960	3400	9	Thursday, December 21...	Arch...	Sin u...
Kaspersky Endpoint D...	2A16-0003F9-577D195E	3400	9	Thursday, December 21...	Arch...	Sin u...
Kaspersky Endpoint S...	368BAE74C8CA4149BA9...	3400	1097	Friday, December 8, 202...	Códi...	Sin u...
Kaspersky Endpoint S...	3D5E-000451-57634278	3400	1097	Friday, December 8, 202...	Arch...	Sin u...
Kaspersky Total Securi...	30EE-000451-577DBF47	3500	732	Sunday, December 28, 2...	Arch...	Sin u...

30EE-000451-577DBF47

Propiedades

Aplicación: Kaspersky Total Security for Business Latin America Edition, 2500-4999 Node 2 year Renewal License: Kaspersky Security for VS and FS

Tipo: Comercial

Periodo de vigencia de la licencia (días): 732

La clave de licencia caduca el: Sunday, December 28, 2025 7:00:00 PM

Fecha de caducidad de la licencia: Sunday, December 28, 2025 7:00:00 PM

Número máximo de dispositivos: 3500

Dispositivos que usan la clave como activa: 0

Dispositivos que usan la clave como de reserva: 0

Usado por el Servidor de administración: Sin usar

Acciones

[Exportar archivo clave](#)

[Ver propiedades de la clave de licencia](#)

[Eliminar clave de licencia](#)

Ilustración 3 Licencia Kaspersky TOTAL instalada en la consola HERMES

En paralelo se crea y ejecuta una segunda tarea la cual tiene como objetivo agregar el licenciamiento de Kaspersky TOTAL Security para la activación del componente de protección endpoint ya que como se mencionó la licencia anterior habilita las opciones de protección para el EDR.

Servidor de administración HERMES > Tareas

Tareas

[Nueva tarea](#) [Importar tarea desde archivo](#) [Actualizar](#)

[Añadir/Quitar columnas](#)

Nombre	Aplicación	Tipo de tarea	Estado	En ej...	Se co...	Fallo	Com...	Grupo
Actualizar								
Actualizar MAC	Kaspersky End...	Actualizar		0	0	0	0	Dispositivos adminis
Instalar actualización	Kaspersky End...	Actualizar	Fallo	0	0	33	0	Dispositivos adminis
Administrar dispositivos								
Reiniciar Equipos	Agente de red ...	Administrar dispositivos	Se completó c...	0	1	0	0	Tareas para dispositi
Análisis								
Análisis MAC	Kaspersky End...	Análisis		0	0	0	0	Dispositivos adminis
Análisis antimalware								
Análisis antimalware Windows	Kaspersky End...	Análisis antimalware	En pausa	43	87	3	0	Dispositivos adminis
Análisis de Antimalware	Kaspersky End...	Análisis antimalware	En ejecución (...)	1	10	0	0	Tareas para dispositi
Añadir clave								
Agregar clave EDR	Kaspersky End...	Añadir clave	Fallo	0	132	1	0	Tareas para dispositi
Añadir clave (EDR) 2025	Kaspersky End...	Añadir clave	Fallo	0	31	2	0	Tareas para dispositi
Añadir clave (EDR) 2025	Kaspersky End...	Añadir clave	Fallo	0	16	104	0	Tareas para dispositi
Añadir clave (Kaspersky Total) 2025	Kaspersky End...	Añadir clave		0	0	0	0	Tareas para dispositi
Buscar vulnerabilidades y actualizaciones requeridas								
Buscar vulnerabilidades y actualización...	Agente de red ...	Buscar vulnerabilidades ...	En ejecución (...)	8	139	2	0	Dispositivos adminis
Copia de seguridad de los datos del Servidor de administración								
Copia de seguridad de los datos del Servi...	Servidor de ad...	Copia de seguridad de l...	Se completó c...	0	1	0	0	Tareas para dispositi
Descargar actualizaciones en el repositorio del Servidor de administración								
Descargar actualizaciones en el repositor...	Servidor de ad...	Descargar actualización...	Se completó c...	0	1	0	0	Tareas para dispositi
Desconocido								

Añadir clave (Kaspersky Total) 2025

Tipo de tarea: Añadir clave

Aplicación: Kaspersky Endpoint Security para Windows (12.2.0)

Grupo: Tareas para dispositivos específicos

Estadísticas de ejecución en dispositivos

[Ver resultados](#)

[Iniciar](#)

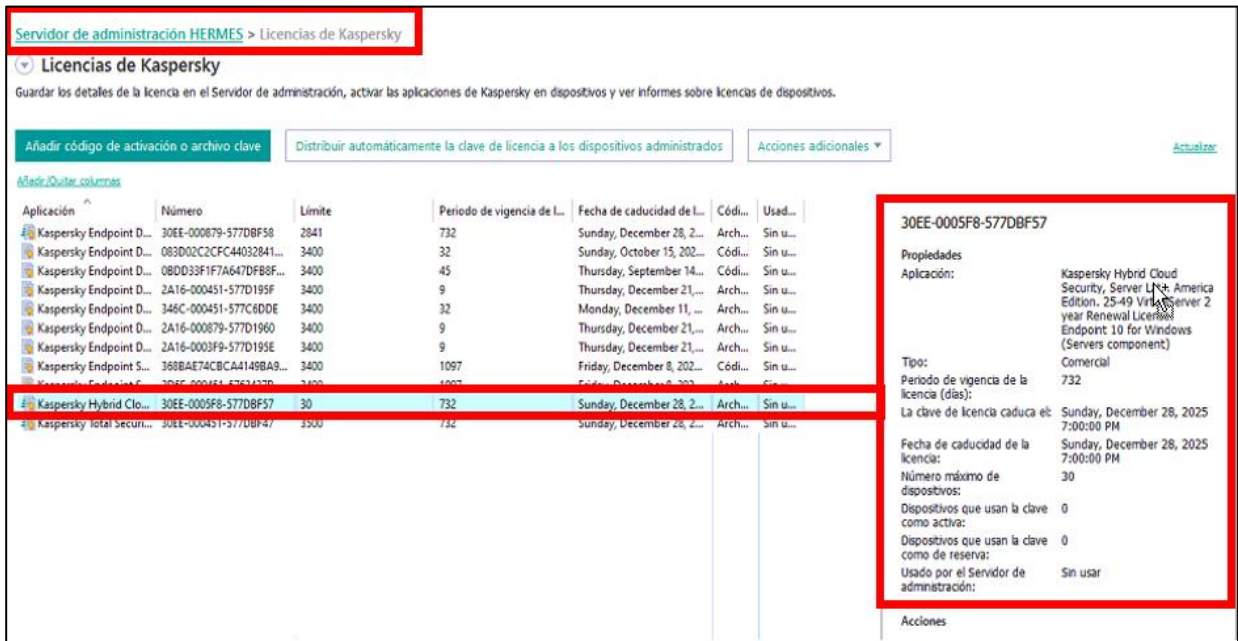
[Configurar tarea](#)

[Exportar tarea a archivo](#)

[Eliminar tarea](#)

Ilustración 4 Tarea despliegue licencia Kaspersky TOTAL en la consola HERMES

Se realiza adición de la licencia que corresponde a Kaspersky Hybrid Cloud Security Server en el contenedor de licencias de la consola de Kaspersky Security Center para despliegue automático a los equipos administrados en esta como se consigna en la evidencia.



Servidor de administración HERMES > Licencias de Kaspersky

Licencias de Kaspersky

Guardar los detalles de la licencia en el Servidor de administración, activar las aplicaciones de Kaspersky en dispositivos y ver informes sobre licencias de dispositivos.

Añadir código de activación o archivo clave Distribuir automáticamente la clave de licencia a los dispositivos administrados Acciones adicionales Actualizar

Añadir/Quitar columnas

Aplicación	Número	Límite	Periodo de vigencia de L...	Fecha de caducidad de L...	Códi...	Usad...
Kaspersky Endpoint D...	30EE-000879-577DBF58	2841	732	Sunday, December 28, 2...	Arch...	Sin u...
Kaspersky Endpoint D...	083D02C2CFC44032841...	3400	32	Sunday, October 15, 202...	Códi...	Sin u...
Kaspersky Endpoint D...	08DD33F1F7A647DFB8F...	3400	45	Thursday, September 14...	Códi...	Sin u...
Kaspersky Endpoint D...	2A16-000451-577D195F	3400	9	Thursday, December 21...	Arch...	Sin u...
Kaspersky Endpoint D...	346C-000451-577C6DDE	3400	32	Monday, December 11...	Arch...	Sin u...
Kaspersky Endpoint D...	2A16-000879-577D1960	3400	9	Thursday, December 21...	Arch...	Sin u...
Kaspersky Endpoint D...	2A16-0003F9-577D195E	3400	9	Thursday, December 21...	Arch...	Sin u...
Kaspersky Endpoint S...	368BAE74CBCA4149BA9...	3400	1097	Friday, December 8, 202...	Códi...	Sin u...
Kaspersky Endpoint S...	30EE-000879-577DBF57	3400	732	Sunday, December 28, 2...	Arch...	Sin u...
Kaspersky Hybrid Clo...	30EE-0005F8-577DBF57	30	732	Sunday, December 28, 2...	Arch...	Sin u...
Kaspersky Total Secur...	30EE-000451-577DBF47	3500	732	Sunday, December 28, 2...	Arch...	Sin u...

30EE-0005F8-577DBF57

Propiedades

Aplicación: Kaspersky Hybrid Cloud Security, Server L...

Tipo: Comercial

Periodo de vigencia de la licencia (días): 732

La clave de licencia caduca el: Sunday, December 28, 2025 7:00:00 PM

Fecha de caducidad de la licencia: Sunday, December 28, 2025 7:00:00 PM

Número máximo de dispositivos: 30

Dispositivos que usan la clave como activa: 0


Dispositivos que usan la clave como de reserva: 0

Usado por el Servidor de administración: Sin usar

Acciones

Ilustración 5 Licencia Kaspersky Hybrid Cloud instalada en la consola HERMES

se crea y ejecuta una segunda tarea la cual tiene como objetivo agregar el licenciamiento de Kaspersky Hybrid Cloud Security - Server para la activación del componente de protección endpoint en cada uno de los servidores con la solución instalada y administrada desde la consola de Kaspersky Security Center.



Servidor de administración HERMES > Tareas

Tareas

Nueva tarea Importar tarea desde archivo Actualizar

Añadir/Quitar columnas

Nombre	Aplicación	Tipo de tarea	Estado	En ej...	Se co...	Fallo	Com...	Grupo
Actualizar								
Actualizar MAC	Kaspersky End...	Actualizar	En ejecución (...)	0	0	0	0	Dispositivos adminis
Instalar actualización	Kaspersky End...	Actualizar		1	0	32	0	Dispositivos adminis
Reiniciar Equipos	Agente de red...	Administrar dispositivos	Se completó c...	0	1	0	0	Tareas para dispositi
Análisis								
Análisis MAC	Kaspersky End...	Análisis		0	0	0	0	Dispositivos adminis
Análisis antimalware								
Análisis antimalware Windows	Kaspersky End...	Análisis antimalware	En pausa	43	87	3	0	Dispositivos adminis
Análisis de Antimalware	Kaspersky End...	Análisis antimalware	En ejecución (...)	1	10	0	0	Tareas para dispositi
Añadir clave								
Agregar clave EDR	Kaspersky End...	Añadir clave	Fallo	0	132	1	0	Tareas para dispositi
Añadir clave (EDR) 2025	Kaspersky End...	Añadir clave	Fallo	0	31	3	0	Tareas para dispositi
Añadir clave (Kaspersky Total) 2025	Kaspersky End...	Añadir clave	Se completó c...	0	34	0	0	Tareas para dispositi
Añadir clave (Kaspersky Total) 2025	Kaspersky End...	Añadir clave	Fallo	0	10	104	0	Tareas para dispositi
Añadir clave (Hybrid Server) 2025	Kaspersky End...	Añadir clave		0	0	0	0	Tareas para dispositi

Añadir clave (Hybrid Server) 2025

Tipo de tarea: Añadir clave

Aplicación: Kaspersky Endpoint Security para Windows (12.2.0)

Grupo: Tareas para dispositivos específicos

Estadísticas de ejecución en dispositivos

Pendiente en 1 dispositivos

Ver resultados

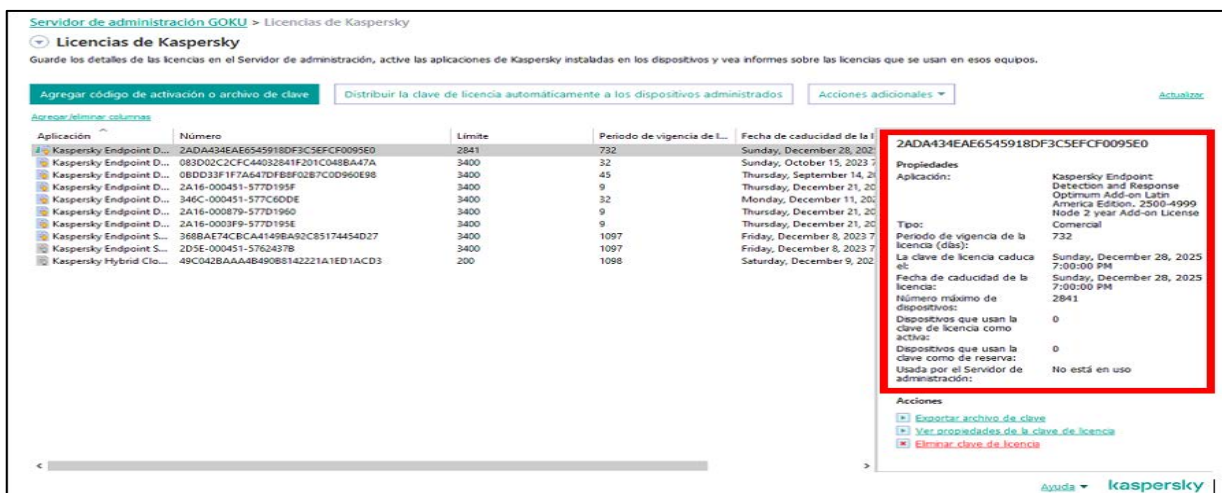
Iniciar

Configurar tarea

Ilustración 6 Tarea de despliegue Licencia Kaspersky Hybrid Cloud en la consola HERMES

4. Renovación y upgrade de licenciamiento Kaspersky EDR Optimum y Kaspersky TOTAL Security Consola Sede Bosa.

En la sede de Bosa más exactamente en el servidor con Hostname **GOKU**, dirección IP Interna 10.x.x.x, se procedió a realizar la renovación de licenciamiento para la solución actualmente instalada que es Kaspersky Endpoint Security and Response OPTIMUM en adelante **KEDRO**, las imágenes a continuación evidencian la adición correcta de la licencia al contenedor de la consola de Kaspersky Security Center así como su fecha de vencimiento según periodo contratado y cantidad de dispositivos que puede proteger.



Aplicación	Número	Límite	Periodo de vigencia de L...	Fecha de caducidad de la l...
Kaspersky Endpoint D...	2ADA434EAE6545918DF3C5EFCF0095E0	2841	732	Sunday, December 28, 2025
Kaspersky Endpoint D...	083D02C2FC44032841F201C048BA47A	3400	32	Sunday, October 15, 2023
Kaspersky Endpoint D...	08DD33F1F7A647DFB8F02B7C0D960E98	3400	45	Thursday, September 14, 2023
Kaspersky Endpoint D...	2A16-000451-577D195F	3400	9	Thursday, December 21, 2023
Kaspersky Endpoint D...	346C-000451-577C60DE	3400	32	Monday, December 11, 2023
Kaspersky Endpoint D...	2A16-000879-577D1950	3400	9	Thursday, December 21, 2023
Kaspersky Endpoint D...	2A16-0003F9-577D195E	3400	9	Thursday, December 21, 2023
Kaspersky Endpoint S...	368BAE74C6CA4149BA92C85174454D27	3400	1097	Friday, December 8, 2023
Kaspersky Endpoint S...	205E-000451-576D437B	3400	1097	Friday, December 8, 2023
Kaspersky Hybrid Cl...	49C042BAAA4B490B5142221A1ED1ACD3	200	1098	Saturday, December 9, 2023

2ADA434EAE6545918DF3C5EFCF0095E0

Propiedades:

Aplicación: Kaspersky Endpoint Security and Response Optimum Add-on Latin America Edition. 2500-4999

Tipo: Node 2 year Add-on License Comercial

Periodo de vigencia de la licencia (días): 732

La clave de licencia caduca el: Sunday, December 28, 2025 7:00:00 PM

Fecha de caducidad de la licencia: Sunday, December 28, 2025 7:00:00 PM

Número máximo de dispositivos: 2841

Dispositivos que usan la clave de licencia como activa: 0

Dispositivos que usan la clave como de reserva: 0

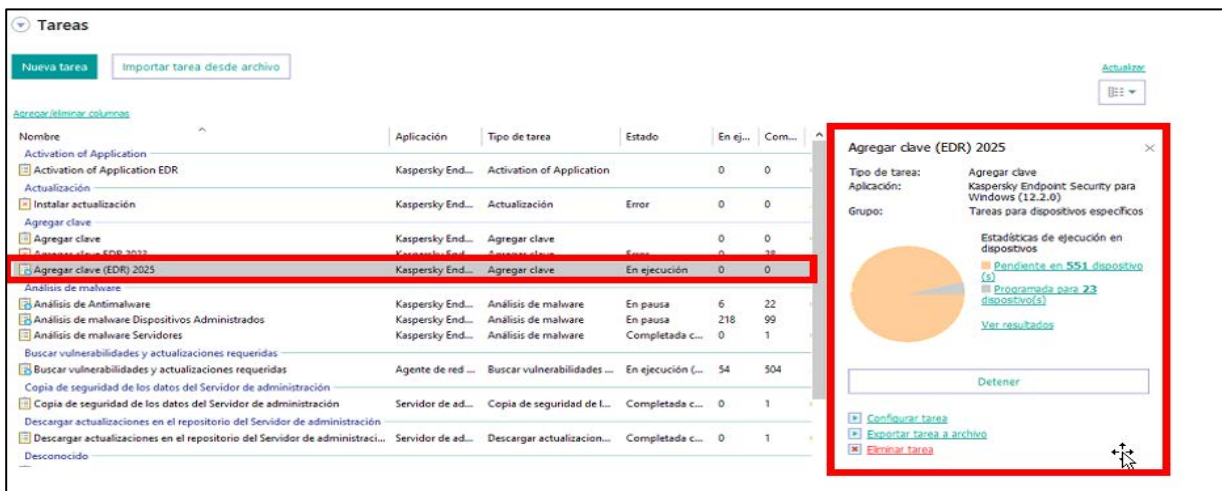
Usada por el Servidor de administración: No está en uso

Acciones:

- Exportar archivo de clave
- Ver propiedades de la clave de licencia
- Eliminar clave de licencia

Ilustración 7 Licencia KEDRO instalada en la consola GOKU

El Despliegue de esta licencia es automático por defecto sin embargo para forzar una aplicación más rápida del licenciamiento en los equipos se realizó la creación y ejecución de una tarea de despliegue de la licencia como se ve en la imagen a continuación.



Nombre	Aplicación	Tipo de tarea	Estado	En ej...	Com...
Activation of Application	Kaspersky End...	Activation of Application	En ejecución	0	0
Actualización	Kaspersky End...	Actualización	Error	0	0
Instalar actualización	Kaspersky End...	Instalar actualización	Error	0	0
Agregar clave	Kaspersky End...	Agregar clave	Error	0	0
Agregar clave EDR 2025	Kaspersky End...	Agregar clave	En ejecución	0	0
Agregar clave (EDR) 2025	Kaspersky End...	Agregar clave	En ejecución	0	0
Análisis de malware	Kaspersky End...	Análisis de malware	En pausa	6	22
Análisis de Antimalware	Kaspersky End...	Análisis de malware	En pausa	218	99
Análisis de malware Dispositivos Administrados	Kaspersky End...	Análisis de malware	Completada c...	0	1
Buscar vulnerabilidades y actualizaciones requeridas	Agente de red	Buscar vulnerabilidades...	En ejecución (...)	54	504
Copia de seguridad de los datos del Servidor de administración	Servidor de ad...	Copia de seguridad de L...	Completada c...	0	1
Descargar actualizaciones en el repositorio del Servidor de administración	Servidor de ad...	Descargar actualización...	Completada c...	0	1
Desconocido					

Agregar clave (EDR) 2025

Tipo de tarea: Agregar clave

Aplicación: Kaspersky Endpoint Security para Windows (12.2.0)

Grupo: Tareas para dispositivos específicos

Estadísticas de ejecución en dispositivos:

- Pendiente en 551 dispositivo(s)
- Programada para 23 dispositivo(s)

Ver resultados

Detener

Configurar tarea

Exportar tarea a archivo

Eliminar tarea

Ilustración 8 Tarea de despliegue Licencia KEDRO en la consola GOKU

Se realiza adición de la licencia que corresponde a Kaspersky Total Security en el contenedor de licencias de la consola de Kaspersky Security Center para despliegue automático a los equipos administrados en esta.

Servidor de administración GOKU > Licencias de Kaspersky

Licencias de Kaspersky

Guarda los detalles de las licencias en el Servidor de administración, active las aplicaciones de Kaspersky instaladas en los dispositivos y vea informes sobre las licencias que se usan en esos equipos.

Agregar código de activación o archivo de clave Distribuir la clave de licencia automáticamente a los dispositivos administrados Acciones adicionales Actualizar

Agregar/eliminar columnas

Aplicación	Número	Límite	Periodo de vigencia de l...	Fecha de caducidad de la
Kaspersky Endpoint D...	ZADA434EAE654918DF3C5EFCF0095E0	2841	732	Sunday, December 28, 2025
Kaspersky Endpoint D...	083D02C2CFC44032841F201C048BA47A	3400	32	Sunday, October 15, 2023
Kaspersky Endpoint D...	08DD33F1F7A647DFB8F02B7C0D960E98	3400	45	Thursday, September 14, 2023
Kaspersky Endpoint D...	2A16-000451-577D195F	3400	9	Thursday, December 21, 2023
Kaspersky Endpoint D...	346C-000451-577C60DE	3400	32	Monday, December 11, 2023
Kaspersky Endpoint D...	2A16-000379-577D1950	3400	9	Thursday, December 21, 2023
Kaspersky Endpoint D...	2A16-000379-577D1950	3400	9	Thursday, December 21, 2023
Kaspersky Endpoint S...	368BAE74C8CA4149BA92C85174454D27	3400	1097	Friday, December 8, 2023
Kaspersky Endpoint S...	2D5E-000451-5762437B	3400	1097	Friday, December 8, 2023
Kaspersky Endpoint S...	49C428A6A3D45095547233A3E7D1ACD1	3400	1097	Saturday, December 9, 2023
Kaspersky Total Security...	BE2B772DF02C47C1B25B8917208F5EDB	3850	732	Sunday, December 28, 2025

BE2B772DF02C47C1B25B8917208F5EDB

Propiedades:

Aplicación: Kaspersky Total Security for Business Latin America Edition, 2500-4999 Node 2 year Renewal License

Tipo: Comercial

Periodo de vigencia de la licencia (días): 732

La clave de licencia caduca el: Sunday, December 28, 2025 7:00:00 PM

Fecha de caducidad de la licencia: Sunday, December 28, 2025 7:00:00 PM

Número máximo de dispositivos: 3850

Dispositivos que usan la clave de licencia como activa: 0

Dispositivos que usan la clave como de reserva: 0

Usada por el Servidor de administración: No está en uso

Acciones:

- Exportar archivo de clave
- Ver propiedades de la clave de licencia
- Eliminar clave de licencia

Ilustración 9 Licencia Kaspersky TOTAL instalada en la consola GOKU

En paralelo se crea y ejecuta una segunda tarea la cual tiene como objetivo agregar el licenciamiento de Kaspersky TOTAL Security para la activación del componente de protección endpoint ya que como se mencionó la licencia anterior habilita las opciones de protección para el EDR.

Tareas

Nueva tarea Importar tarea desde archivo Actualizar

Agregar/eliminar columnas

Nombre	Aplicación	Tipo de tarea	Estado	En ej...	Com...
Activation of Application	Kaspersky End...	Activation of Application	En ejecución	0	0
Actualización	Kaspersky End...	Actualización	Error	0	0
Instalar actualización	Kaspersky End...	Instalar actualización	Error	0	0
Agregar clave	Kaspersky End...	Agregar clave	En ejecución	0	0
Agregar clave (EDR) 2025	Kaspersky End...	Agregar clave	En ejecución	19	3
Agregar clave (EDR) 2025	Kaspersky End...	Agregar clave	En ejecución	0	0
Agregar clave (Kaspersky Total) 2025	Kaspersky End...	Agregar clave	En ejecución	0	0
Análisis de malware	Kaspersky End...	Análisis de malware	En pausa	6	22
Análisis de Antimalware	Kaspersky End...	Análisis de malware	En pausa	219	99
Análisis de malware Dispositivos Administrados	Kaspersky End...	Análisis de malware	Completada c...	0	1
Buscar vulnerabilidades y actualizaciones requeridas	Agente de red ...	Buscar vulnerabilidades ...	En ejecución (...)	54	504
Copia de seguridad de los datos del Servidor de administración	Servidor de ad...	Copia de seguridad de l...	Completada c...	0	1
Descargar actualizaciones en el repositorio del Servidor de administración	Servidor de ad...	Descargar actualización...	Completada c...	0	1
Desconocido	Desconocido	Desconocido	Desconocido	0	0
Critical Areas Scan	Desconocido	Desconocido	Desconocido	0	0
Malware Scan	Desconocido	Desconocido	Desconocido	0	0
System Integrity Check	Desconocido	Desconocido	Desconocido	0	0

Agregar clave (Kaspersky Total) 2025

Tipo de tarea: Agregar clave

Aplicación: Kaspersky Endpoint Security para Windows (12.2.0)

Grupo: Tareas para dispositivos específicos

Estadísticas de ejecución en dispositivos:

- Pendiente en 552 dispositivo(s)
- Programada para 22 dispositivo(s)

Ver resultados

Detener

Configurar tarea Exportar tarea a archivo Eliminar tarea

ayuda kaspersky

Ilustración 10 Tarea de despliegue Licencia Kaspersky TOTAL en la consola GOKU

Se realiza adición de la licencia que corresponde a Kaspersky Hybrid Cloud Security Server en el contenedor de licencias de la consola de Kaspersky Security Center para despliegue automático a los equipos administrados en esta como se consigna en la evidencia

Servidor de administración GOKU > Licencias de Kaspersky

Licencias de Kaspersky

Guarde los detalles de las licencias en el Servidor de administración, active las aplicaciones de Kaspersky instaladas en los dispositivos y vea informes sobre las licencias que se usan en esos equipos.

Agregar código de activación o archivo de clave Distribuir la clave de licencia automáticamente a los dispositivos administrados Acciones adicionales Actualizar

Agregar/eliminar columnas

Aplicación	Número	Límite	Período de vig...	Fecha de caducidad de la licen...
Kaspersky Anti Targeted Attack Platform EDR Agent Latin America Edition, 250-499 Node 1 year Add-on License	30EE-00078B-577DBF5D	400	367	Saturday, December 28, 2024 7:00
Kaspersky Endpoint Detection and Response Optimum Add-on Latin America Edition, 2500-4999 Node 2 year Add-on Li...	2AD4A434AE6545918DF3C5...	2841	732	Sunday, December 28, 2025 7:00
Kaspersky Endpoint Detection and Response Optimum Add-on Latin America Edition, 2500-4999 Node 2 year Add-on Li...	30EE-000879-577DBF59	2841	732	Sunday, December 28, 2025 7:00
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1 year NFR License	083D02C2FC4403284F201...	3400	32	Sunday, October 13, 2023 12:51
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1 year NFR License	08D033F1F7A647DF8BF028...	3400	45	Thursday, September 14, 2023 11
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1 year NFR License: Kasp...	2A16-000451-577D195F	3400	9	Thursday, December 21, 2023 7:1
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1 year NFR License: Kasp...	346C-000451-577C6D0E	3400	32	Monday, December 11, 2023 7:0
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1 year NFR License: KE A...	2A16-000879-577D1960	3400	9	Thursday, December 21, 2023 7:1
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1 year NFR License: Secu...	2A16-0003F9-577D195E	3400	9	Thursday, December 21, 2023 7:1
Kaspersky Endpoint Security for Business - Select Latin America Edition, 2500-4999 Node 3 year Educational Renewal Lic...	368BAE74C8CA4149BA92C8...	3400	1097	Friday, December 8, 2023 7:00:00
Kaspersky Endpoint Security for Business - Select Latin America Edition, 2500-4999 Node 3 year Educational Renewal Lic...	2D5E-000451-5762437B	3400	1097	Friday, December 8, 2023 7:00:00
Kaspersky Hybrid Cloud Security, Desktop Latin America Edition, 150-249 VirtualWorkstation 2 year Renewal License: KSV	30EE-0005D3-577DBF5A	200	732	Sunday, December 28, 2025 7:00
Kaspersky Hybrid Cloud Security, Desktop Latin America Edition, 150-249 VirtualWorkstation 2 year Educational Renewal...	8FC042BAA4A8490814222...	200	1098	Saturday, December 9, 2023 7:00
Kaspersky Hybrid Cloud Security, Server Latin America Edition, 25-49 VirtualServer 2 year Renewal License: KSV	30EE-0005D3-577DBF56	30	732	Sunday, December 28, 2025 7:00
Kaspersky Total Security for Business Latin America Edition, 2500-4999 Node 2 year Renewal License	8E2B772D02C47C1B258B9...	3550	732	Sunday, December 28, 2025 7:00
Kaspersky Total Security for Business Latin America Edition, 2500-4999 Node 2 year Renewal License: Kaspersky Security ...	30EE-000451-577DBF47	3500	732	Sunday, December 28, 2025 7:00

30EE-0005D3-577DBF56

Propiedades

Aplicación: Kaspersky Hybrid Cloud Security, Server Latin America Edition, 25-49 VirtualServer 2 year Renewal License: KSV

Tipo: Comercial

Período de vigencia de la licencia (días): 732

La clave de licencia caduca el: Sunday, December 28, 2025 7:00:00 PM

Fecha de caducidad de la licencia: Sunday, December 28, 2025 7:00:00 PM

Número máximo de dispositivos: 30

Dispositivos que usan la clave de licencia como activa: 2

Dispositivos que usan la clave como de reserva: 0

Usada por el Servidor de administración: No está en uso

Acciones

- Exportar archivo de clave
- Ver propiedades de la clave de licencia
- Eliminar clave de licencia

Ilustración 11 Licencia Kaspersky Hybrid Cloud – Server- instalada en la consola GOKU

Se realiza adición de la licencia que corresponde a Kaspersky Hybrid Cloud Security Server en el contenedor de licencias de la consola de Kaspersky Security Center para despliegue automático a los equipos administrados en esta como se consigna en la evidencia

Servidor de administración GOKU > Licencias de Kaspersky

Licencias de Kaspersky

Guarde los detalles de las licencias en el Servidor de administración, active las aplicaciones de Kaspersky instaladas en los dispositivos y vea informes sobre las licencias que se usan en esos equipos.

Agregar código de activación o archivo de clave Distribuir la clave de licencia automáticamente a los dispositivos administrados Acciones adicionales Actualizar

Agregar/eliminar columnas

Aplicación	Número	Límite	Período de vig...	Fecha de caducidad de la licen...
Kaspersky Anti Targeted Attack Platform EDR Agent Latin America Edition, 250-499 Node 1 year Add-on License	30EE-00078B-577DBF5D	400	367	Saturday, December 28, 2024 7:00
Kaspersky Endpoint Detection and Response Optimum Add-on Latin America Edition, 2500-4999 Node 2 year Add-on Li...	2AD4A434AE6545918DF3C5...	2841	732	Sunday, December 28, 2025 7:00
Kaspersky Endpoint Detection and Response Optimum Add-on Latin America Edition, 2500-4999 Node 2 year Add-on Li...	30EE-000879-577DBF59	2841	732	Sunday, December 28, 2025 7:00
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1 year NFR License	083D02C2FC4403284F201...	3400	32	Sunday, October 13, 2023 12:51
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1 year NFR License	08D033F1F7A647DF8BF028...	3400	45	Thursday, September 14, 2023 11
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1 year NFR License: Kasp...	2A16-000451-577D195F	3400	9	Thursday, December 21, 2023 7:1
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1 year NFR License: Kasp...	346C-000451-577C6D0E	3400	32	Monday, December 11, 2023 7:0
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1 year NFR License: KE A...	2A16-000879-577D1960	3400	9	Thursday, December 21, 2023 7:1
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1 year NFR License: Secu...	2A16-0003F9-577D195E	3400	9	Thursday, December 21, 2023 7:1
Kaspersky Endpoint Security for Business - Select Latin America Edition, 2500-4999 Node 3 year Educational Renewal Lic...	368BAE74C8CA4149BA92C8...	3400	1097	Friday, December 8, 2023 7:00:00
Kaspersky Endpoint Security for Business - Select Latin America Edition, 2500-4999 Node 3 year Educational Renewal Lic...	2D5E-000451-5762437B	3400	1097	Friday, December 8, 2023 7:00:00
Kaspersky Hybrid Cloud Security, Desktop Latin America Edition, 150-249 VirtualWorkstation 2 year Renewal License: KSV	30EE-0005D3-577DBF5A	200	732	Sunday, December 28, 2025 7:00
Kaspersky Hybrid Cloud Security, Desktop Latin America Edition, 150-249 VirtualWorkstation 2 year Educational Renewal...	8FC042BAA4A8490814222...	200	1098	Saturday, December 9, 2023 7:00
Kaspersky Hybrid Cloud Security, Server Latin America Edition, 25-49 VirtualServer 2 year Renewal License: KSV	30EE-0005D3-577DBF56	30	732	Sunday, December 28, 2025 7:00
Kaspersky Total Security for Business Latin America Edition, 2500-4999 Node 2 year Renewal License	8E2B772D02C47C1B258B9...	3550	732	Sunday, December 28, 2025 7:00
Kaspersky Total Security for Business Latin America Edition, 2500-4999 Node 2 year Renewal License: Kaspersky Security ...	30EE-000451-577DBF47	3500	732	Sunday, December 28, 2025 7:00

30EE-0005D3-577DBF5A

Propiedades

Aplicación: Kaspersky Hybrid Cloud Security, Desktop Latin America Edition, 150-249 VirtualWorkstation 2 year Renewal License: KSV

Tipo: Comercial

Período de vigencia de la licencia (días): 732

La clave de licencia caduca el: Sunday, December 28, 2025 7:00:00 PM

Fecha de caducidad de la licencia: Sunday, December 28, 2025 7:00:00 PM

Número máximo de dispositivos: 200

Dispositivos que usan la clave de licencia como activa: 0

Dispositivos que usan la clave como de reserva: 0

Usada por el Servidor de administración: No está en uso

Acciones

- Exportar archivo de clave
- Ver propiedades de la clave de licencia
- Eliminar clave de licencia

Ilustración 12 Tarea de despliegue Licencia Kaspersky Hybrid Cloud Desktop- en la consola GOKU

5. Renovación y upgrade de licenciamiento Kaspersky EDR Optimum y TOTAL Security Consola Sede Paiba.

En la sede de PAIBA más exactamente en el servidor con Hostname **CONSOLAKASAB**, dirección IP Interna 10.x.x.x, se procedió a realizar la renovación de licenciamiento para la solución actualmente instalada que es Kaspersky Endpoint Security and Response OPTIMUM en adelante **KEDRO**, las imágenes a continuación evidencian la adición correcta de la licencia al contenedor de la consola de Kaspersky Security Center así como su fecha de vencimiento según periodo contratado y cantidad de dispositivos que puede proteger.

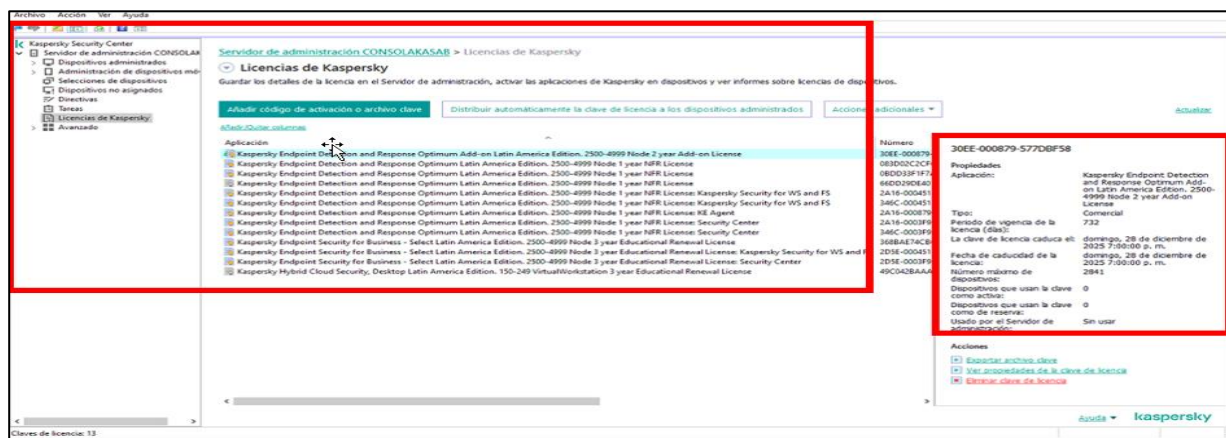


Ilustración 13 Licencia KEDRO instalada en la consola CONSOLAKASAB

El Despliegue de esta licencia es automático por defecto sin embargo para forzar una aplicación más rápida del licenciamiento en los equipos se realizó la creación y ejecución de una tarea de despliegue de la licencia como se ve en la imagen a continuación.

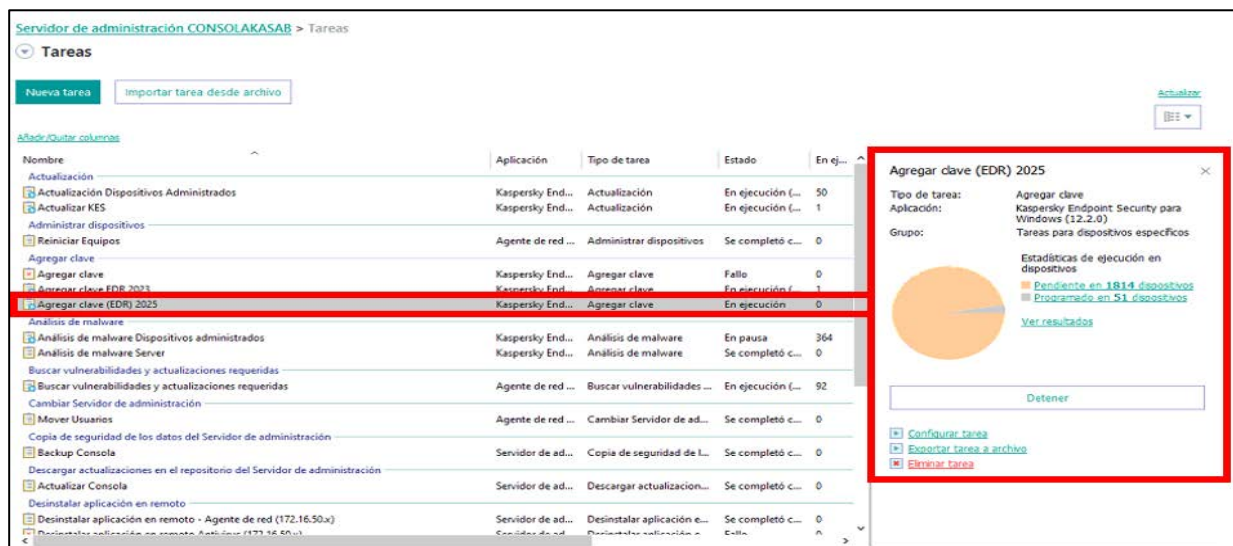


Ilustración 14 Tarea de despliegue Licencia KEDRO en la consola CONSOLAKASAB

Se realiza adición de la licencia que corresponde a Kaspersky Total Security en el contenedor de licencias de la consola de Kaspersky Security Center para despliegue automático a los equipos administrados en esta.

Servidor de administración CONSOLAKASAB > Licencias de Kaspersky

Licencias de Kaspersky
Guardar los detalles de la licencia en el Servidor de administración, activar las aplicaciones de Kaspersky en dispositivos y ver informes sobre licencias de dispositivos.

Añadir código de activación o archivo clave Distribuir automáticamente la clave de licencia a los dispositivos administrados Acciones adicionales Actualizar

Añadir/Quitar columnas

Aplicación	Número	Límite	Periodo de vigencia
Kaspersky Endpoint Detection and Response Optimum Add-on Latin America Edition. 2500-4999...	30EE-000879-577DBF58	2841	732
Kaspersky Endpoint Detection and Response Optimum Latin America Edition. 2500-4999 Node 1...	083D02C2CFC44032841...	3400	32
Kaspersky Endpoint Detection and Response Optimum Latin America Edition. 2500-4999 Node 1...	08D033F1F7A647DF8BF...	3400	45
Kaspersky Endpoint Detection and Response Optimum Latin America Edition. 2500-4999 Node 1...	2A16-000451-577D195F	3400	9
Kaspersky Endpoint Detection and Response Optimum Latin America Edition. 2500-4999 Node 1...	346C-000451-577C60DE	3400	32
Kaspersky Endpoint Detection and Response Optimum Latin America Edition. 2500-4999 Node 1...	2A16-000879-577D1960	3400	9
Kaspersky Endpoint Detection and Response Optimum Latin America Edition. 2500-4999 Node 1...	2A16-0003F9-577D195E	3400	9
Kaspersky Endpoint Detection and Response Optimum Latin America Edition. 2500-4999 Node 1...	346C-0003F9-577C60DD	3400	32
Kaspersky Endpoint Security for Business - Select Latin America Edition. 2500-4999 Node 3 year E...	3688AE74BCA4149BA9...	3400	1097
Kaspersky Endpoint Security for Business - Select Latin America Edition. 2500-4999 Node 3 year E...	2D5E-000451-57624378	3400	1097
Kaspersky Endpoint Security for Business - Select Latin America Edition. 2500-4999 Node 3 year E...	2D5E-0003F9-5762437A	3400	1097
Kaspersky Total Security for Business Latin America Edition. 2500-4999 Node 2 year Renewal Lice...	30EE-000451-577DBF47	3500	732

30EE-000451-577DBF47

Propiedades

Aplicación: Kaspersky Total Security for Business Latin America Edition. 2500-4999 Node 2 year Renewal License: Kaspersky Security for WS and FS

Tipo: Comercial

Periodo de vigencia de la licencia (días): 732

La clave de licencia caduca el: domingo, 28 de diciembre de 2025 7:00:00 p. m.

Fecha de caducidad de la licencia: domingo, 28 de diciembre de 2025 7:00:00 p. m.

Número máximo de dispositivos: 3500

Dispositivos que usan la clave como activa: 151

Dispositivos que usan la clave como de reserva: 0

Usado por el Servidor de administración: Sin usar

Acciones

- Exportar archivo clave
- Ver propiedades de la clave de licencia
- Eliminar clave de licencia

Ilustración 15 Licencia Kaspersky TOTAL instalada en la consola CONSOLAKASAB

En paralelo se crea y ejecuta una segunda tarea la cual tiene como objetivo agregar el licenciamiento de Kaspersky TOTAL Security para la activación del componente de protección endpoint ya que como se mencionó la licencia anterior habilita las opciones de protección para el EDR.

Servidor de administración CONSOLAKASAB > Tareas

Tareas

Nueva tarea Importar tarea desde archivo Actualizar

Añadir/Quitar columnas

Nombre	Aplicación	Tipo de tarea	Estado	En ej...
Actualización				
Actualización Dispositivos Administrados	Kaspersky End...	Actualización	En ejecución (...)	50
Actualizar KES	Kaspersky End...	Actualización	En ejecución (...)	1
Administrar dispositivos				
Reiniciar Equipos	Agente de red ...	Administrar dispositivos	Se completó c...	0
Agregar clave	Kaspersky End...	Agregar clave	Fallo	0
Agregar clave (EDR) 2025	Kaspersky End...	Agregar clave	Fallo	0
Agregar clave (Kaspersky Total) 2025	Kaspersky End...	Agregar clave	En ejecución (...)	0
Análisis de malware				
Análisis de malware Dispositivos administrados	Kaspersky End...	Análisis de malware	En pausa	364
Análisis de malware Server	Kaspersky End...	Análisis de malware	Se completó c...	0
Buscar vulnerabilidades y actualizaciones requeridas	Agente de red ...	Buscar vulnerabilidades ...	En ejecución (...)	92
Buscar vulnerabilidades y actualizaciones requeridas	Agente de red ...	Buscar vulnerabilidades ...	En ejecución (...)	92
Cambiar Servidor de administración	Agente de red ...	Cambiar Servidor de ad...	Se completó c...	0
Mover Usuarios	Agente de red ...	Cambiar Servidor de ad...	Se completó c...	0
Copia de seguridad de los datos del Servidor de administración	Servidor de ad...	Copia de seguridad de l...	Se completó c...	0
Backup Consola	Servidor de ad...	Copia de seguridad de l...	Se completó c...	0
Descargar actualizaciones en el repositorio del Servidor de administración	Servidor de ad...	Descargar actualización...	Se completó c...	0
Actualizar Consola	Servidor de ad...	Descargar actualización...	Se completó c...	0
Desinstalar aplicación en remoto	Servidor de ad...	Desinstalar aplicación...	Se completó c...	0
Desinstalar aplicación en remoto	Servidor de ad...	Desinstalar aplicación...	Se completó c...	0

Agregar clave (Kaspersky Total) 2025

Tipo de tarea: Agregar clave

Aplicación: Kaspersky Endpoint Security para Windows (12.2.0)

Grupo: Tareas para dispositivos específicos

Estadísticas de ejecución en dispositivos

Pendiente en 1866 dispositivos

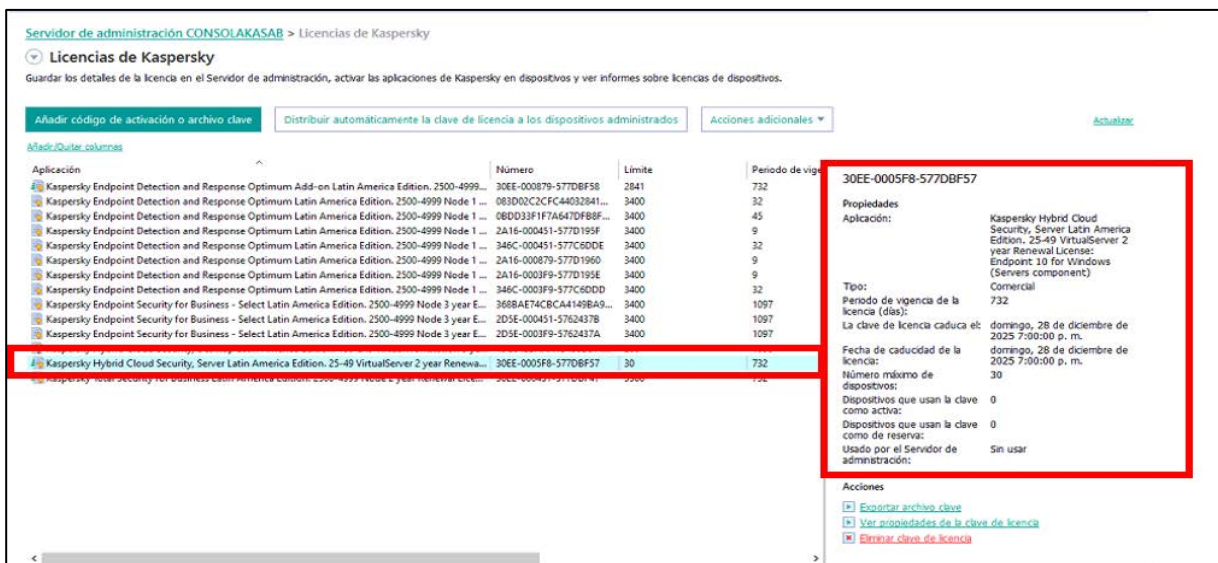
Ver resultados

Detener

Configurar tarea Exportar tarea a archivo Eliminar tarea

Ilustración 16 Tarea de despliegue Licencia Kaspersky TOTAL en la consola CONSOLAKASAB

Se realiza adición de la licencia que corresponde a Kaspersky Hybrid Cloud Security Server en el contenedor de licencias de la consola de Kaspersky Security Center para despliegue automático a los equipos administrados en esta como se consigna en la evidencia



Servidor de administración CONSOLAKASAB > Licencias de Kaspersky

Licencias de Kaspersky
Guardar los detalles de la licencia en el Servidor de administración, activar las aplicaciones de Kaspersky en dispositivos y ver informes sobre licencias de dispositivos.

[Añadir código de activación o archivo clave](#) [Distribuir automáticamente la clave de licencia a los dispositivos administrados](#) [Acciones adicionales](#) [Actualizar](#)

[Añadir/Quitar columnas](#)

Aplicación	Número	Límite	Período de vigencia
Kaspersky Endpoint Detection and Response Optimum Add-on Latin America Edition, 2500-4999...	30EE-000879-577DBF58	2041	732
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1...	081002C3CFC440326A1...	3400	32
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1...	08D033F1F7A6470F8B...	3400	45
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1...	2A16-000451-577D195F	3400	9
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1...	346C-000451-577C6DDE	3400	32
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1...	2A16-000879-577D1960	3400	9
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1...	2A16-0003F9-577C195E	3400	9
Kaspersky Endpoint Detection and Response Optimum Latin America Edition, 2500-4999 Node 1...	346C-0003F9-577C6DD0	3400	32
Kaspersky Endpoint Security for Business - Select Latin America Edition, 2500-4999 Node 3 year E...	3688AE74CBA4149BA9...	3400	1097
Kaspersky Endpoint Security for Business - Select Latin America Edition, 2500-4999 Node 3 year E...	2D5E-000451-5762437B	3400	1097
Kaspersky Endpoint Security for Business - Select Latin America Edition, 2500-4999 Node 3 year E...	2D5E-0003F9-5762437A	3400	1097
Kaspersky Hybrid Cloud Security, Server Latin America Edition, 25-49 VirtualServer 2 year Renewal...	30EE-0005F8-577DBF57	30	732
Kaspersky Total Security for Business Latin America Edition, 2500-4999 Node 2 year Renewal Licen...	30EE-000451-577DBF57	2500	732

30EE-0005F8-577DBF57

Propiedades

Aplicación: Kaspersky Hybrid Cloud Security, Server Latin America Edition, 25-49 VirtualServer 2 year Renewal License: Endpoint 10 for Windows (Servers component)

Tipo: Comercial

Período de vigencia de la licencia (días): 732

La clave de licencia caduca el: domingo, 28 de diciembre de 2025 7:00:00 p. m.

Fecha de caducidad de la licencia: domingo, 28 de diciembre de 2025 7:00:00 p. m.

Número máximo de dispositivos: 30

Dispositivos que usan la clave como activa: 0

Dispositivos que usan la clave como de reserva: 0

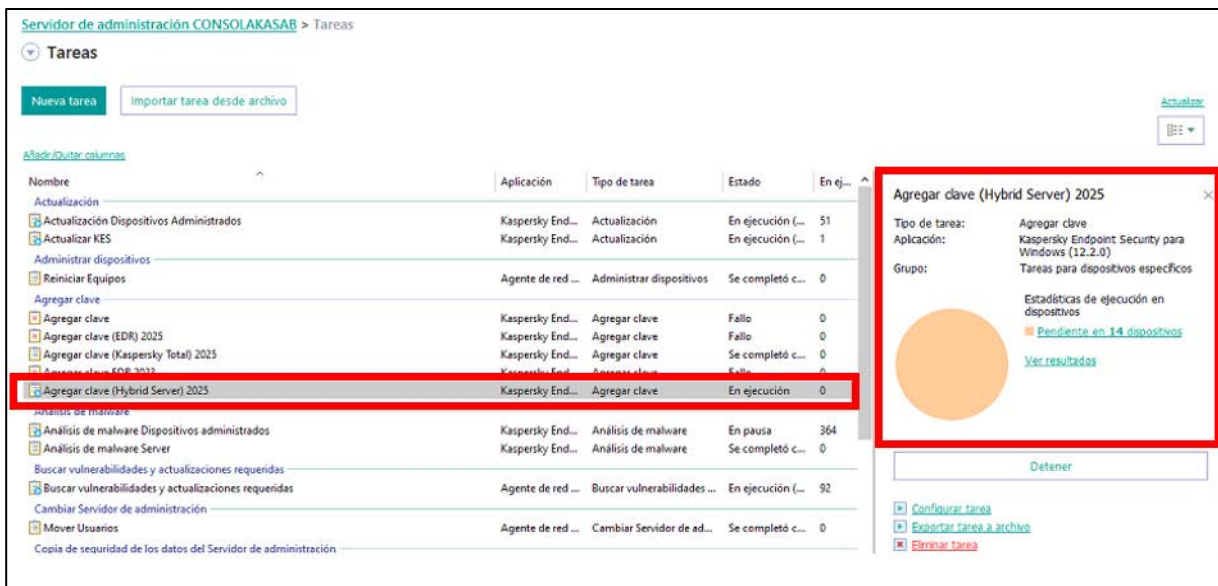
Usado por el Servidor de administración: Sin usar

Acciones

[Exponer archivo clave](#) [Ver propiedades de la clave de licencia](#) [Eliminar clave de licencia](#)

Ilustración 17 Licencia Kaspersky Hybrid Cloud Server- instalada en la consola CONSOLAKASAB

Se crea y ejecuta una segunda tarea la cual tiene como objetivo agregar el licenciamiento de Kaspersky Hybrid Cloud Security - Server para la activación del componente de protección endpoint en cada uno de los servidores con la solución instalada y administrada desde la consola de Kaspersky Security Center.



Servidor de administración CONSOLAKASAB > Tareas

Tareas

[Nueva tarea](#) [Importar tarea desde archivo](#) [Actualizar](#)

[Añadir/Quitar columnas](#)

Nombre	Aplicación	Tipo de tarea	Estado	En ejecución
Actualización				
Actualización Dispositivos Administrados	Kaspersky End...	Actualización	En ejecución (...)	51
Actualizar KES	Kaspersky End...	Actualización	En ejecución (...)	1
Administrar dispositivos				
Reiniciar Equipos	Agente de red ...	Administrar dispositivos	Se completó c...	0
Agregar clave				
Agregar clave (EDR) 2025	Kaspersky End...	Agregar clave	Fallo	0
Agregar clave (Kaspersky Total) 2025	Kaspersky End...	Agregar clave	Fallo	0
Agregar clave EDR 2025	Kaspersky End...	Agregar clave	Se completó c...	0
Agregar clave EDR 2025	Kaspersky End...	Agregar clave	Fallo	0
Agregar clave (Hybrid Server) 2025	Kaspersky End...	Agregar clave	En ejecución	0
Análisis de malware				
Análisis de malware Dispositivos administrados	Kaspersky End...	Análisis de malware	En pausa	364
Análisis de malware Server	Kaspersky End...	Análisis de malware	Se completó c...	0
Buscar vulnerabilidades y actualizaciones requeridas				
Buscar vulnerabilidades y actualizaciones requeridas	Agente de red ...	Buscar vulnerabilidades ...	En ejecución (...)	92
Cambiar Servidor de administración				
Mover Usuarios	Agente de red ...	Cambiar Servidor de ad...	Se completó c...	0
Copia de seguridad de los datos del Servidor de administración				

Agregar clave (Hybrid Server) 2025

Tipo de tarea: Agregar clave

Aplicación: Kaspersky Endpoint Security para Windows (12.2.0)

Grupo: Tareas para dispositivos específicos

Estadísticas de ejecución en dispositivos: **Pendiente en 14 dispositivos**

[Ver resultados](#)

[Detener](#)

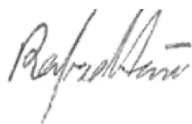
[Configurar tarea](#) [Exponer tarea a archivo](#) [Eliminar tarea](#)

Ilustración 18 Tarea de despliegue Licencia Kaspersky Hybrid Cloud en la consola CONSOLAKASAB

6. Tareas Programadas y Ejecutadas.

- Creación de los paquetes de instalación para cada una de las versiones para servidores y estaciones de trabajo en cada una de las consolas Kaspersky que administran los equipos de la Universidad Distrital Francisco Jose de Caldas.
- Creación y despliegue de tareas de instalación de los componentes de protección con versiones actualizadas previamente en la creación de paquetes de instalación, labor realizada en cada consola de administración Kaspersky.
- En la consola de la sede BOSA que corresponde al servidor de administración GOKU se ha realizado el despliegue e la solución Kaspersky Hybrid Cloud security para servidores y escritorios virtuales ya que, según requerimiento de la universidad distrital, estos equipos serán administrados desde esa consola.
- El licenciamiento restante hace parte del otro informe que incluye la implementación de las soluciones de protección de red.
- Se ha realizado transferencia de conocimiento en cada sesión a los participantes de la instalación y administración de la solución indicando las nuevas funcionalidades, así como el modo de operación y ejecución
- Todos los componentes de la solución se entregaron instalados y en completo funcionamiento, comprobado en el envío y recepción de datos para el análisis de cada uno, así como la aprobación de los ingenieros encargados de la instalación por parte de la Universidad Distrital

Elaboró.



Rafael Mariano Acuña Giraldo
Gerente de Soporte TI
Infocomunicaciones S.A.S

Revisó.



Juan Sebastian Gil Bolaños
Área de Plataformas Red de Datos UDNET
Universidad Distrital Francisco José de Caldas

PRODUCTO	FECHA PROGRAMADA	HORA PROGRAMADA	RESPONSABLES INFOCOMUNICACIONES	RESPONSABLES UNIVERSIDAD DISTRITAL
PRESENTACIÓN, CAPACITACION, O BOLETIN DE SEGURIDAD INFORMATICA (CONTRATO 2038 -2023)	1/12/2024	10:00 a. m.	Rafael Acuña Area de Tecnología Infocomunicaciones	Area de Plataformas - Red de Datos UDNET - Universidad Distrital
	15/3/2024			
	17/5/2024			
	7/12/2024			
	13/9/2024			
	15/11/2024			
	17/1/2025			
	14/3/2025			
	16/5/2025			
	18/7/2025			
	19/9/2025			
	14/11/2025			
	15/1/2026			
	19/3/2026			
	14/5/2026			
	16/7/2026			
	17/9/2026			
	19/11/2026			

NOTA: Las fechas estipuladas estaran sujetas a modificación si la Universidad así lo considera previo a la programación inicial.

Las sesiones se realizaran por espacio de una hora de manera virtual mediante el enlace de Microsoft Teams o la plataforma de video conferencia que la Universidad destine o la sugerida por Infocomunicaciones S.A.S.

Los temas para cada sesión estaran enfocados en las principales novedades de seguridad informática que se presenten a la fecha, en caso de sugerencia de algun nuevo tema por parte de la Universidad Distrital debiera ser comunicado por lo menos con una semana de antelación para poder revisar los detalles necesarios.

Representación Gráfica

Datos del Documento

Código Único de Factura - CUFE :
badba98fd3e8adff926dd1a5dfe747ff5076dbd8c9cd683d83e9372946d5e10b19b244af20b39152a0865871ea0c571d

Número de Factura: FEV-1
Fecha de Emisión: 24/05/2024
Fecha de Vencimiento: 08/07/2024
Tipo de Operación: 10 - Estándar

Forma de pago: Crédito
Medio de Pago: Transferecia Crédito
Orden de pedido:
Fecha de orden de pedido:

Datos del Emisor / Vendedor

Razón Social: UNIÓN TEMPORAL INFO COMUNICACIONES S.A.S. LAN SECURITY NETWORKS S.A.S
Nombre Comercial: UNIÓN TEMPORAL INFO COMUNICACIONES S.A.S. LAN SECURITY NETWORKS S.A.S
Nit del Emisor: 901783379
Tipo de Contribuyente: Persona Jurídica
Régimen Fiscal:O-23
Responsabilidad tributaria: 01 - IVA
Actividad Económica: 4741

País: Colombia
Departamento: Bogotá
Municipio / Ciudad: Bogotá, D.c.
Dirección: AUTOPISTA MEDELLIN KM 3.5 TERMINAL TERRESTRE DE CARGA OF C4
Teléfono / Móvil: 3176433159
Correo: bibiana@infocomunicaciones.net

Datos del Adquiriente / Comprador

Nombre o Razón Social: UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS
Tipo de Documento: NIT
Número Documento: 899999230
Tipo de Contribuyente: Persona Jurídica
Régimen fiscal: R-99-PN
Responsabilidad tributaria: ZZ - No aplica

País: Colombia
Departamento: Bogotá
Municipio / Ciudad: Bogotá, D.c.
Dirección: Calle 13 # 31 -75
Teléfono / Móvil: 6013239300
Correo: udnet@udistrital.edu.co

Detalles de Productos

Nro.	Código	Descripción	U/M	Cantidad	Precio unitario	Descuento detalle	Recargo detalle	IMPUESTOS				Precio unitario de venta
								IVA	%	INC	%	
1	001	LICENCIAMIENTO POR UN (1) AÑO PARA LA SOLUCIÓN DE DETECCIÓN, PREVENCIÓN Y RESPUESTA DE RED KL7122DY*FZ	NIU	1,00	\$ 370.000.000,00	\$ 0,00	\$ 0,00	\$ 70.300.000,00	19.00			\$ 370.000.000,00
2	002	LICENCIAS PARA ENDPOINTS POR UN (1) AÑO SOBRE LA SOLUCIÓN DE DETECCIÓN, PREVENCIÓN Y RESPUESTA DE RED	NIU	200,00	\$ 200.000,00	\$ 0,00	\$ 0,00	\$ 7.600.000,00	19.00			\$ 40.000.000,00
3	003	SERVICIO DE SOPORTE DE PARTNER EN ESQUEMA 7x24 POR UN (1) AÑO PARA TODA LA SOLUCIÓN DE DETECCIÓN, PREVENCIÓN Y RESPUESTA DE RED INCLUYENDO ACTUALIZACIONES (UPDATE Y UPGRADE)	NIU	1,00	\$ 90.000.000,00	\$ 0,00	\$ 0,00	\$ 17.100.000,00	19.00			\$ 90.000.000,00
4	004	SERVICIO INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN CORRECTO FUNCIONAMIENTO DE LA SOLUCIÓN DE DETECCIÓN, PREVENCIÓN Y RESPUESTA DE RED, ASÍ COMO LA INTEGRACIÓN CON LAS LICENCIAS KL7222D2*FZ	NIU	1,00	\$ 80.000.000,00	\$ 0,00	\$ 0,00	\$ 15.200.000,00	19.00			\$ 80.000.000,00

Datos Totales



Documento validado por la DIAN 2024-05-24 12:44:48
Documento generado el: 2024-05-24 12:44:48
Generado por: Solución Gratuita DIAN
Nit:800197268

Numero de Autorización: 18764070518710

Rango desde: 1

MONEDA	COP
TASA DE CAMBIO	

Subtotal	580.000.000,00
Descuento detalle	0,00
Recargo detalle	0,00
Total Bruto Factura	580.000.000,00
IVA	110.200.000,00
INC	0,00
Bolsas	0,00
Otros impuestos	0,00
Total impuesto (=)	110.200.000,00
Total neto factura (=)	690.200.000,00
Descuento Global (-)	0,00
Recargo Global (+)	0,00
Total factura (=)	COP \$ \$ 690.200.000,00

Valores informativos

ANTICIPOS	
Anticipos	0,00
RETENCIONES	
Rete fuente	0,00
Rete IVA	0,00
Rete ICA	0,00

Rango hasta: 10

Vigencia: 2026-05-10

Representación Gráfica

Datos del Documento

Código Único de Factura - CUFE :
a8b65a19adcf6868e82717a09813594d1383fb07c5e748cedabe6b9ec50860cf70726d8f99ed61ee481882da1de8f6bf

Número de Factura: FEV-3	Forma de pago: Crédito
Fecha de Emisión: 28/05/2024	Medio de Pago: Transferecia Crédito
Fecha de Vencimiento: 12/07/2024	Orden de pedido:
Tipo de Operación: 10 - Estándar	Fecha de orden de pedido:

Datos del Emisor / Vendedor

Razón Social: UNIÓN TEMPORAL INFO COMUNICACIONES S.A.S. LAN SECURITY NETWORKS S.A.S	
Nombre Comercial: UNIÓN TEMPORAL INFO COMUNICACIONES S.A.S. LAN SECURITY NETWORKS S.A.S	
Nit del Emisor: 901783379	País: Colombia
Tipo de Contribuyente: Persona Jurídica	Departamento: Cundinamarca
Régimen Fiscal:O-23	Municipio / Ciudad: Cota
Responsabilidad tributaria: 01 - IVA	Dirección: AUTOPISTA MEDELLIN KM 3.5 TERMINAL TERRESTRE DE CARGA OF C4
Actividad Económica: 4741	Teléfono / Móvil: 3176433159
	Correo: bibiana@infocomunicaciones.net

Datos del Adquiriente / Comprador

Nombre o Razón Social: UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS	
Tipo de Documento: NIT	País: Colombia
Número Documento: 899999230	Departamento: Bogotá
Tipo de Contribuyente: Persona Jurídica	Municipio / Ciudad: Bogotá, D.c.
Régimen fiscal: R-99-PN	Dirección: Calle 13 # 31 -75
Responsabilidad tributaria: ZZ - No aplica	Teléfono / Móvil: 6013239300
	Correo: udnet@udistrital.edu.co

Detalles de Productos

								IMPUESTOS				Precio unitario de venta
Nro.	Código	Descripción	U/M	Cantidad	Precio unitario	Descuento detalle	Recargo detalle	IVA	%	INC	%	
1	005	LICENCIAMIENTO POR DOS (2) AÑOS PARA EL SOFTWARE DE SEGURIDAD PARA DISPOSITIVOS DE USUARIO FINAL KL4869DAXTR	NIU	3.000,00	\$ 48.000,00	\$ 0,00	\$ 0,00	\$ 27.360.000,00	19.00			\$ 144.000.000,00
2	006	LICENCIAMIENTO POR DOS (2) AÑOS DEL AGENTE EDR DEL SOFTWARE DE ANTIVIRUS PARA DISPOSITIVOS DE USUARIO FINAL KL4707DAXTH	NIU	2.841,00	\$ 21.000,00	\$ 0,00	\$ 0,00	\$ 11.335.590,00	19.00			\$ 59.661.000,00
3	007	LICENCIAMIENTO POR DOS (2) AÑOS PARA LA SOLUCIÓN DE SEGURIDAD ANTIVIRUS PARA AMBIENTES VIRTUALES COMPATIBLES CON XENDESKTOP 7.15 KL4155DASTR	NIU	200,00	\$ 86.000,00	\$ 0,00	\$ 0,00	\$ 3.268.000,00	19.00			\$ 17.200.000,00
4	008	LICENCIAMIENTO POR DOS (2) AÑOS PARA LA SOLUCIÓN DE SEGURIDAD ANTIVIRUS PARA SERVIDORES VIRTUALES KL4255DAPTR	NIU	30,00	\$ 188.000,00	\$ 0,00	\$ 0,00	\$ 1.071.600,00	19.00			\$ 5.640.000,00
5	009	SERVICIO DE SOPORTE PARTNER EN ESQUEMA 7x24 POR DOS (2) AÑOS PARA LA SOLUCIÓN DE SEGURIDAD ANTIVIRUS INCLUYENDO ACTUALIZACIONES (UPDATE Y UPGRADE)	NIU	1,00	\$ 40.000.000,00	\$ 0,00	\$ 0,00	\$ 7.600.000,00	19.00			\$ 40.000.000,00
6	010	SERVICIO INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN CORRECTO FUNCIONAMIENTO DE LA SOLUCIÓN DE SEGURIDAD ANTIVIRUS SOBRE LOS EQUIPOS DE LA UNIVERSIDAD	NIU	1,00	\$ 1,00	\$ 1,00	\$ 0,00					\$ 0,00

Notas Finales

Linea de negocio:

Datos Totales



Documento validado por la DIAN 2024-05-28 09:57:50
Documento generado el: 2024-05-28 09:57:49
Generado por: Solución Gratuita DIAN
Nit:800197268

Numero de Autorización: 18764070518710

Rango desde: 1

MONEDA	COP
TASA DE CAMBIO	

Subtotal	266.501.001,00
Descuento detalle	1,00
Recargo detalle	0,00
Total Bruto Factura	266.501.000,00
IVA	50.635.190,00
INC	0,00
Bolsas	0,00
Otros impuestos	0,00
Total impuesto (=)	50.635.190,00
Total neto factura (=)	317.136.190,00
Descuento Global (-)	0,00
Recargo Global (+)	0,00
Total factura (=)	COP \$ \$ 317.136.190,00

Valores informativos

ANTICIPOS	
Anticipos	0,00

RETENCIONES	
Rete fuente	0,00
Rete IVA	0,00
Rete ICA	0,00

Rango hasta: 10

Vigencia: 2026-05-10