Instructivo de Trabajo:
INSTALACIÓN DE SERVIDOR DE ANTIVIRUS
(ME-I-ITR-RM- ISA-33)
Versión 01

Aprobado por:	Cargo:	Fecha	Firma
Lic. Giovanni Verbena de León	Viceministro de Inversión y Competencia	5/8/16	

Revisado por:	Cargo:	Fecha	Firma
Lic. Rodrigo Valladares Molina	Registrador Mercantil	22/7/16	

Elaborado por:	Cargo:	Fecha	Firma
Ricardo Antonio Chinchilla Sandoval	Técnico Informático	21/7/16	

Rige a partir de: 05 AGO 2016

Índice de contenido			Hoja

1 OBJETIVO:

La presente Guía Técnica tiene por finalidad describir la manera de instalar el servidor de antivirus en el Data Center del Registro Mercantil y su configuración, considerando de igual manera a los clientes (Computadoras Personales).

2 ALCANCE:

Esta guía será de uso exclusivo del o los Técnicos Informáticos que conformar el Departamento de Informática.

3 RESPONSABILIDADES:

3.1 El Jefe del Departamento de Informática, es responsable de:

3.1.1 Planificar y solicitar los recursos Humanos técnicos y financieros necesarios para contar con los recursos básicos para el buen cumplimiento de este manual.

3.1.2 Realizar las pruebas del buen funcionamiento del Software para garantizar un buen desempeño al momento de ejecutarlo los operadores registrales.

4 DOCUMENTOS Y/O DATOS RELACIONADOS:

Esta Guía Técnica no cuenta con Documentos Relacionados

5 DEFINICIONES:

5.1 Instalación: Es el Proceso por el cual nuevos programas son transferidos a un computador con el fin de ser configurados y preparados para ser ejecutados en el sistema informático para cumplir la función para la cual fueron desarrollados.

5.2 Antivirus: Programa diseñado para evitar la intrusión de virus cibernéticos a un computador o servidor.

5.3 Hardware: Es la parte física que conforma un computador o dispositivo informático.

5.4 IP: Es un número que identifica, de manera lógica y jerárquica, a una interfaz o dirección lógica en una red de computadoras.

5.5 Copia de Seguridad: Es el proceso de realizar una copia de una parte o total de un dispositivo de almacenamiento a otro, por motivos de resguardo o cuidado de la integridad de la misma.

5.6 Servidor Proxy: Es un ordenador que sirve de intermediario entre un navegador web e Internet. El proxy contribuye a la seguridad de la red.

5.7 URL: Un localizador de recursos uniforme LRU (más conocido por la sigla URL, del inglés *Uniform Resource Locator*) es un identificador de recursos uniforme

5.8 Código Malicioso: es código informático que provoca infracciones de seguridad para dañar un sistema informático. es código informático que provoca infracciones de seguridad para dañar un sistema informático.

5.9 POP3: En informática se utiliza el Post Office Protocol (POP3, Protocolo de Oficina de Correo o "Protocolo de Oficina Postal") en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto, denominado Servidor POP. Es un protocolo de nivel de aplicación en el Modelo OSI.

5.10 MAPI: (Mail API) Interfaz de programación que permite que una aplicación envíe y reciba correo através del sistema de mensajería Microsoft Mail. El MAPI simple es un subconjunto de MAPIque incluye una docena de funciones para enviar y recuperar correspondencia.

5.11 IMAP: Internet Message Access Protocol (IMAP, Protocolo de acceso a mensajes de internet), es un protocolo de aplicación que permite el acceso a mensajes almacenados en un servidor de Internet. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet

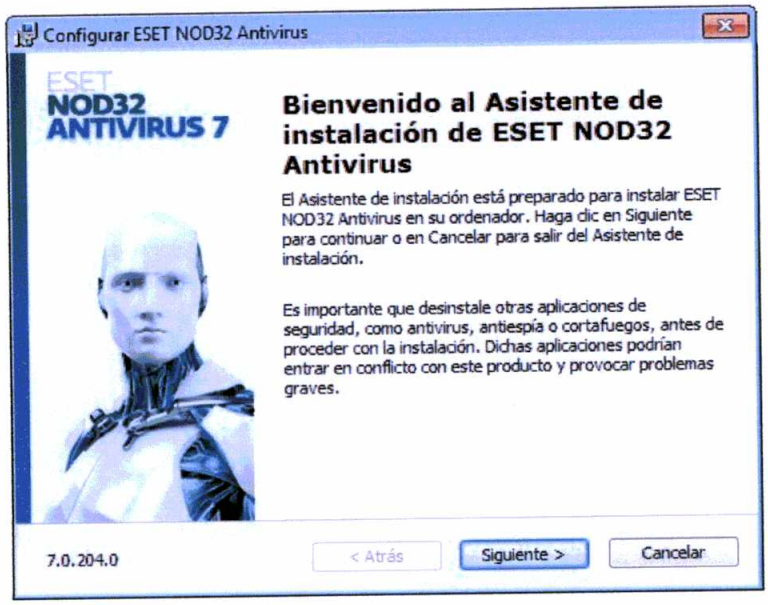
5.12 HTTPS: Hypertext Transfer Protocol Secure (ó HTTPS) es una combinación del protocoloHTTP y protocolos criptográficos. Se emplea para lograr conexiones más seguras en la WWW, generalmente para transacciones de pagos o cada vez que se intercambie información sensible (por ejemplo, claves) en internet.

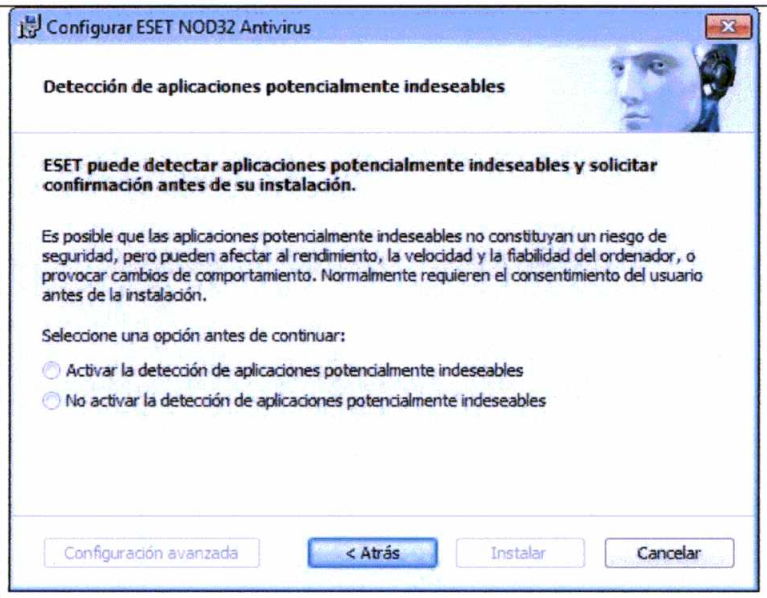
6. PROCEDIMIENTO Y/O INSTRUCTIVO:

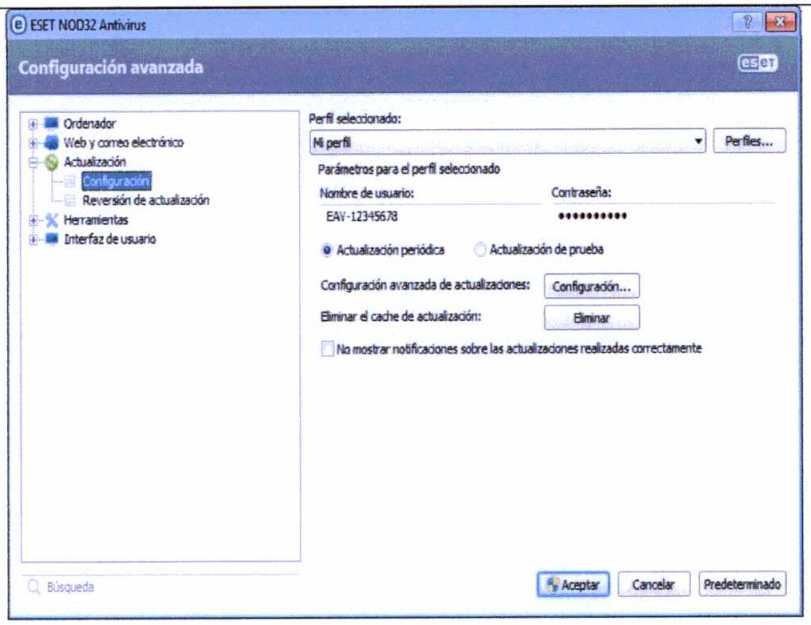
Responsable	Procedimiento	Tiempo
Técnico Informático	**Requisitos para su Instalación:** Para un funcionamiento óptimo de ESET NOD32 Antivirus, el sistema debería cumplir con los siguientes requisitos de hardware y software, ya que el Registro Mercantil cuenta aún con computadoras con sistema operativo XP y W7 se colocan las características. **Microsoft® Windows® XP** 600 MHz 32 bits (x86)/64 bits (x64) 128 MB RAM de memoria del sistema 320 MB de espacio disponible Super VGA (800 x 600) **Microsoft® Windows® 8.1, 8, 7, Vista, Server 2003 o Superior** 1 GHz 32 bits (x86)/ 64 bits (x64) 512 MB RAM de memoria del sistema	5 Minutos

	320 MB de espacio disponible Super VGA (800 x 600)	
Técnico Informático	**Consideraciones Importantes para la Instalación de su Servidor de ESET o en su Computador Personal** **Prevención** Cuando trabaja con el ordenador y, especialmente, cuando navega por Internet, tenga en cuenta que ningún sistema antivirus del mundo puede eliminar completamente el riesgo de amenazas y ataques. Para disfrutar de una protección y una comodidad máximas, es esencial usar correctamente su solución antivirus y cumplir varias reglas útiles: **Actualización regular** De acuerdo con las estadísticas cada día se crean miles de nuevas amenazas únicas para burlar las medidas de seguridad existentes y proporcionar un beneficio a sus autores, todo ello a costa de otros usuarios. Para garantizar la máxima eficacia de estas actualizaciones es importante que estén bien configuradas en el sistema. **Descarga de parches de seguridad** Es importante descargar estas actualizaciones de seguridad a medida que se publican. Microsoft Windows y los navegadores web como Internet Explorer son dos ejemplos de programas que publican de forma periódica actualizaciones de seguridad. **Copia de seguridad de los datos importantes** Es importante realizar copias de seguridad periódicas de sus datos importantes y confidenciales en una fuente externa, como un DVD o un disco duro externo. Estas precauciones facilitan y aceleran la recuperación de los datos en caso de fallo del sistema. **Análisis regular del ordenador en busca de virus** El módulo de protección del sistema de archivos en tiempo real se encarga de la detección de los virus, gusanos, troyanos y rootkits, conocidos o no. Esto significa que cada vez que entra en un archivo o lo abre, este se analiza en busca de actividad de código malicioso. Se Recomienda que realice un análisis completo del ordenador al menos una vez al mes, ya que las firmas de códigos maliciosos pueden variar y la base de firmas de virus se actualiza todos los	30 Minutos

	días.	
Técnico Informático	**Instalación** Ya que la distribución de las licencias ya no son físicas ósea CD'S O DVD'S, este programa deberá ser descargado de la página del Proveedor y se ingresara la Clave que fuera proporcionada por el proveedor local del programa. El **Live installer** se puede descargar del sitio web de ESET. Este paquete de instalación es universal para todos los idiomas (elija el idioma Español). **Live installer** es un pequeño archivo, los archivos adicionales que necesite para instalar ESET NOD32 Antivirus se descargarán automáticamente.	15 Minutos
Técnico Informático	**Live installer** Cuando haya descargado el paquete de instalación de Live installer, haga doble clic en el archivo de instalación y siga las instrucciones paso a paso de la ventana del instalador. Importante: Para este tipo de instalación debe estar conectado a Internet.  Seleccione el idioma Español y haga clic en Instalar. Los archivos de instalación tardarán unos momentos en descargarse. .	10 Minutos
Técnico Informático	El paso siguiente del proceso de instalación consiste en configurar la detección de aplicaciones potencialmente indeseables. Las aplicaciones potencialmente indeseables no tienen por qué ser maliciosas, pero pueden influir negativamente en el	10 Minutos

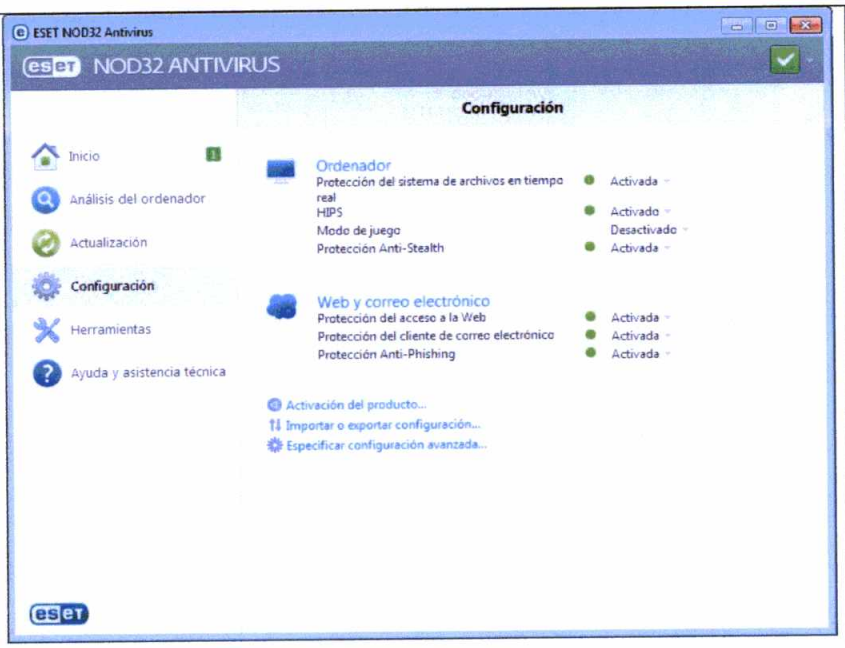
	comportamiento del sistema operativo. Consulte el capítulo Aplicaciones potencialmente indeseables para ver más detalles.  Haga clic en Siguiente para iniciar el proceso de instalación	
Técnico Informático	Primero, el programa comprueba si hay una versión más reciente de ESET NOD32 Antivirus y, si se encuentra una versión más reciente, se le notificará en el primer paso del proceso de instalación. Si selecciona la opción Descargar e instalar la nueva versión, se descargará la nueva versión y el proceso de instalación continuará. Esta casilla de verificación solo está visible cuando hay disponible una versión más reciente que la versión que está instalando.	5 Minutos

	 Esta configuración proporciona un nivel de seguridad excelente, es fácil de configurar y permite un elevado rendimiento del sistema. **Configuración avanzada** está diseñada para usuarios que tienen experiencia en el ajuste de programas y que desean modificar opciones avanzadas durante la instalación. Haga clic en **Instalar** para iniciar el proceso de instalación y omitir la configuración avanzada.	
Técnico Informático	**Configuración avanzada** Después de seleccionar Configuración avanzada, se le pedirá que seleccione una ubicación para la instalación. De forma predeterminada, el programa se instala en el directorio siguiente: **C:\Archivos de programa\ESET\ESET NOD32 Antivirus**	10 Minutos



Para configurar la conexión a Internet. Si utiliza un servidor Proxy, este debe estar configurado correctamente para que las actualizaciones de la base de firmas de virus funcionen correctamente. Si no está seguro de si utiliza un servidor proxy para conectarse a Internet, seleccione Usar las mismas características establecidas para Internet Explorer (recomendado).

Para configurar el servidor Proxy, seleccione Conexión mediante servidor Proxy y haga clic en Siguiente. Introduzca la dirección IP o URL de su servidor Proxy en el campo Dirección. En el campo Puerto, especifique el puerto donde el servidor Proxy acepta conexiones (3128 de forma predeterminada). En el caso de que el servidor Proxy requiera autenticación, debe introducir un nombre de usuario y una contraseña válidos que permitan acceder al servidor Proxy. La configuración del servidor Proxy también se puede copiar de Internet Explorer, si se desea Para ello, haga clic en Aplicar y confirme la selección.

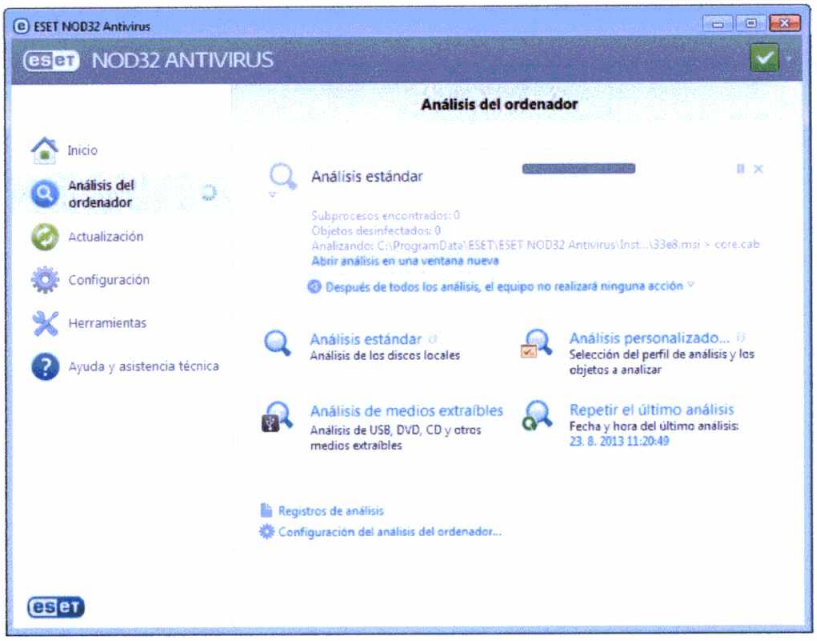


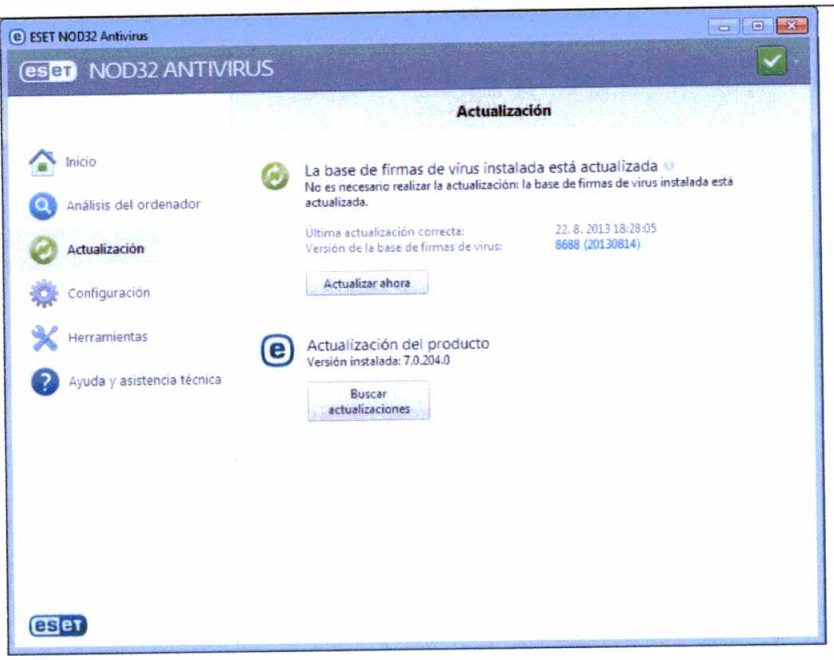
Si no desea que se actualicen los componentes del programa, seleccione Nunca actualizar los componentes del programa. Seleccione Avisar antes de descargar componentes del programa para ver una ventana de confirmación cada vez que el sistema intente descargar los componentes del programa. Para descargar las actualizaciones de componentes del programa de forma automática, seleccione Actualizar siempre los componentes del programa.

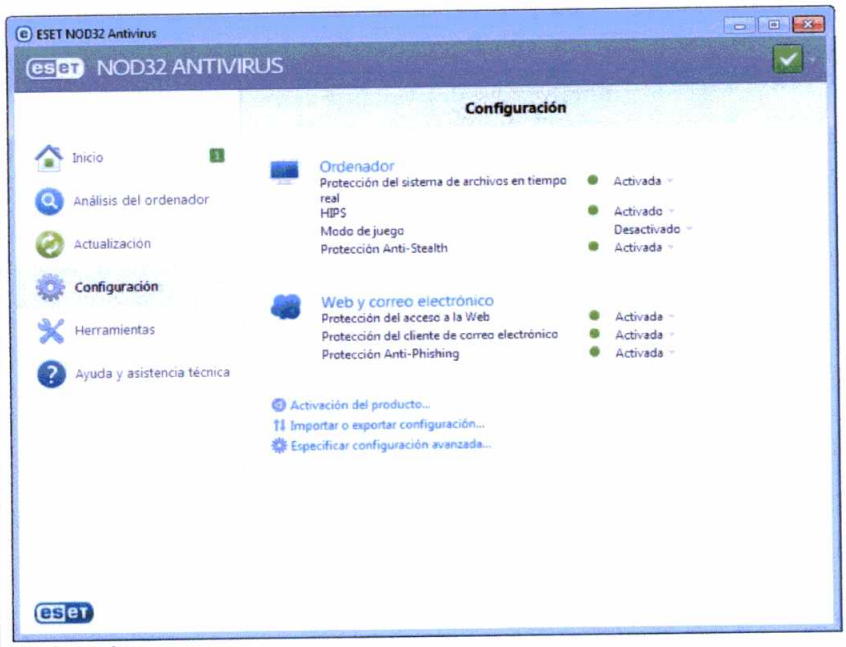
NOTA: normalmente, después de actualizar componentes del programa, es necesario reiniciar el ordenador. Le recomendamos que seleccione Si es necesario, reiniciar el ordenador sin avisar.

En la próxima ventana de instalación tiene la opción de definir una contraseña para proteger la configuración del programa. Seleccione Proteger la configuración con contraseña e introduzca la contraseña en los campos Contraseña nueva y Confirmar contraseña. Necesitará esta contraseña para acceder a la configuración de ESET NOD32 Antivirus o cambiarla. Si ambos campos coinciden, haga clic en Siguiente para continuar.

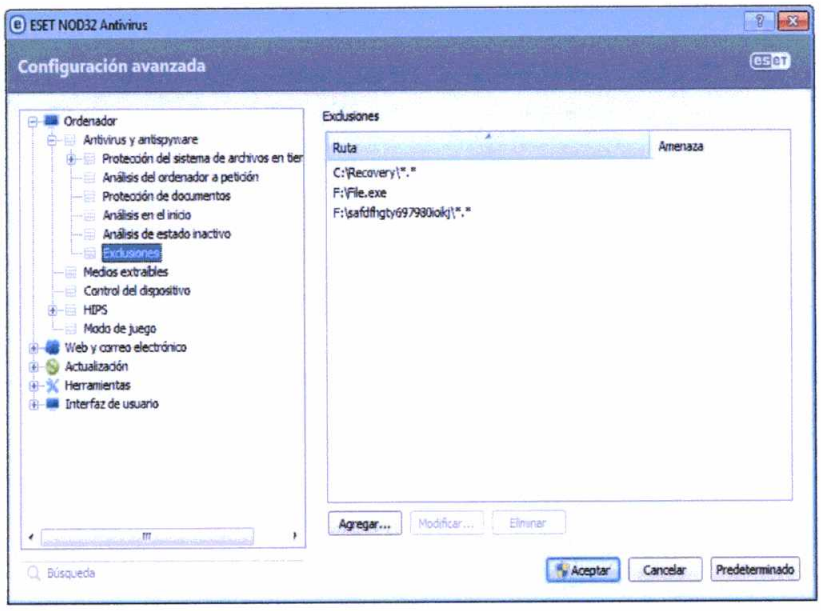
Para desactivar la operación de Analizar primero tras la instalación que se suele realizar cuando la instalación finaliza para comprobar si existe código malicioso, anule la selección de la casilla de verificación situada junto a Activar análisis tras la instalación. Haga clic en Instalar, en la ventana Preparado para instalar, para completar la instalación.

Técnico Informático	**Analizar primero tras la instalación** Después de instalar ESET NOD32 Antivirus, un análisis del ordenador comenzará 20 minutos después de la instalación o del reinicio del ordenador para comprobar si existe código malicioso. También puede iniciar un análisis del ordenador manualmente desde la ventana principal del programa haciendo clic en Análisis del ordenador > Análisis estándar. Encontrará más información sobre los análisis del ordenador en la sección Análisis del ordenador. 	20 Minutos
Técnico Informático	**Actualizaciones** La actualización de la base de firmas de virus y la actualización de componentes del programa son partes importantes a la hora de proteger su sistema frente a código malicioso. Preste especial atención a su configuración y funcionamiento. En el menú principal, haga clic en Actualizar y, a continuación, en Actualizar ahora para comprobar si hay alguna actualización de la base de firmas de virus. Si no ha introducido el nombre de usuario y la contraseña durante la activación de ESET NOD32 Antivirus, se le pedirá que lo haga ahora.	15 Minutos

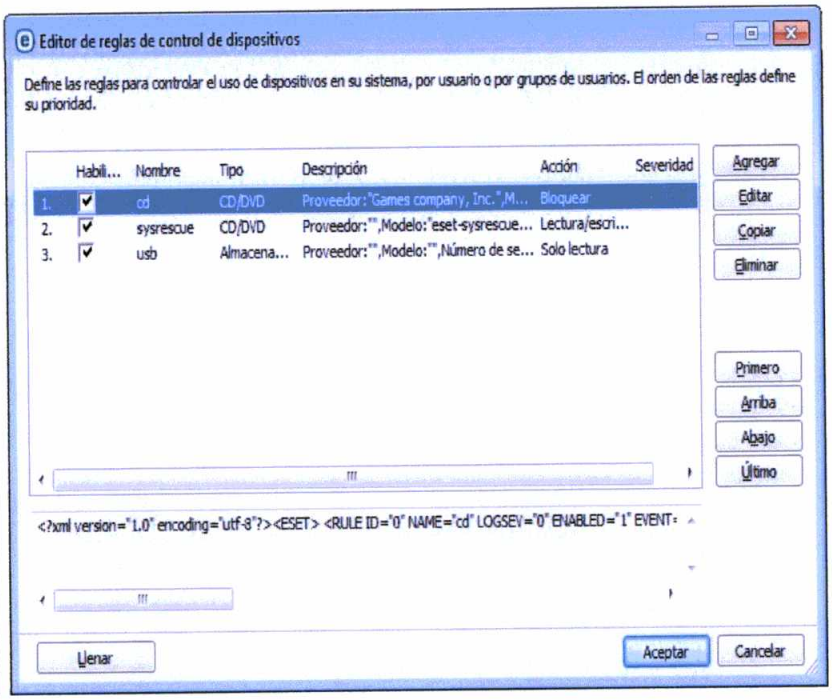


Técnico Informático	El menú Configuración incluye las siguientes opciones:  Ordenador Web y correo electrónico	10 Minutos

	Haga clic en cualquier componente para ajustar la configuración avanzada del correspondiente módulo de protección. La configuración de protección de Ordenador le permite activar o desactivar los siguientes componentes: **Protección en tiempo real del sistema de archivos:** todos los archivos se analizan en busca de código malicioso en el momento de abrirlos, crearlos o ejecutarlos en el ordenador. **HIPS:** el sistema HIPS controla los sucesos del sistema operativo y reacciona según un conjunto de reglas personalizado. **Modo jugador:** activa o desactiva el modo jugador. Cuando se active el modo de juego, recibirá un mensaje de alerta (posible riesgo de seguridad) y la ventana principal se volverá naranja. **Protección Anti-Stealth:** detecta programas peligrosos, como rootkits, que se ocultan del sistema operativo y las técnicas de análisis ordinarias. La configuración de protección de Web y correo electrónico le permite activar o desactivar los siguientes componentes: Protección del tráfico de Internet: si esta opción está activada, se analiza todo el tráfico a través de HTTP o HTTPS para detectar la presencia de software malicioso. Protección del cliente de correo electrónico: supervisa comunicaciones recibidas a través de los protocolos POP3 e IMAP. Protección Anti-Phishing: filtra los sitios web sospechosos de distribuir contenido destinado a manipular a los usuarios para que envíen información confidencial. Para volver a activar la protección del componente de seguridad desactivado, haga clic en Desactivado y luego en Activar.	
Técnico Informático	**Exclusiones** Las exclusiones le permiten excluir archivos y carpetas del análisis. Para garantizar que se analizan todos los objetos en busca de amenazas, le recomendamos que solo cree exclusiones cuando sea absolutamente necesario. No obstante, puede que haya situaciones en las que necesite excluir un objeto, como por ejemplo entradas de una base de datos grande que ralenticen el ordenador durante el análisis o software que entre en conflicto con el análisis.	10 Minutos

	Para excluir un objeto del análisis: 1. Haga clic en Agregar..., 2. Escriba la ruta de un objeto o selecciónelo en la estructura de árbol. Puede utilizar comodines para abarcar un grupo de archivos. El signo de interrogación (?) representa un carácter único variable y el asterisco (*), una cadena variable de cero o más caracteres. **Ejemplos:** Si desea excluir todos los archivos de una carpeta, escriba la ruta a la carpeta y utilice la máscara "*.*". Para excluir una unidad entera incluidos archivos y subcarpetas, utilice la máscara "D:*". Si desea excluir únicamente los archivos .doc, utilice la máscara "*.doc". Si el nombre de un archivo ejecutable tiene un determinado número de caracteres (y los caracteres varían) y solo conoce con seguridad el primero (por ejemplo, "D"), utilice el siguiente formato: "D????.exe". Los símbolos de interrogación sustituyen a los caracteres que faltan (desconocidos).  	
Técnico Informático	**Reglas de control de dispositivos** La ventana Editor de reglas de control de dispositivos muestra las reglas existentes para dispositivos externos que los usuarios	10 Minutos

conectan al ordenador y permite controlarlos de forma precisa.

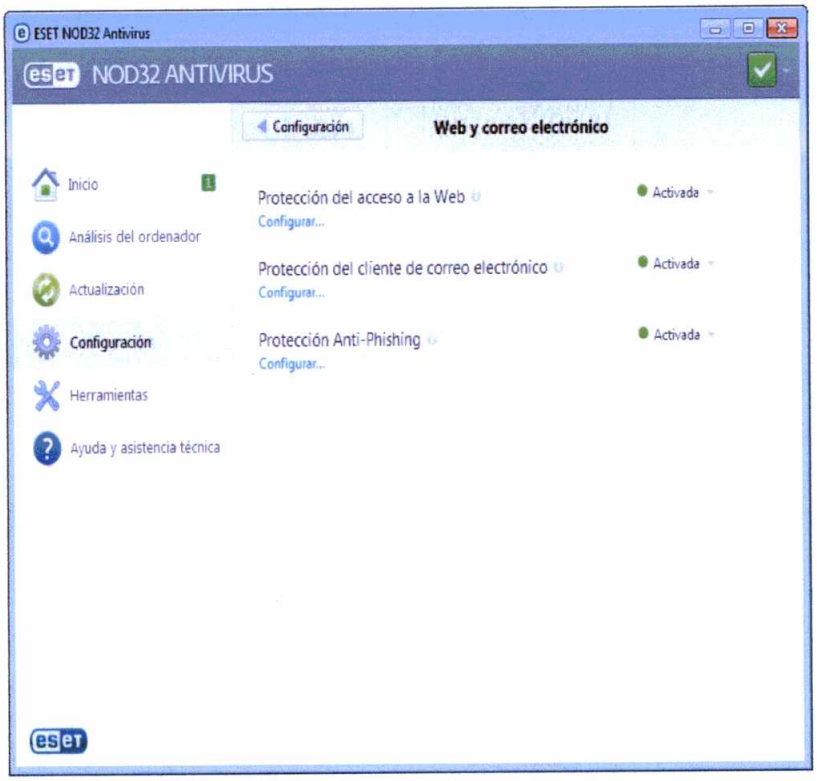


Determinados dispositivos se pueden permitir o bloquear por usuario o por grupo de usuarios y según parámetros adicionales del dispositivo que se pueden especificar en la configuración de las reglas. La lista de reglas contiene varias descripciones de una regla, como el nombre, el tipo de dispositivo externo, la acción que debe realizarse tras conectar un dispositivo externo al ordenador y la gravedad del registro.

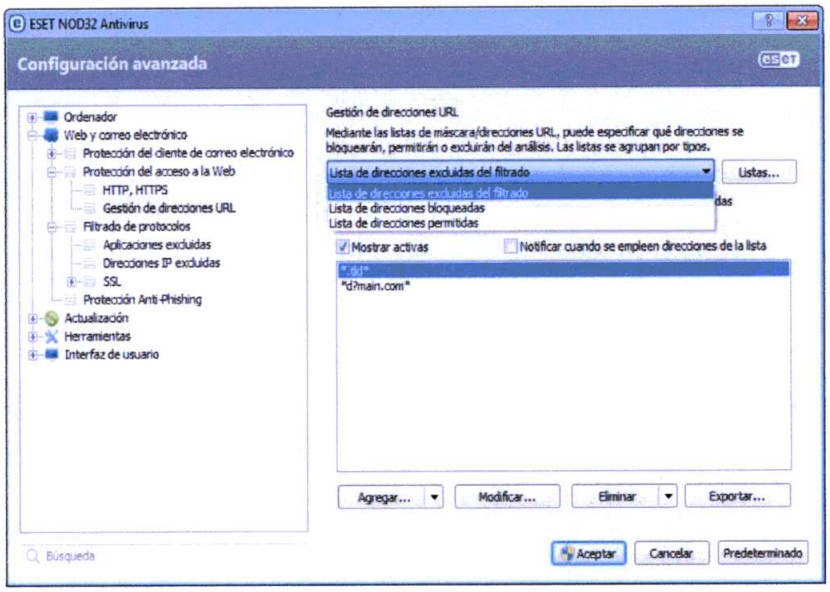
Haga clic en Agregar o en Modificar para administrar una regla. Haga clic en Copiar para crear una nueva regla con opciones predefinidas utilizadas para otra regla seleccionada. Las cadenas XML que se muestran al hacer clic en una regla se pueden copiar en el portapapeles para ayudar a administradores de sistemas a exportar o importar datos y utilizarlos; por ejemplo en ESET Remote Administrator.

Al mantener pulsado CTRL y hacer clic, puede seleccionar varias reglas y aplicar acciones, como eliminarlas o moverlas hacia arriba o hacia abajo en la lista, a todas las reglas seleccionadas. La casilla de verificación Activado desactiva o activa una regla; puede ser útil si no desea eliminar una regla de forma permanente, por si decide utilizarla en el futuro.

El control se efectúa mediante reglas que se clasifican en el orden

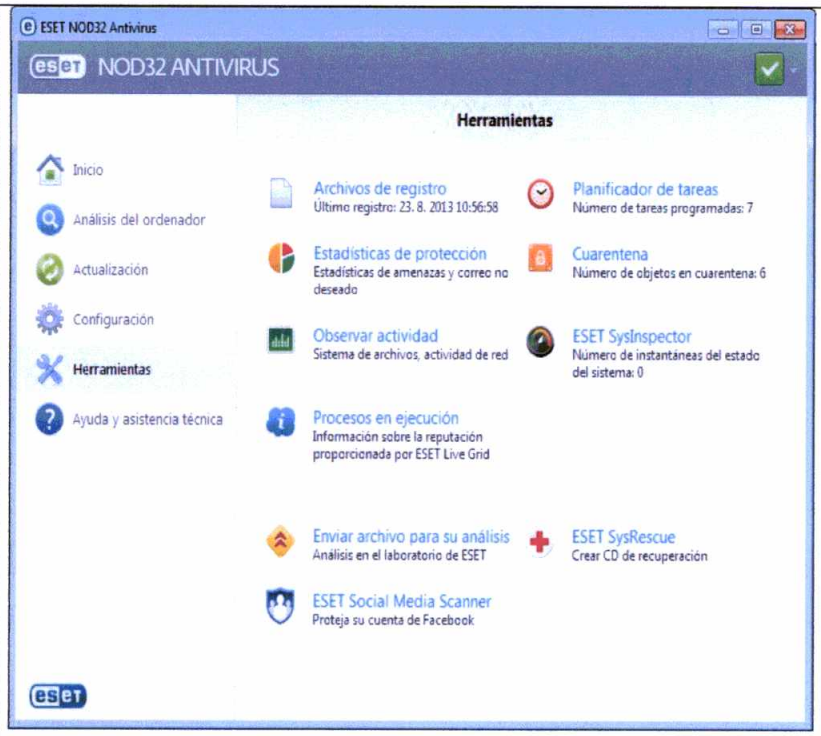
	que determina su prioridad, situándose al principio las reglas con la prioridad más alta. Puede hacer clic con el botón derecho en una regla para mostrar el menú contextual. Aquí puede definir el nivel de detalle (gravedad) de las entradas de registro de una regla. Las entradas de registro se pueden ver desde la ventana principal de ESET NOD32 Antivirus en Herramientas > Archivos de registro. Haga clic en Llenar para rellenar automáticamente los parámetros del medio extraíble conectado a su ordenador.	
Técnico Informático	Web y correo electrónico Puede consultar la configuración web y del correo electrónico en el panel Configuración haciendo clic en Web y correo electrónico. Desde aquí puede acceder a configuraciones más detalladas del programa.  La conectividad de Internet es una característica estándar de cualquier ordenador personal. Lamentablemente, también se ha convertido en el principal medio de transferencia de código malicioso. Por eso, es fundamental prestar la debida atención a la protección del tráfico de Internet.	10 Minutos

	Haga clic en Configurar para abrir opciones de protección de web/correo electrónico/anti-phishing en la configuración avanzada. Protección del cliente de correo electrónico proporciona control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3 e IMAP. Con el programa de complemento para su cliente de correo electrónico, ESET NOD32 Antivirus ofrece control de todas las comunicaciones realizadas a y desde el cliente de correo electrónico (POP3, MAPI, IMAP, HTTP). Protección Anti-Phishing le permite bloquear páginas web conocidas por distribuir contenido de phishing. Le recomendamos encarecidamente que deje Anti-Phishing activado. Puede desactivar temporalmente el módulo de protección de web/correo electrónico/anti-phishing haciendo clic en Activado.	
Técnico Informático	**Gestión de direcciones URL** En esta sección puede especificar las direcciones HTTP que desea bloquear, permitir o excluir del análisis. Agregar, Modificar, Quitar y Exportar se utilizan para gestionar las listas de direcciones. No se podrá acceder a los sitios web de la lista de direcciones bloqueadas. Se puede acceder a los sitios web de la lista de direcciones excluidas sin analizarlos en busca de código malicioso. Si selecciona Permitir el acceso solo a las direcciones URL de la lista de direcciones permitidas, solo se podrá acceder a las direcciones presentes en la lista de direcciones permitidas; todas las demás direcciones HTTP se bloquearán. Si añade una dirección URL a la Lista de direcciones excluidas del filtrado, esta dirección se excluirá del análisis. También puede permitir o bloquear determinadas direcciones añadiéndolas a la Lista de direcciones permitidas o Lista de direcciones bloqueadas. Haga clic en Listas... para abrir la ventana Listas de máscaras/direcciones HTTP en la que puede agregar o quitar listas de direcciones. Para poder agregar direcciones URL HTTPS a la lista, la opción Analizar siempre el protocolo SSL debe estar seleccionada. En todas las listas, pueden utilizarse los símbolos especiales * (asterisco) y ? (signo de interrogación). El asterisco sustituye a cualquier cadena de caracteres y el signo de interrogación, a cualquier símbolo. Tenga especial cuidado al especificar direcciones excluidas, ya que la lista solo debe contener direcciones seguras y de confianza. Del mismo modo, es necesario asegurarse de que los símbolos * y ? se utilizan correctamente en esta lista. Para activar una lista, seleccione la opción Lista activa. Si desea que le notifiquen cuando se introduzca una dirección de la lista actual, seleccione Notificar cuando se empleen direcciones de la lista.	10 Minutos

	 **Agregar/Desde archivo:** le permite agregar una dirección a la lista, bien manualmente (haga clic en Agregar) o bien desde un archivo de texto sencillo (haga clic en Desde archivo). La opción Desde archivo le permite agregar varias máscaras/direcciones URL, que se guardan en un archivo de texto. **Modificar:** permite modificar direcciones manualmente; por ejemplo agregando una máscara ("*" y "?"). **Quitar/Quitar todo:** haga clic en Quitar para quitar la dirección seleccionada de la lista. Para eliminar todas las direcciones, seleccione Quitar todo. **Exportar:** le permite guardar direcciones de la lista actual en un archivo de texto sencillo.	
Técnico Informático	**Agregar dirección IPv4** Esta opción le permite agregar una dirección IP, un intervalo de direcciones o una subred de un punto remoto al que se aplica la regla. El protocolo de Internet versión 4 es el más antiguo, pero sigue siendo el más utilizado. Dirección única: agrega la dirección IP de un ordenador individual al que debe aplicarse la regla (por ejemplo, 192.XXX.X.XX). Rango de direcciones: especifique las direcciones IP inicial y final para delimitar el intervalo de direcciones (de varios ordenadores) al que se aplicará la regla (por ejemplo, de 192.XXX.X.1 a	15 Minutos

	192.XXX.X.99). Subred: grupo de ordenadores definido por una dirección IP y una máscara. Por ejemplo, 255.255.255.0 es la máscara de red del prefijo 192.168.1.X/24 (es decir, el intervalo de direcciones de 192.168.1.X a 192.168.X.254). **Agregar dirección IPv6** Esta opción le permite agregar una dirección IPv6 o una subred de un punto remoto al que se aplica la regla. Esta es la versión más reciente del protocolo de Internet, que sustituirá a la versión 4 anterior. Dirección única: agrega la dirección IP de un ordenador individual al que debe aplicarse la regla, (por ejemplo, 2001:718:1c01:16:214:22ff:fec9:ca5). Subred: grupo de ordenadores definido por una dirección IP y una máscara (por ejemplo: 2002:c0a8:6301:1::1/64).	
Técnico Informático	**Certificados de confianza** Además del archivo de autoridades certificadoras de confianza integrado, donde ESET NOD32 Antivirus almacena los certificados de confianza, puede crear una lista personalizada de certificados de confianza. Esta lista se puede ver en Configuración avanzada (F5) > Web y correo electrónico > Filtrado de protocolos > SSL > Certificados > Certificados de confianza. ESET NOD32 Antivirus utilizará los certificados de esta lista para comprobar el contenido de las comunicaciones cifradas. Para eliminar los elementos seleccionados de la lista, haga clic en Quitar. Haga clic en Mostrar (o haga doble clic en el certificado) para ver información sobre el certificado seleccionado. **Certificados excluidos** La sección Certificados excluidos contiene certificados que se consideran seguros. No se buscarán amenazas en el contenido de las comunicaciones cifradas que utilicen los certificados de la lista. Se recomienda excluir únicamente los certificados web que tengan una garantía de seguridad y cuya comunicación no sea necesario comprobar. Para eliminar los elementos seleccionados de la lista, haga clic en Quitar. Haga clic en Mostrar (o haga doble clic en el certificado) para ver información sobre el certificado seleccionado.	45 Minutos

	Conexión SSL cifrada Si el ordenador está configurado para análisis del protocolo SSL, es posible que se abra un cuadro de diálogo solicitándole que seleccione una acción cuando hay un intento de establecer una comunicación cifrada (utilizando un certificado desconocido). El cuadro de diálogo contiene la siguiente información: nombre de la aplicación que inició la comunicación y nombre del certificado utilizado. Si no se encuentra el certificado en el archivo de autoridades certificadoras de confianza, se considerará que no es de confianza. Están disponibles las siguientes acciones para certificados: Sí: el certificado se marca temporalmente como de confianza. No se mostrará la ventana de alerta en el siguiente intento de utilizar el certificado durante la sesión actual. Sí, siempre: marca el certificado como de confianza y lo agrega a la lista de certificados de confianza. No se mostrará ninguna ventana de alerta para los certificados de confianza. No: marca el certificado como de no confianza para la sesión actual. La ventana de alerta se mostrará en el siguiente intento de utilizar el certificado. Excluir: agrega el certificado a la lista de certificados excluidos y los datos transferidos a través del canal cifrado no se analizan.	
Técnico Informático	**Herramientas** El menú **Herramientas** incluye módulos que ayudan a simplificar la administración del programa y ofrece opciones adicionales para usuarios avanzados.	10 Minutos

		
Técnico Informático	**Accesos directos del teclado** Los accesos directos que se pueden utilizar en ESET SysInspector son: **Archivo** Ctrl + O abre el registro existente Ctrl + S guarda los registros creados **Generar** Ctrl + G genera una instantánea estándar del estado del ordenador Ctrl + H genera una instantánea del estado del ordenador que también puede registrar información confidencial **Filtrado de elementos** 1, O seguro, se muestran los elementos que tienen un nivel de riesgo de 1 a 9 2 seguro, se muestran los elementos que tienen un nivel de riesgo de 2 a 9 3 seguro, se muestran los elementos que tienen un nivel de riesgo de 3 a 9 4, U desconocido, se muestran los elementos que tienen	30 Minutos

un nivel de riesgo de 4 a 9
5 desconocido, se muestran los elementos que tienen un nivel de riesgo de 5 a 9
6 desconocido, se muestran los elementos que tienen un nivel de riesgo de 6 a 9
7, B peligroso, se muestran los elementos que tienen un nivel de riesgo de 7 a 9
8 peligroso, se muestran los elementos que tienen un nivel de riesgo de 8 a 9
9 peligroso, se muestran los elementos que tienen un nivel de riesgo de 9
- disminuye el nivel de riesgo
+ aumenta el nivel de riesgo
Ctrl + 9 modo de filtrado, nivel igual o mayor
Ctrl + 0 modo de filtrado, nivel igual únicamente

Ver

Ctrl + 5 ver por proveedor, todos los proveedores
Ctrl + 6 ver por proveedor, solo Microsoft
Ctrl + 7 ver por proveedor, todos los demás proveedores
Ctrl + 3 muestra todos los detalles
Ctrl + 2 muestra la mitad de los detalles
Ctrl + 1 visualización básica
Retroceso retrocede un espacio
Espacio avanza un espacio
Ctrl + W expande el árbol
Ctrl + Q contrae el árbol

Otros controles

Ctrl + T va a la ubicación original del elemento tras seleccionarlo en los resultados de búsqueda
Ctrl + P muestra información básica sobre un elemento Ctrl + A muestra toda la información sobre un elemento Ctrl + C copia el árbol del elemento actual
Ctrl + X copia elementos
Ctrl + B busca información en Internet acerca de los archivos seleccionados
Ctrl + L abre la carpeta en la que se encuentra el archivo seleccionado
Ctrl + R abre la entrada correspondiente en el editor de registros
Ctrl + Z copia una ruta de acceso a un archivo (si el elemento está asociado a un archivo) Ctrl + F activa el campo de búsqueda
Ctrl + D cierra los resultados de búsqueda
Ctrl + E ejecuta el script de servicio

	Comparación Ctrl + Alt + O abre el registro original/comparativo Ctrl + Alt + R cancela la comparación Ctrl + Alt + 1 muestra todos los elementos Ctrl + Alt + 2 muestra solo los elementos agregados, el registro mostrará los elementos presentes en el registro actual Ctrl + Alt + 3 muestra solo los elementos eliminados, el registro mostrará los elementos presentes en el registro anterior Ctrl + Alt + 4 muestra solo los elementos sustituidos (archivos incluidos) Ctrl + Alt + 5 muestra solo las diferencias entre registros Ctrl + Alt + C muestra la comparación Ctrl + Alt + N muestra el registro actual Ctrl + Alt + P abre el registro anterior **Varios** F1 ver ayuda Alt + F4 cerrar programa Alt + Shift + F4 cerrar programa sin preguntar Ctrl + I estadísticas de registro	

7. FLUJOGRAMA