INFORME DE ACTIVIDADES

CONTRATO 225-2024

ADQUISICIÓN DE LA RENOVACION DEL LICENCIAMIENTO
ANTIVIRUS ESET PROTECT COMPLETE PARA
LA INSTITUCION UNIVERSITARIA DE ENVIGADO.

La vigencia del Licenciamiento y del soporte técnico será por DOCE (12) meses.

SOLUCIONES EN SEGURIDAD INFORMATICA S.A.S
Representante Legal

Omar Balmore Calvo Monsalve
c.c. 98557333 Envigado

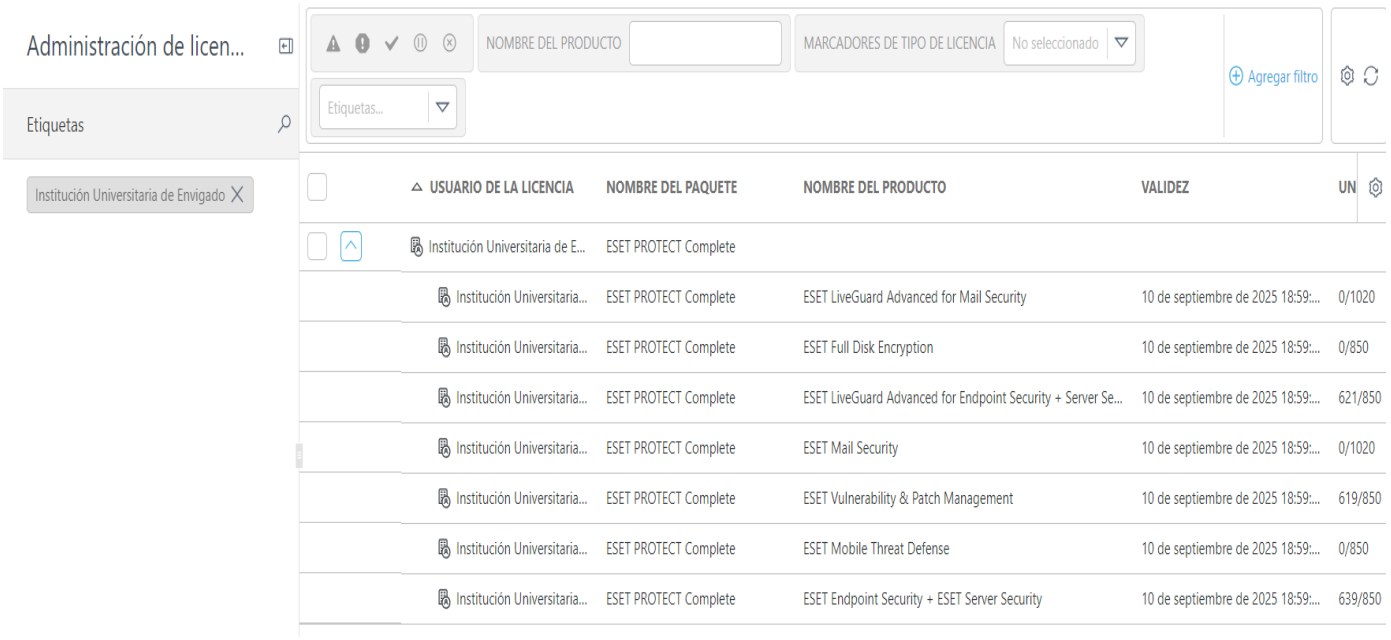
Informe de activación y actualización ESET PROTECT COMPLETE
Sres. Institución Universitaria de Envigado
Viviana Vélez

Saludos

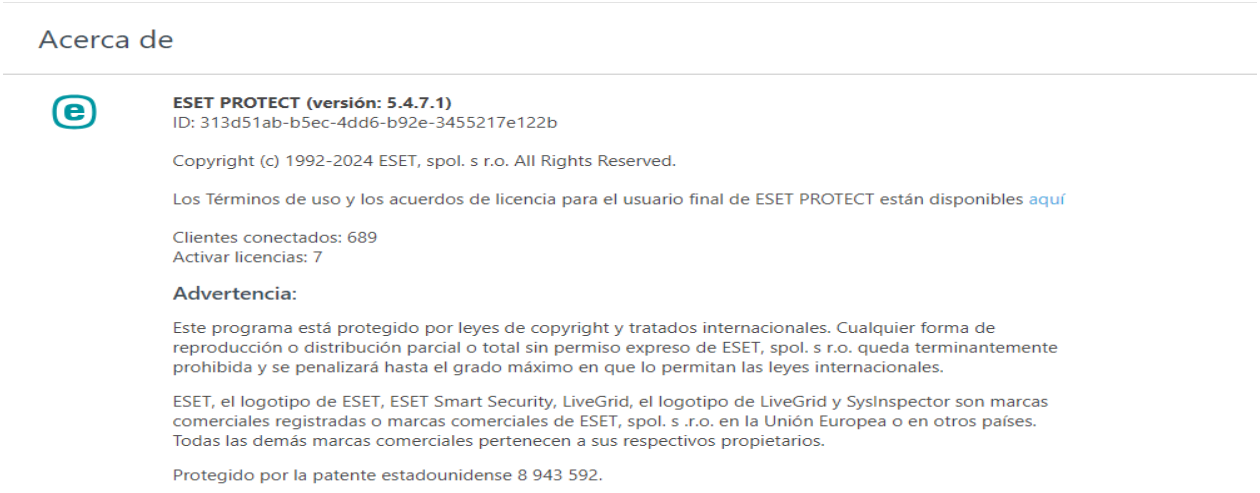
El lunes 2 de septiembre en compañía del Ingeniero Wadis Arcila se realizó la conexión a la consola de ESET PROTECT, en esta se realizaron los siguientes procesos:

1. Se procedió a cargar el licenciamiento generado, se verifica el periodo de caducidad, aplicación y distribución a los clientes.

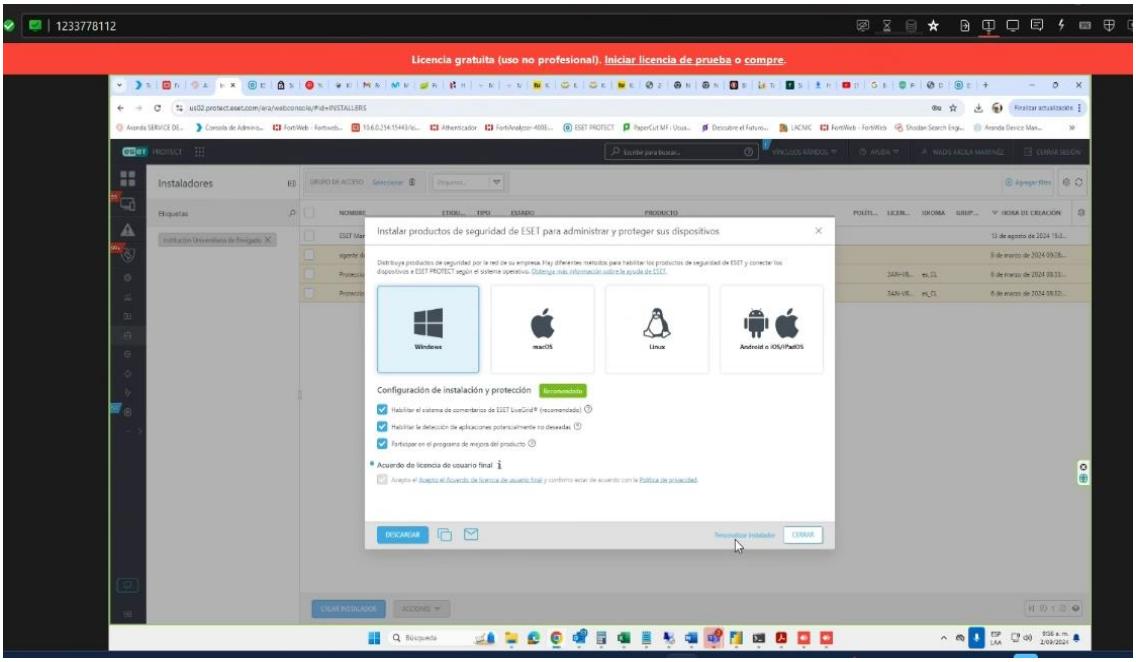
Producto:
ESET PROTECT Complete
Clave de licencia:
THRM-X73D-WXN6-2VW3-BWTW
ID público:
3AN-V8X-A7W
Cliente:
INSTITUCION UNIVERSITARIA DE ENVIGADO
Opción de Compra:
Downgrade
Expiración:
10/09/2025
Licencias:
850
Capas de seguridad:
ESET Endpoint Security + ESET Server Security
ESET LiveGuard Advanced for Endpoint Security + Server Security
ESET Full Disk Encryption
ESET Mail Security
ESET Cloud Office Security (component)
ESET LiveGuard Advanced for Mail Security
ESET LiveGuard Advanced for Cloud Office Security
ESET Endpoint Security para Android



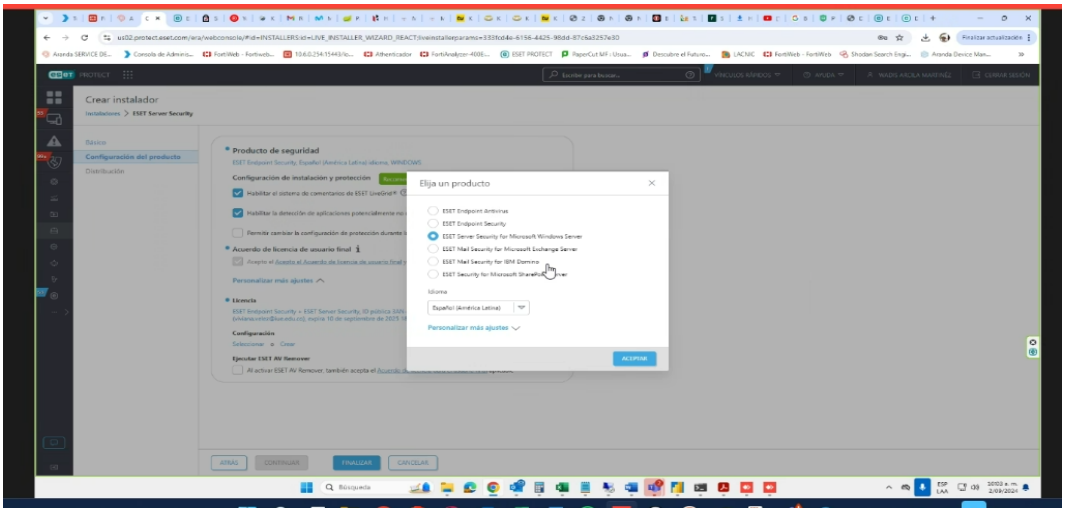
2. Se verifica que se encuentre instalado la última versión de la consola de administración ESET PROTECT



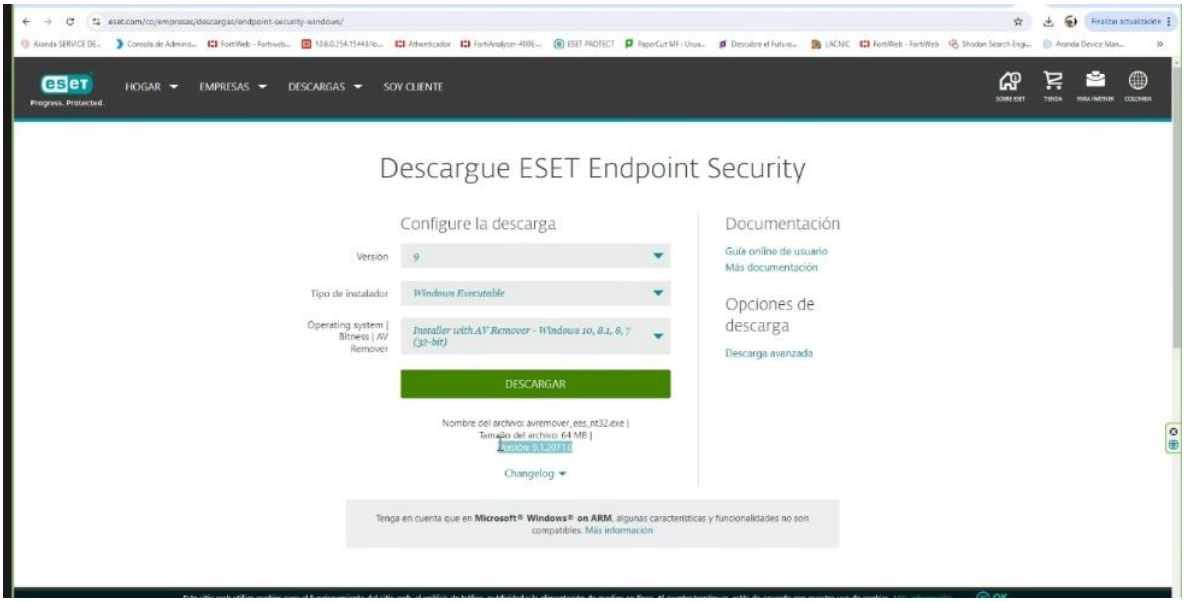
3. Se crean los nuevos paquetes “Todo en Uno” para servidores ESET Server Security 11.0.1.2012, para estaciones ESET Endpoint Security 11.1.2039 y para el agente de comunicaciones



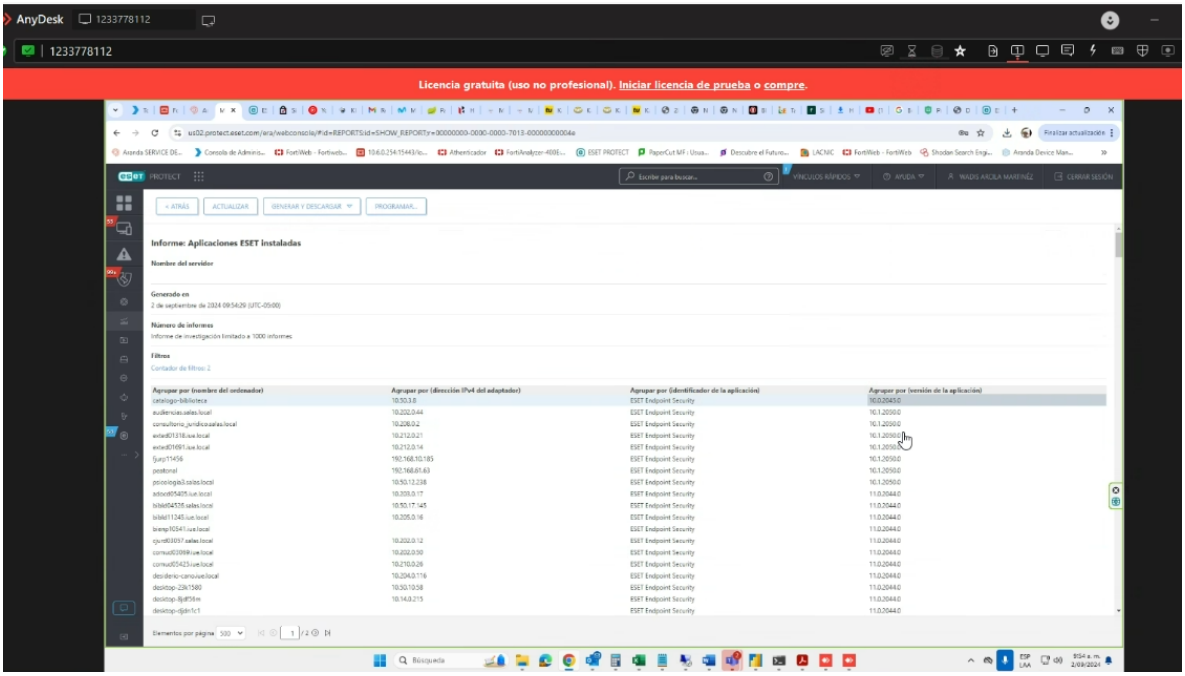
	NOMBRE	ETIQUET...	TIPO	ESTADO	PRODUC...	POLÍTICA	LICENCIA	IDIOMA	GRUPO ...	HORA DE CREACIÓN
☐	ESET Management Agent		Live Insta...							2 de septiembre de 2024 10:...
☐	ESET Server Security		Live Insta...		ESET Serv...		3AN-V8X...	es_CL		2 de septiembre de 2024 10:...
☐	ESET Endpoint Security 11.1		Live Insta...		ESET End...		3AN-V8X...	es_CL		2 de septiembre de 2024 10:...
☐	ESET Endpoint Security para Windo...		Live Insta...		ESET End...		3AN-V8X...	es_CL		2 de septiembre de 2024 10:...



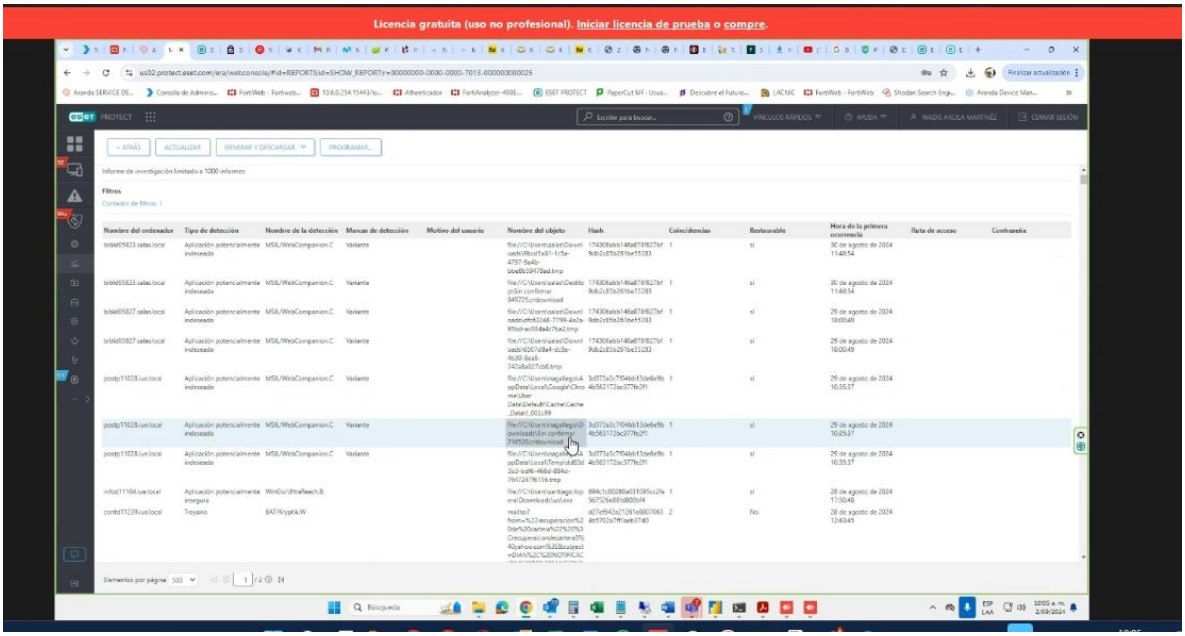
El ingeniero manifiesta que tiene unos equipos con Windows 8.1 y que le sale el mensaje que no es compatible con la versión 11, se busca cual es la versión compatible que corresponde a la versión 9 y se le generan los paquetes de instalación



4. Se realiza el despliegue de las nuevas protecciones para estaciones de trabajo y servidores para que queden en la última versión disponible



5. Se revisa los eventos de detecciones centralizadas en la consola de administración y se confirma que han sido procesados de forma correcta. En un caso puntual realizamos exclusión de unos correos electrónicos que estaban llegando infectados y se bloquean los remitentes.



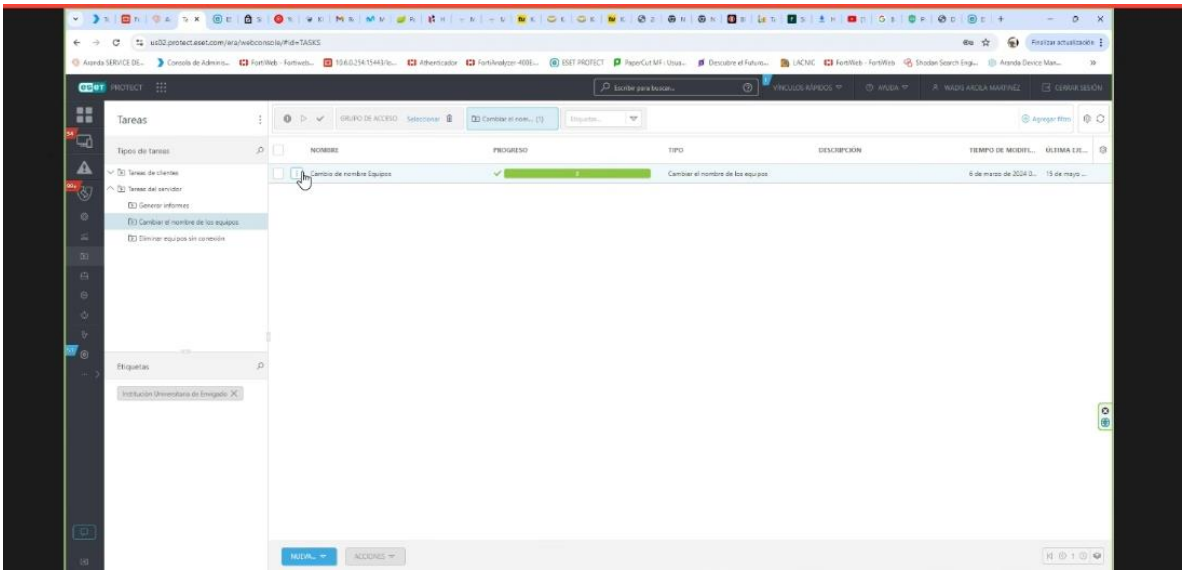
	ECC...	CAUSA	ACCIÓN	OC...	RES...	NOMBRE DEL ORDENADOR	DIRECCIONES IP	OBJETO
	co...	Bloqueado por lista negra PUA	Bloqueado	1		bibld04124.iu...	10.205.0.13	https://my.rtmark.net
	co...	Bloqueado por lista negra PUA	Bloqueado	1		comup10536....	10.210.0.29	https://my.rtmark.net
	co...	Bloqueado por lista negra PUA	Bloqueado	1		fsocp10551.iu...	172.20.4.95	https://my.rtmark.net
	co...	Bloqueado por lista negra PUA	Bloqueado	1		bibld04124.iu...	10.205.0.13	https://my.rtmark.net
	co...	Bloqueado por lista negra PUA	Bloqueado	1		comup10536....	10.210.0.29	https://my.rtmark.net
	co...	Bloqueado por lista negra PUA	Bloqueado	1		comup10536....	10.210.0.29	https://my.rtmark.net
	co...	Bloqueado por lista negra PUA	Bloqueado	1		fsocp10551.iu...	172.20.4.95	https://my.rtmark.net
	co...	Bloqueado por lista negra PUA	Bloqueado	1		comup10536....	10.210.0.29	https://my.rtmark.net
	co...	Bloqueado por lista negra PUA	Bloqueado	1		bibld04124.iu...	10.205.0.13	https://my.rtmark.net
	co...	Bloqueado por lista negra PUA	Bloqueado	1		comup10536....	10.210.0.29	https://my.rtmark.net
	co...	Bloqueado por lista negra PUA	Bloqueado	1		fsocp10551.iu...	172.20.4.95	https://my.rtmark.net
	co...	Bloqueado por lista negra PUA	Bloqueado	1		comup10536....	10.210.0.29	https://my.rtmark.net
	co...	Bloqueado por lista negra PUA	Bloqueado	1		bibld04124.iu...	10.205.0.13	https://my.rtmark.net

6. Se eliminan registros obsoletos de computadores que perdieron comunicación con la consola de administración ESET PROTECT por motivos como formateo, actualización o dados de baja.

NOMBRE	DIRECCIONES IP	NOMBRE DEL SISTEMA OP	USUARIOS REGISTRADOS	ÚLTIMA CONEXIÓN	DI
peatonal	192.168.61.63	Microsoft Windows 10 Pro	IUE	2 oct 2023, 18:33:22	
equipo-8-imac...	10.255.253.39	macOS 13 (Ventura)	sala209	12 abr 2024, 11:43:49	
audiencias.salas.local	10.202.0.44	Microsoft Windows 11 Ed...	Consultorio.Juridico	17 abr 2024, 16:15:32	
fempp1...	10.50.23.199	Microsoft Windows 10 Ed...	lfcano	19 abr 2024, 17:07:59	
iinnd05...	10.12.0.17	Microsoft Windows 10 Ed...	luisa.buritica	24 abr 2024, 15:21:29	
exted11...	10.212.0.1	Microsoft Windows 11 Ed...	victor.ramirez	29 abr 2024, 12:52:09	
bienp1...		Microsoft Windows 11 Ed...	Administrador	2 may 2024, 08:03:53	
fempp1...	192.168.1.3	Microsoft Windows 10 Ed...	vapabon	15 may 2024, 20:44:36	
pc205-...	10.1.0.246	Microsoft Windows 10 Ed...		16 may 2024, 18:36:22	
marcela-escob...	10.12.0.43	macOS 10.15 (Catalina)	2	17 may 2024, 10:30:56	
desktop...	10.50.10.58	Microsoft Windows 10 Ed...	iue	20 may 2024, 13:28:24	
fempp0...	10.15.0.58	Microsoft Windows 10 Ed...	lzapata	21 may 2024, 13:16:38	
bibld11...	10.205.0.16	Microsoft Windows 10 Ed...	adela.gallego	27 may 2024, 08:38:43	

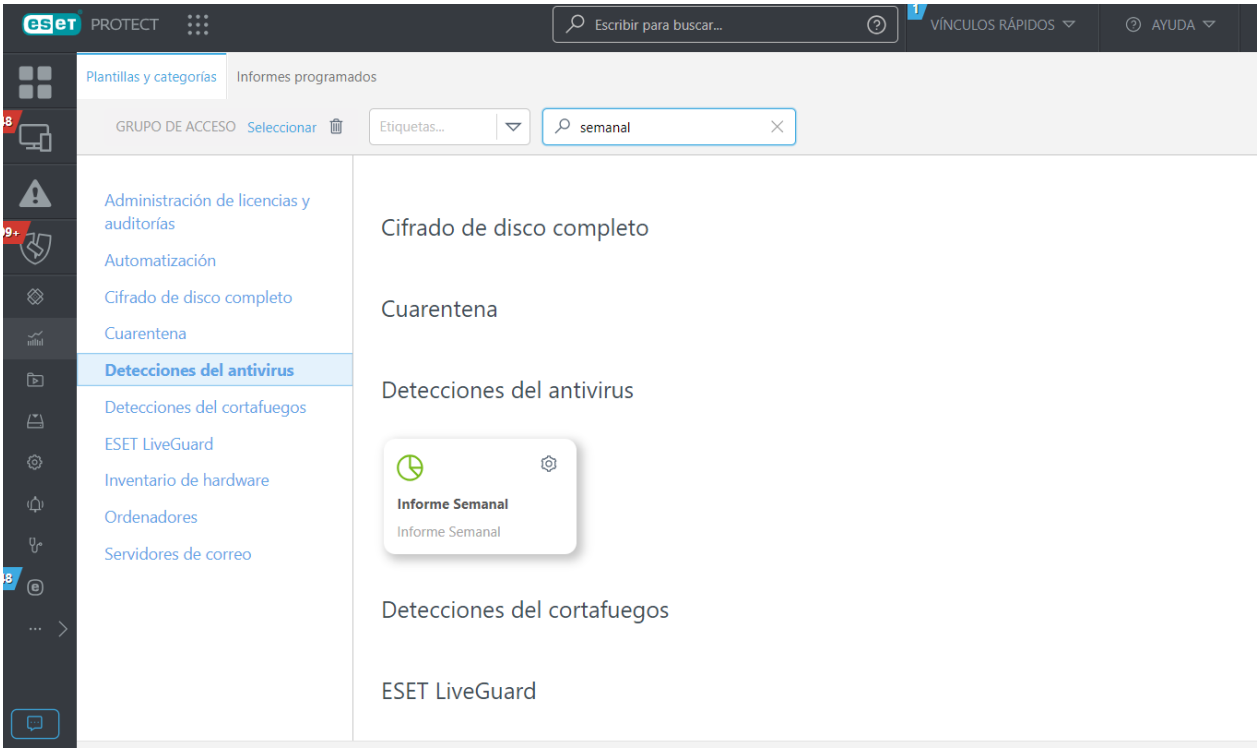
0 / 692

El ingeniero nos informa que han formateado mucha maquina y que adicional han cambiado el nombre de algunos equipos por lo que se corre la tarea de cambio de nombre en las maquinas



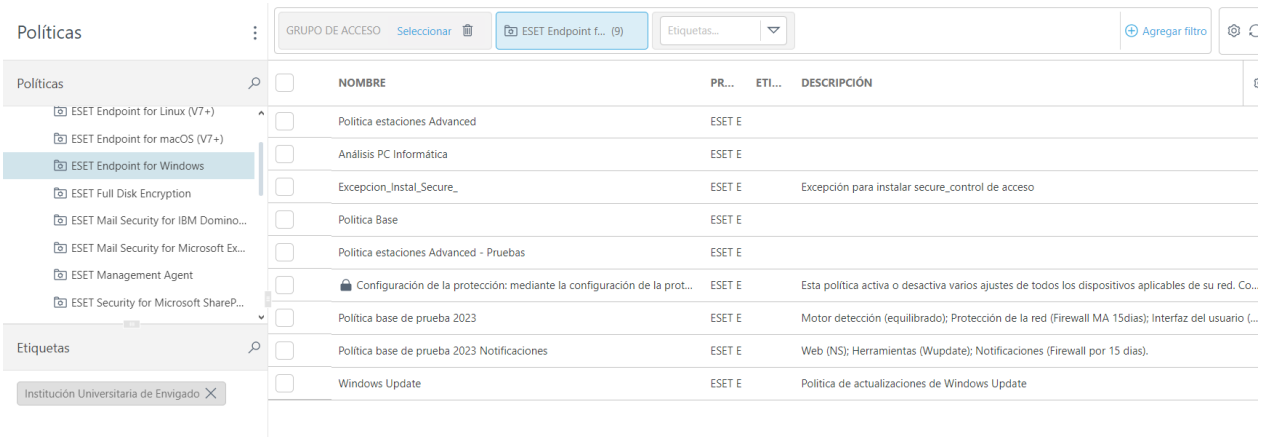
7. Se revisa los informes de versión de protección, cuarentena, los ordenadores más infectados durante los últimos 30 días.

8. Se revisan los informes generados por ESET que le estén llegando de manera correcta al ingeniero. Se encuentra que el informe de vulnerabilidades no esta llegando bien por lo que es necesario volverlo a parametrizar

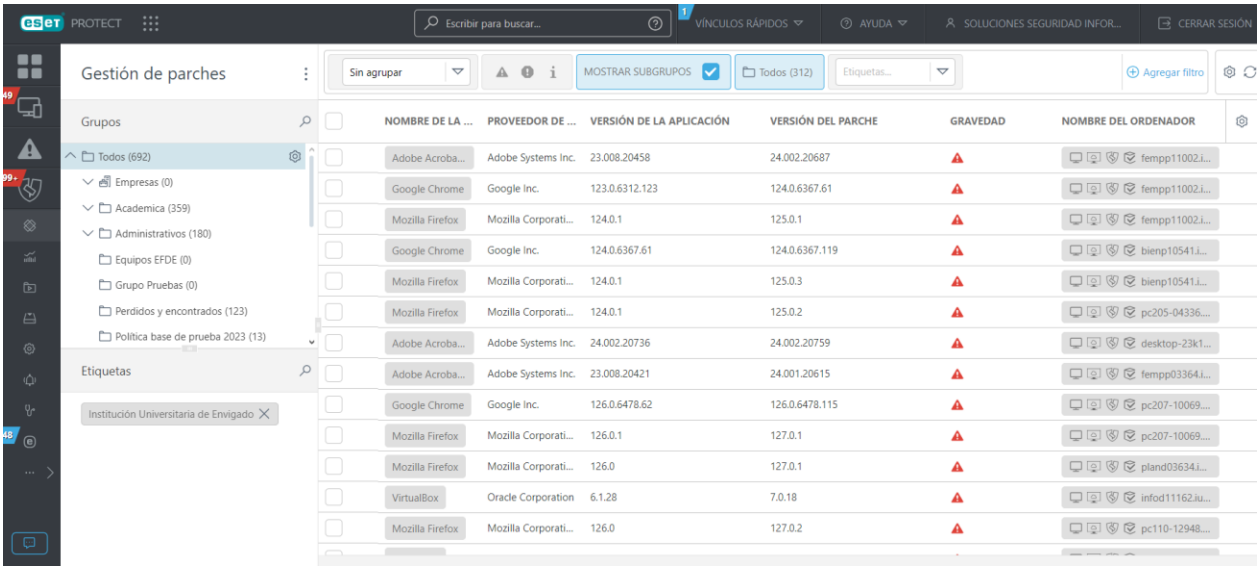


9. Se depuran las tareas viejas y se dejan solo las que están operativas.

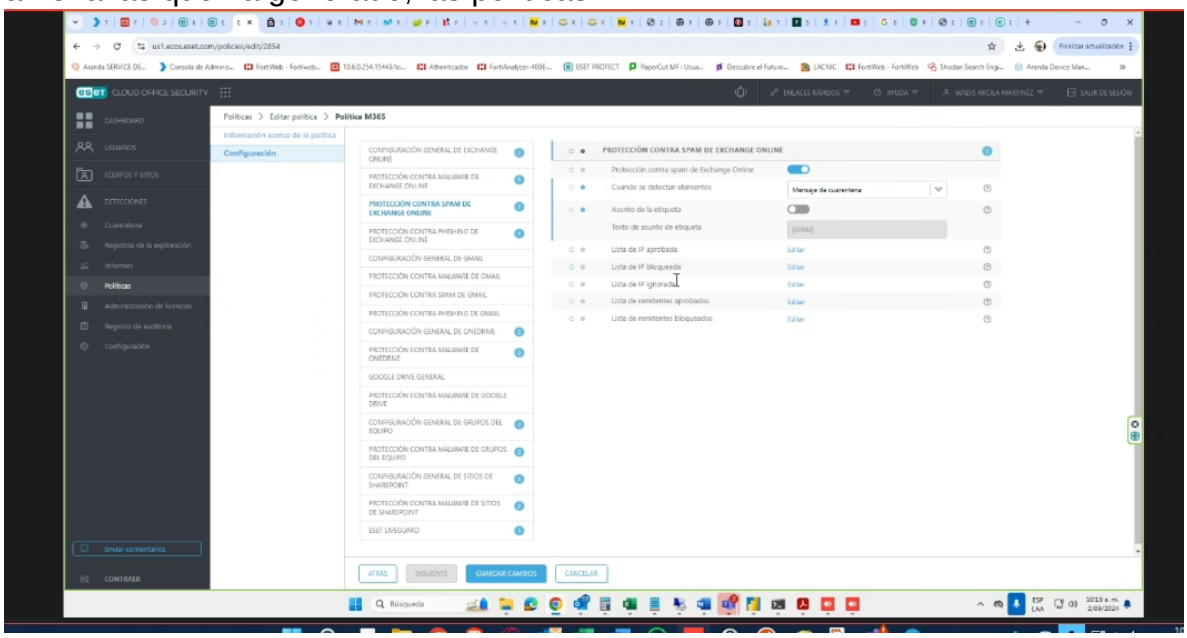
10. Se revisa que las políticas y configuraciones estén correctas, de acuerdo al sistema operativo.



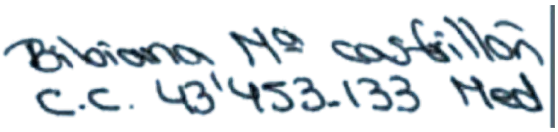
11. Se revisa el módulo de búsqueda de vulnerabilidades ESET Vulnerability & Patch Management, se valida que este aplicando los parches correctamente .



12. Se revisa la consola de ESET **Cloud Office Security (component)**, las amenazas que ha generado, las políticas.

13. 

Soporte realizado por:



Soluciones en Seguridad Informática
BIBIANA MARIA CASTRILLON TORO.
Ingeniera de Soporte
Email: bibianacastrillon@segurinfo.co
Teléfono: (574) 4445088 ext. 1001 Celular: (57) 3148941012
Carrera 79A No 53B-116 Int 101 Medellín – Colombia
Visita nuestra página www.segurinfo.co