

Implementación del Agente Nessus Professional
Superintendencia de Industria y Comercio

Noviembre del 2024

TABLA DE CONTENIDO

1 DERECHOS DEL DOCUMENTO....3
2 OBJETIVOS....3
3 ENTREGA E INSTALACIÓN....3
4 PROTOCOLO DE ESCALAMIENTO....5
5 RECOMENDACIONES....6

1 DERECHOS DEL DOCUMENTO

Documento de uso interno y exclusivo de la Empresa, que contiene información confidencial de SIC Y MCO GLOBAL, por lo cual MCO GLOBAL se compromete a resguardar y utilizar la información contenida en el mismo para los fines del proyecto, y a respetar los acuerdos de confidencialidad establecidos y firmados entre las partes. Así mismo, este documento se considera propiedad de la MCO GLOBAL y su divulgación parcial o total a terceros no está permitida sin el consentimiento previo y explícito (por escrito) de la Empresa.

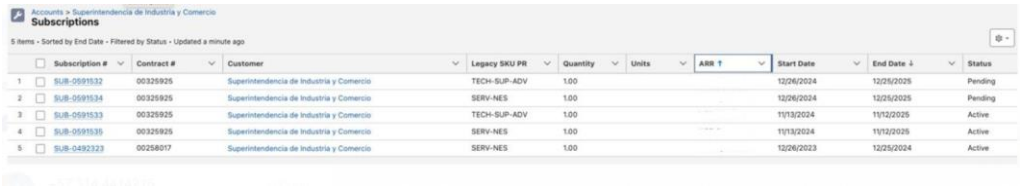
2 OBJETIVOS

Este informe detalla las actividades realizadas para la entrega, instalación, configuración y puesta en funcionamiento del Agente Nessus Professional conforme a las disposiciones del contrato y requisitos de pago para ambas suscripciones. Además, se especifican las obligaciones específicas, el cumplimiento durante la vigencia del contrato, los Acuerdos de Nivel de Servicio (SLA) y el protocolo de escalamiento para requerimientos de servicio y soporte.

3 ENTREGA E INSTALACIÓN

3.1 Actividades Realizadas

Recepción del software y licencias: Se recibieron las claves de activación y el acceso a las plataformas correspondientes para las dos suscripciones de Nessus Professional.


Accounts > Superintendencia de Industria y Comercio

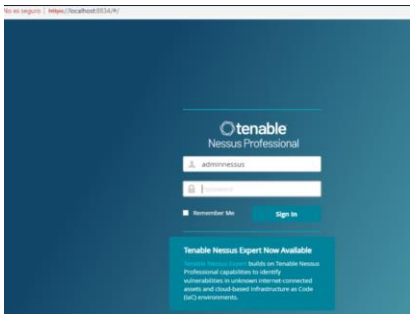
Subscriptions

5 items - Sorted by End Date - Filtered by Status - Updated a minute ago

	Subscription #	Contract #	Customer	Legacy SKU PR	Quantity	Units	ARR	Start Date	End Date	Status
1	SUB-0591532	00325925	Superintendencia de Industria y Comercio	TECH-SUP-ADV	1.00			12/26/2024	12/25/2025	Pending
2	SUB-0591534	00325925	Superintendencia de Industria y Comercio	SERV-NES	1.00			12/26/2024	12/25/2025	Pending
3	SUB-0591533	00325925	Superintendencia de Industria y Comercio	TECH-SUP-ADV	1.00			11/13/2024	11/12/2025	Active
4	SUB-0591535	00325925	Superintendencia de Industria y Comercio	SERV-NES	1.00			11/13/2024	11/12/2025	Active
5	SUB-0492323	00258017	Superintendencia de Industria y Comercio	SERV-NES	1.00			12/26/2023	12/25/2024	Active

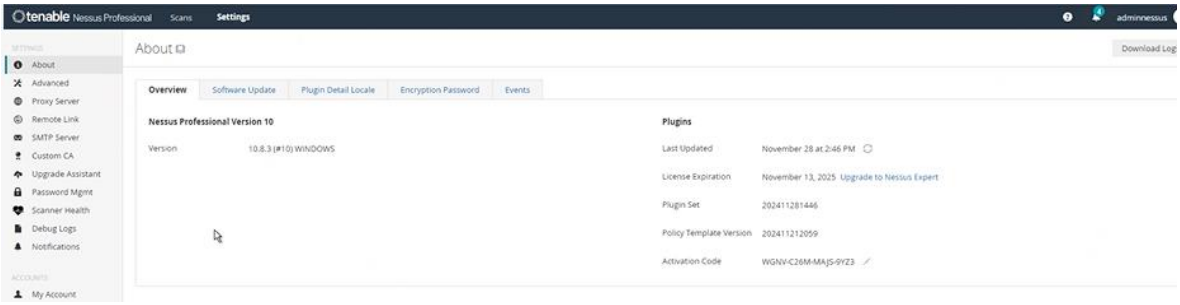
Entrega al cliente: Se realizó la entrega formal de las licencias al cliente, junto con la documentación técnica proporcionada por el fabricante.

Instalación del agente:
Se Instalo el agente Nessus Professional en las máquinas designadas, siguiendo las mejores prácticas de Tenable.



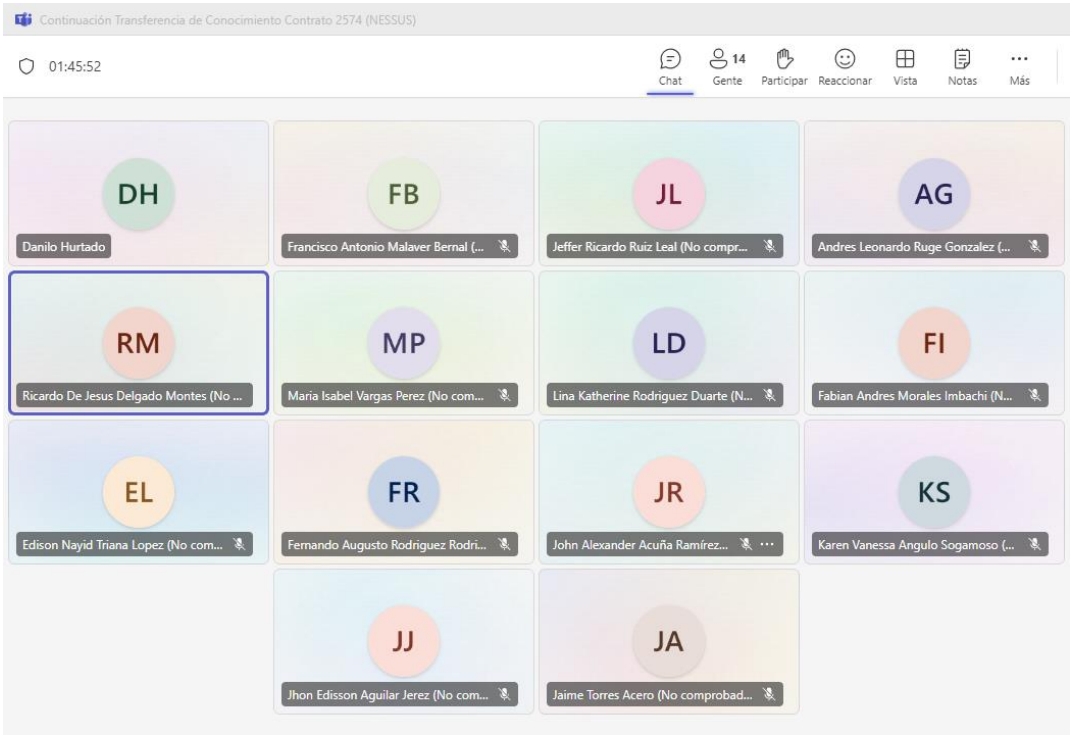
3.2 Configuración y Puesta en Funcionamiento

Configuración Inicial: se realizó el registro y activación de las licencias en el sistema, se realizaron configuración de políticas de escaneo conforme a los requerimientos del cliente.



Pruebas Funcionales: se realizó escaneos de prueba para validar el correcto funcionamiento, resolución de incidentes detectados durante la fase de pruebas.

Capacitación: Se brindó una sesión de capacitación para los usuarios designados, cubriendo temas como: Uso del panel de Nessus Professional. Creación y programación de escaneos.Generación de reportes.



3.3 Acuerdos de Nivel de Servicio (SLA)

Plan de Soporte Avanzado con tenable

	Advanced
Support Hours	24x7x365
Initial Response Times	P1-Critical: < 2 hr P2-High: < 4 hr P3-Medium: < 12 hr P4-Informational: < 24 hr
Email Support	-
Portal Support	Yes
Chat Support	Yes
Phone Support	Yes

Gravedad del problema: El tiempo de respuesta inicial se prioriza en función de la gravedad de la incidencia. Las incidencias de gravedad crítica deben abrirse por teléfono o chat para que se apliquen los objetivos de tiempo de respuesta inicial.

P1 - Crítico
Funcionalidad del producto completamente degradada - impacto crítico en las operaciones de negocio
P2 - Alta
Funcionalidad del producto severamente degradada - impacto severo en las operaciones de negocio
P3 - Medio
Errores/problemas generales - el producto se ve afectado, pero las operaciones de la empresa siguen siendo funcionales
P4 - Informativo
Información básica o asistencia con los productos de Tenable - poco o ningún impacto en las operaciones de la empresa

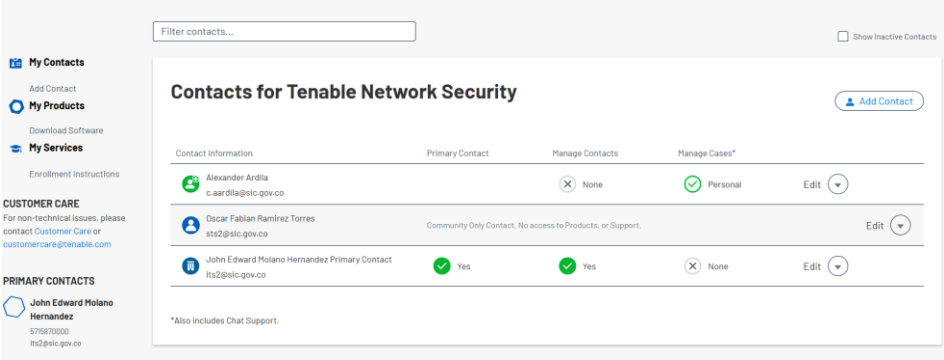
4 PROTOCOLO DE ESCALAMIENTO

4.1 Comunidad Tenable

Todos los contactos designados con un contrato de asistencia válido pueden abrir un caso de asistencia en la plataforma de Tenable iniciando sesión. La Comunidad contiene la Base de Conocimientos, documentación e información sobre licencias y un botón para iniciar una sesión de chat en vivo. El contacto de soporte principal también puede añadir/eliminar contactos de soporte utilizando la Comunidad.

4.2 Asistencia por chat

La asistencia por chat está disponible 24 horas al día, 365 días al año. La función de chat está disponible una vez que un contacto designado ha iniciado sesión en la Comunidad de Tenable.



4.3 Apertura para Soporte

Para apertura de casos solo lo podrá realizar el contacto principal desde su sesión en https://www.tenable.com/support . Los contactos de asistencia deben hablar inglés y realizar las solicitudes de asistencia en inglés. Los contactos de asistencia deben proporcionar la información razonablemente solicitada por Tenable con el fin de resolver una solicitud de asistencia Nativo.

5 RECOMENDACIONES

Al trabajar con Nessus a gran escala o en entornos únicos, puede resultar complicado equilibrar el tiempo de escaneo, el uso de recursos de destino y la eficacia de la evaluación, por tal razon se debe abordar algunas configuraciones comunes que puede utilizar para optimizar los tiempos de escaneo y reducir la carga en los destinos de escaneo y la infraestructura de red.

El primer elemento que se debe tener en cuenta es el método de análisis o evaluación adecuado para su objetivo. Los distintos tipos de sistemas requieren distintos métodos de evaluación y existen diferentes objetivos al realizar un análisis de host o red, entre ellos:

- Escanee una red grande y vea qué hosts hay en ella.
- Evaluar las estaciones de trabajo de los usuarios remotos en busca de vulnerabilidades.
- Revise la configuración de Apache comparándola con una línea base de seguridad.
- Asegúrese de que no se agreguen sistemas a una red sensible que estén fuera del control de cambios.

Cada uno de estos escenarios podría utilizar la misma configuración básica, pero como cada entorno de TI es único, comprender la forma de optimizar cada uno hará que su programa sea más efectivo

A la hora de explorar la forma más eficaz de realizar una evaluación, escanear varios sistemas simultáneamente no siempre es la mejor opción. El hecho de que la herramienta sea capaz de alcanzar un determinado umbral no significa que deba utilizarse al máximo.

Tenga en cuenta lo siguiente:

- Si el tráfico de red de su escaneo pasa por un solo cuello de botella, esa infraestructura de red puede verse abrumada por la cantidad de hosts que se evalúan en un momento dado.
- Los análisis en hosts que comparten la misma infraestructura subyacente, como recursos de almacenamiento o de procesamiento, pueden saturar esos sistemas si se inician demasiadas evaluaciones al mismo tiempo.
- Algunas comprobaciones consultarán otras infraestructuras locales o de Internet como parte de la evaluación. Esto puede sobrecargar la infraestructura con conexiones adicionales o consultar los sistemas que no se están evaluando explícitamente.

Las configuraciones de escaneo predeterminadas para evaluaciones simultáneas de objetivos de escaneo son suficientes para la mayoría de los casos de uso. Sin embargo, esto se puede ampliar para aumentar el rendimiento o reducir para reducir el impacto en la infraestructura. Existen otras opciones dentro de las configuraciones de escaneo para abordar problemas específicos, como:

- Escalonar los tiempos de lanzamiento del escaneo para los agentes de Nessus
- Aleatorizar el orden en el que se escanean las IP
- Disminuya la velocidad del escaneo cuando se detecte congestión en la red

SIC:		
Nombre/Cargo	Firma	Fecha
MCO GLOBAL:		
Nombre/Cargo	Firma	Fecha
Danilo Hurtado – INGENIERO ELECTRONICO		Noviembre 2024

LUIS EDUAR CUESTA TAUTIVA

OSCAR FABIAN RAMIREZ TORRES