Manual de Configuración de Máquina Virtuales (VirtualBox) y Safe Exam Browser (SEB) para Exámenes

Aplicación en Entornos Virtualizados y Controlados

Autor: Francisco Ortega Zamorano

Departamento: Lenguajes y Ciencias de la Computación

Universidad: Universidad de Málaga

Curso académico: 2025–2026

Versión del documento: v1.0

Fecha: 26 de enero de 2026

Resumen

Este manual describe los distintos niveles de configuración de *Safe Exam Browser (SEB)* aplicados a exámenes en el Campus Virtual, así como la preparación de máquinas virtuales y herramientas auxiliares para garantizar un entorno seguro, controlado y reproducible durante la realización de pruebas evaluables.

Introducción al uso de Safe Exam Browser (SEB) en el Campus Virtual

Safe Exam Browser (SEB) es una aplicación diseñada para la realización de exámenes en línea en entornos controlados, cuyo objetivo principal es garantizar la integridad de las pruebas y reducir las posibilidades de copia, fraude o uso indebido de recursos externos.

Mediante el uso de SEB, el alumnado accede al examen a través de un navegador específico que restringe de forma automática el funcionamiento habitual del sistema, creando un entorno seguro supervisado por el profesorado.

Durante la realización de una prueba con SEB, el sistema:

- Bloquea el acceso a páginas web no autorizadas.
- Impide el uso de aplicaciones externas, como herramientas de mensajería, captura de pantalla o grabación.
- Desactiva combinaciones de teclas habituales (Alt+Tab, Ctrl+Esc, etc.) que permiten cambiar de aplicación.
- Restringe determinadas funciones del sistema operativo que podrían comprometer el desarrollo correcto del examen.

El uso de SEB se integra plenamente con el Campus Virtual, de modo que el alumnado accede a las actividades evaluables desde la plataforma habitual, pero bajo las condiciones de seguridad definidas previamente por el profesorado.

No obstante, el grado de control y restricción del entorno de examen puede variar en función de las necesidades específicas de cada prueba, del tipo de contenidos evaluados y de las herramientas requeridas por el alumnado. Por este motivo, en este manual se presentan distintos niveles de configuración de SEB, organizados según su grado de complejidad y seguridad, que van desde entornos básicos con restricciones mínimas hasta escenarios avanzados basados en máquinas virtuales y control de red.

Cada nivel se describe de forma detallada, proporcionando las pautas necesarias para su correcta implantación en función del contexto de uso. De este modo, el profesorado puede seleccionar el nivel más adecuado para cada prueba, garantizando un equilibrio entre seguridad, usabilidad y fiabilidad del proceso de evaluación.

Nivel 1 – Examen básico con SEB

La configuración del examen se realiza a través del Campus Virtual, utilizando la herramienta de integración con *Safe Exam Browser (SEB)*, que proporciona un entorno de examen seguro sin necesidad de editar archivos de configuración.

Esta herramienta permite definir parámetros básicos de seguridad, así como especificar las aplicaciones permitidas y las URLs autorizadas, facilitando la preparación del examen por parte del profesorado.

En este nivel, SEB puede configurarse para:

- Permitir únicamente aquellas aplicaciones estrictamente necesarias para la realización del examen.
- Autorizar el acceso a determinadas URLs, que deben estar claramente indicadas en el enunciado o ser accesibles desde el propio Campus Virtual (por ejemplo, enlaces incluidos en la actividad).

Es importante tener en cuenta que todas las direcciones web permitidas deben estar explícitamente definidas, ya que el alumnado no podrá navegar libremente por Internet durante la prueba.

Limitaciones del examen básico

Este nivel presenta algunas restricciones importantes que deben considerarse antes de su utilización:

- No se deben permitir aplicaciones con acceso directo a Internet, ya que comprometerían la seguridad del entorno del examen.
- No es posible utilizar entornos de desarrollo o editores de programación con conectividad de red, como:
    - Visual Studio Code
    - Eclipse
    - La mayoría de los editores de programación modernos
- Las aplicaciones que permiten abrir archivos (lectores PDF, procesadores de texto, editores) pueden acceder al sistema de archivos del equipo, lo que posibilita la apertura de documentos almacenados en cualquier carpeta accesible para el alumnado.

Por este motivo, se recomienda limitar al máximo la autorización de este tipo de aplicaciones en el Nivel 1.

Configuración

Para acceder a la configuración del entorno Safe Exam Browser (SEB), es necesario crear previamente una tarea en el Campus Virtual siguiendo el procedimiento habitual.
Una vez creada la tarea, deben configurarse las opciones que se muestran numeradas en la Figura 1, que se describen a continuación:

1. **Activación del navegador de examen seguro**
   Activar la opción "Navegador de examen seguro". Al marcar esta opción, se despliegan automáticamente los parámetros específicos de configuración de SEB asociados a la tarea.
2. **Selección del modo de uso de SEB**
   En el apartado "Usar Safe Exam Browser (SEB)", se debe seleccionar la opción "Solo permitir esta tarea y las aplicaciones seleccionadas".
   Esta opción establece una configuración controlada desde el Campus Virtual, permitiendo al profesorado definir las URLs autorizadas y las aplicaciones permitidas durante el examen.

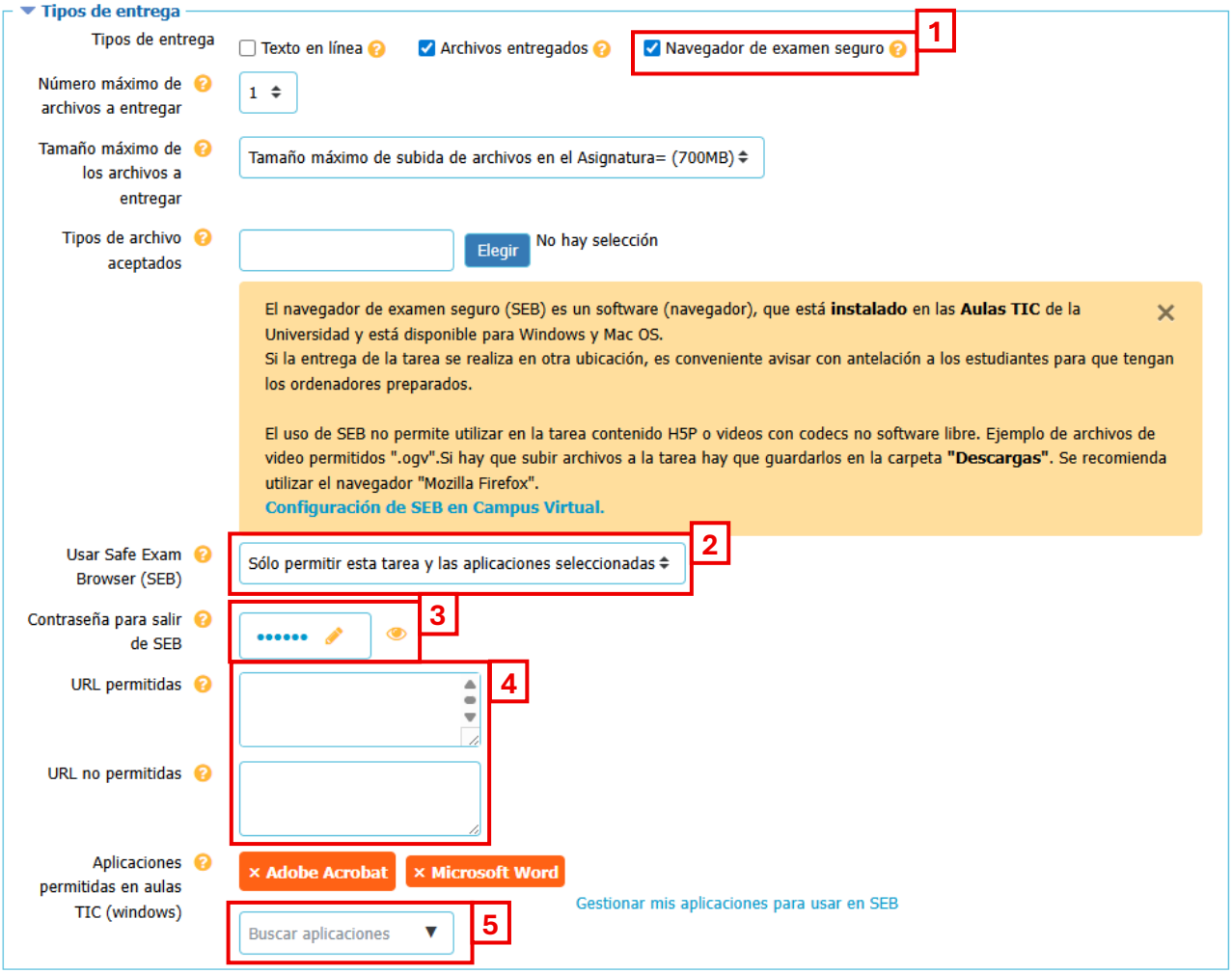

Fig. 1 Opciones de configuración de Safe Exam Browser (SEB) en una tarea del Campus Virtual.

3. **Definición de la contraseña de salida**
   En la opción "Contraseña para salir de SEB" se debe introducir una contraseña que permita cerrar el entorno seguro.
   Esta contraseña garantiza que el alumnado permanezca dentro del entorno de examen y solo pueda abandonarlo bajo autorización del profesorado, por ejemplo, ante incidencias técnicas o al finalizar la prueba.

4. **Configuración de URLs permitidas y no permitidas**
   En el apartado "URLs permitidas" se deben introducir todas aquellas direcciones web a las que el alumnado podrá acceder durante el examen.
   Estas URLs deben estar directamente relacionadas con la prueba y ser accesibles desde el enunciado o desde el propio Campus Virtual.
   De forma opcional, en "URLs no permitidas" pueden especificarse direcciones que se deseen bloquear explícitamente, reforzando las restricciones del entorno.

5. **Selección de aplicaciones permitidas**
   En el apartado "Aplicaciones permitidas en aulas TIC" se pueden seleccionar las aplicaciones que estarán disponibles durante el examen (por ejemplo, lectores PDF o procesadores de texto).
   Únicamente las aplicaciones seleccionadas estarán accesibles para el alumnado, permaneciendo bloqueado el resto del sistema.

Nivel 2 – Examen con SEB con navegación permitida en la asignatura del Campus Virtual

Este nivel está diseñado para exámenes en los que, además de las restricciones básicas de seguridad, resulta necesario permitir al alumnado el acceso controlado a los contenidos de la asignatura dentro del Campus Virtual.

Este nivel se basa en la configuración del Nivel 1, manteniendo un entorno SEB con aplicaciones limitadas y navegación restringida, pero incorpora un mecanismo adicional que facilita la gestión de las direcciones web autorizadas correspondientes a la asignatura.

Para ello, se utiliza el programa **Generar_Urls_Asig.py** (disponible en GitHub[1]), cuya función es extraer automáticamente todas las URLs asociadas a la asignatura y a sus recursos. De este modo, el alumnado puede navegar por los contenidos completos del curso dentro del Campus Virtual, permaneciendo siempre dentro del entorno seguro definido por SEB (para su uso, véase la sección *Uso del programa Generar_Urls_Asig.py*).

El programa genera un archivo de texto (.txt) que contiene exclusivamente las direcciones web vinculadas a la asignatura, garantizando que no sea posible acceder a otras áreas del Campus Virtual. Un ejemplo de este archivo se muestra en la Figura 2.

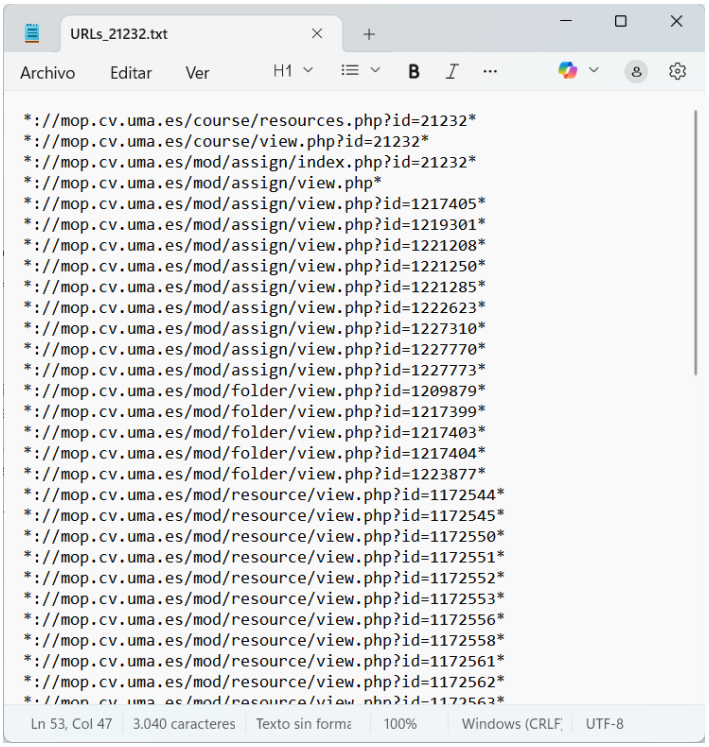

Fig. 2 Archivo de texto generado con todas las URLs asociadas a una asignatura del Campus Virtual.

Una vez generado el archivo .txt, basta con copiar su contenido en el apartado "URLs permitidas" (paso 4 de la Figura 1) de la configuración del examen básico con SEB, habilitando así la navegación controlada por los recursos de la asignatura durante la prueba.

[1] https://github.com/PacoOrtegaUMA/SEB

Limitaciones del examen con navegación

Este nivel presenta algunas limitaciones que deben tenerse en cuenta:

- Los documentos PDF deben configurarse para abrirse en una ventana nueva. En la sección de Modificar Ajustes del documento en la sección apariencia se debe poner "Nueva Ventana" (ver Fig. 3). Si los PDF se abren en la misma ventana ("Automático"), la navegación queda bloqueada en dicho documento y el alumnado no podrá volver atrás, ya que la versión de preconfiguración de SEB no permite navegación adelante o atrás, sino únicamente a través de enlaces.

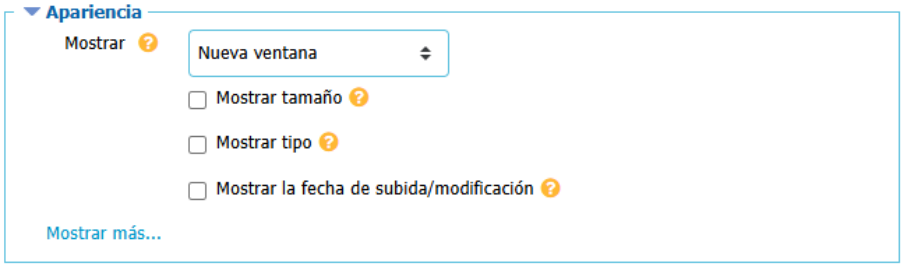

Fig. 3 Configuración de apertura de documentos PDF en una ventana nueva.

- Si en la asignatura existen enlaces a URLs externas, el alumnado podrá navegar por ellas, ya que el programa **Generar_Urls_Asig.py** también extrae las URLs externas. En caso de que no se desee permitir el acceso a estos enlaces externos, será necesario ocultarlos previamente en la asignatura o eliminarlos del contenido visible durante el examen. Al igual que en el resto de los recursos, los enlaces (internos o externos) deben configurarse para abrirse en una ventana nueva.
- La autorización de aplicaciones del sistema operativo durante el examen puede comprometer la seguridad del entorno. En particular, los programas con acceso al sistema de archivos permiten al alumnado explorar libremente las carpetas del equipo. Si se autorizan aplicaciones como procesadores de texto (Microsoft Word, LibreOffice Writer) o lectores de documentos (Adobe Acrobat, lectores PDF), estos podrán abrir cualquier archivo disponible en el sistema nativo, incluyendo documentos personales, materiales no autorizados o recursos externos al examen.

  Por este motivo, se recomienda evitar la autorización de aplicaciones de lectura o edición de archivos en este nivel, salvo que sea estrictamente necesario y se disponga de un entorno previamente controlado.

Nivel 3 – Examen con SEB en entorno aislado (MV sin Internet).

Este escenario está diseñado para exámenes en los que es necesario el uso de aplicaciones avanzadas, herramientas del sistema operativo o entornos de desarrollo, que no pueden ser utilizados de forma segura en los niveles anteriores, además de las restricciones habituales impuestas por SEB.

En este nivel, el examen se realiza dentro de una máquina virtual (MV) específicamente preparada como entorno de trabajo seguro (véase la sección *Configuración de la máquina virtual*), configurada como un sistema cerrado, sin acceso directo a Internet.

Arquitectura del entorno

En este escenario, el entorno de examen se estructura en varios niveles de aislamiento, organizados de forma jerárquica, con el objetivo de garantizar un alto grado de control y seguridad:

- **Sistema anfitrión (equipo del aula).** En este caso, el entorno se basa en sistemas Windows, al ser el sistema operativo instalado en los ordenadores del laboratorio.
- **Safe Exam Browser (SEB).** Se utiliza como capa principal de control, al tratarse de una herramienta gratuita e integrada en el Campus Virtual, que permite restringir el acceso a recursos y aplicaciones durante la prueba.
- **Plataforma de virtualización (VirtualBox).** Se emplea como sistema de virtualización gratuito que permite ejecutar máquinas virtuales independientes del sistema anfitrión, facilitando el aislamiento del entorno de examen.
- **Sistema operativo invitado (MV Linux).** Se utiliza una distribución Linux dentro de la máquina virtual, ya que ofrece mayores posibilidades de control por usuario y de configuración de restricciones a nivel de sistema.

Esta arquitectura multinivel permite separar completamente el entorno de examen del sistema nativo del equipo, garantizando un alto grado de control, aislamiento y homogeneidad entre los distintos puestos de trabajo.

Deshabilitación de la conectividad de red

Para bloquear la conectividad de red en la máquina virtual, debe ejecutarse el script **Sc_quitar_internet.bat**, disponible en el repositorio oficial del proyecto en GitHub. Este script aplica automáticamente las reglas necesarias para impedir el acceso a Internet y al Campus Virtual desde el entorno de examen. De este modo, aunque el alumnado disponga de herramientas con capacidad de red, estas no pueden establecer comunicaciones externas.

Con el fin de aplicar esta configuración de forma simultánea en todos los equipos del laboratorio, se recomienda el uso de la herramienta ***Veyon***, que permite ejecutar el script de forma remota y centralizada desde el equipo del profesor.

Recomendaciones operativas para el profesorado

Antes del inicio del examen, se recomienda realizar las siguientes comprobaciones:

- Comprobar el arranque correcto de todas las máquinas virtuales mediante el script **MV_Encender.bat** disponible en GitHub.
- Verificar la ausencia de conectividad externa utilizando el script **Sc_ver_reglas.bat**, con el fin de confirmar que las reglas de bloqueo se encuentran activas.
- Validar el correcto funcionamiento de todas las herramientas necesarias para la realización de la prueba (entorno de desarrollo, navegador, compiladores, etc.).
- Disponer de una copia de respaldo del entorno mediante el uso del script **MV_instantanea.bat**, que permite iniciar el examen a partir de una máquina virtual previamente configurada.

Estas acciones permiten garantizar que el entorno de evaluación se encuentra correctamente preparado y reducen significativamente el riesgo de incidencias durante la prueba.

Configuración de la tarea con archivo SEB configurado

Para aplicar correctamente este nivel de seguridad, no es suficiente utilizar la configuración básica de SEB desde el Campus Virtual. Es necesario crear previamente un archivo de configuración avanzado mediante la **SEB Configuration Tool** (ver sección *Configuración de SEB Configuration Tool*), que se guarda con extensión .seb.

Una vez generado dicho archivo, debe asociarse a la tarea del Campus Virtual siguiendo estos pasos (Fig. 4):

1. Activar la opción "Navegador de Examen Seguro" (1).
2. En la opción "*Usar Safe Exam Browser (SEB)*", seleccionar la opción *Subir mi propia configuración* (2).
3. Cargar el archivo de configuración (.seb) generado previamente con la **SEB Configuration Tool** (3).

Este archivo será el que defina todas las restricciones y parámetros del entorno de examen, garantizando que la prueba se ejecute bajo la configuración establecida.

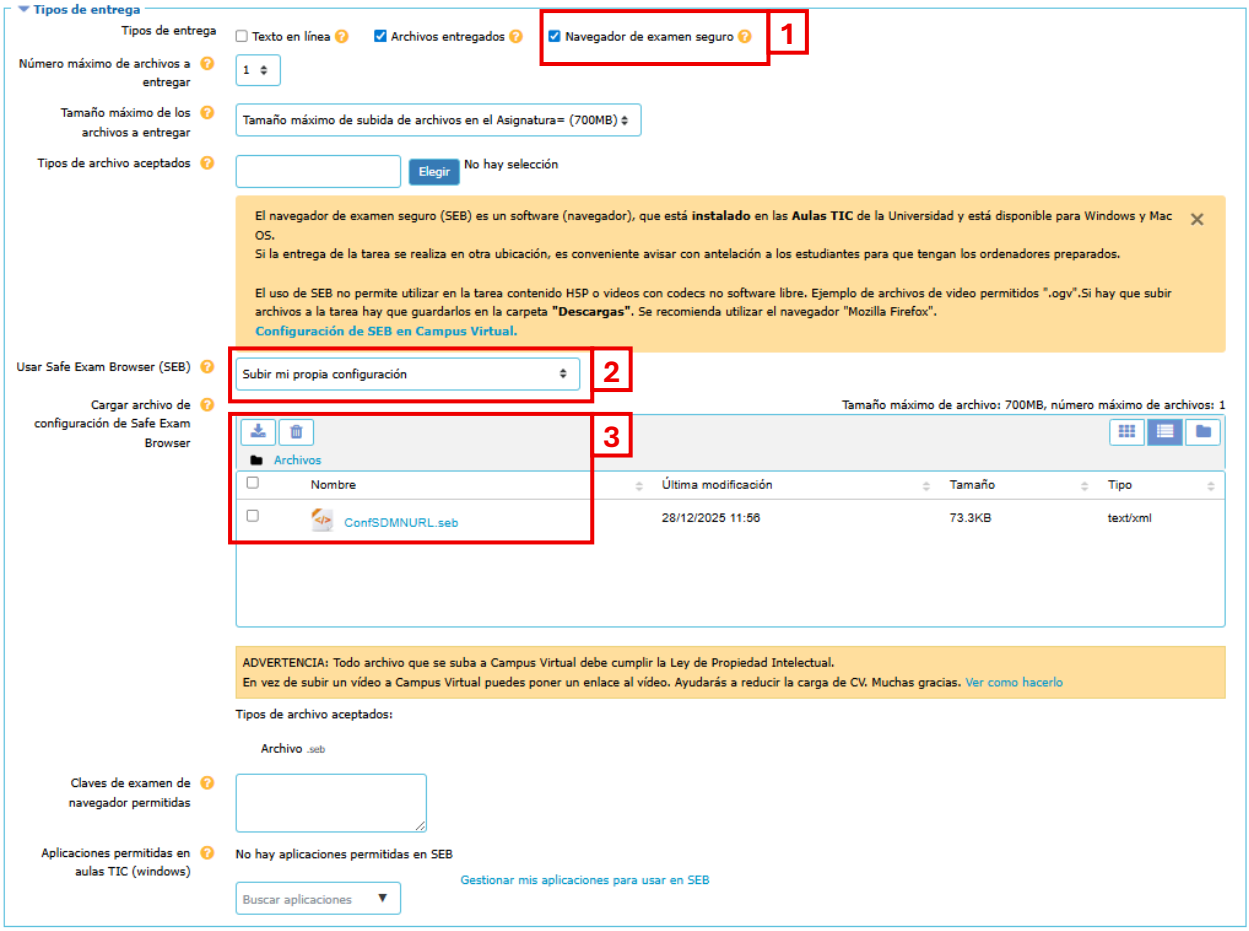

Fig. 4 Activación del Navegador de Examen Seguro y selección de configuración personalizada.

Nivel 4 – Examen con SEB en entorno abierto (MV con Internet).

Este nivel ha sido diseñado para exámenes en los que es necesario mantener el acceso a Internet desde la máquina virtual, pero bajo un control de las aplicaciones que pueden enviar y recibir datos de internet. A diferencia del Nivel 3, la máquina virtual no se configura para permanecer aislada de la red, sino que dispone de conectividad, limitada y supervisada.

El objetivo de este nivel es permitir el uso de servicios o recursos online específicos (por ejemplo, plataformas internas, APIs o servicios web concretos), evitando al mismo tiempo el acceso libre a Internet y el uso de aplicaciones no autorizadas. Este nivel se recomienda para exámenes avanzados en los que se requiere conectividad limitada y controlada, manteniendo un entorno flexible pero seguro.

Para conseguir este escenario se realiza una serie de actuaciones:

- Restringir mediante SEB el uso de aplicaciones y acceso limitado a URLs específicas.
- Configurar la máquina virtual, para bloquear o restringir programas con salida a Internet.
- Filtrar URLs dentro de la Máquina Virtual, permitiendo únicamente los dominios o direcciones necesarios para el examen.

Con esta configuración, aplicaciones que normalmente permiten acceso libre a Internet, como navegadores webs alternativos (por ejemplo, Firefox) o entornos de desarrollo con conectividad integrada (por ejemplo, Visual Studio Code), permanecen bloqueadas durante el examen. De este modo, aunque la máquina virtual tenga acceso a Internet, el alumnado solo puede utilizar los recursos explícitamente autorizados.

Configuración de SEB en el Nivel 4

En el Nivel 4, la configuración de Safe Exam Browser se realiza siguiendo el mismo procedimiento descrito para el Nivel 3, utilizando la *SEB Configuration Tool* y un archivo de configuración .seb personalizado.

Se mantienen, por tanto:

- La definición de aplicaciones permitidas y prohibidas.
- Las restricciones del sistema operativo.
- El control del portapapeles, capturas y combinaciones de teclas.
- El filtrado de URLs mediante lista blanca.
- La protección del archivo de configuración mediante contraseña.

La diferencia principal con respecto al Nivel 3 no reside en la configuración general de SEB, sino en la política de conectividad de la máquina virtual, que en este nivel dispone de acceso a Internet controlado.

En este contexto, el único apartado que debe adaptarse específicamente es la pestaña Network, donde se deben incluir exclusivamente las URLs a las que se desea permitir el acceso durante el examen. No se recomienda autorizar direcciones genéricas ni dominios completos, sino únicamente los recursos estrictamente necesarios.

Para facilitar esta tarea, puede utilizarse el programa ***Generar_SEB.py***, que permite incorporar automáticamente al archivo .seb las URLs almacenadas en archivos de texto, agilizando la configuración y reduciendo errores manuales (ver sección *Uso del programa Generar_Seb.py*).

Por tanto, el archivo .seb utilizado en el Nivel 4 debe basarse en el del Nivel 3, modificando únicamente el listado de URLs permitidas en función de los recursos online necesarios para cada examen.

Configuración de la máquina virtual en el Nivel 4

En el Nivel 4, la máquina virtual dispone de acceso a Internet, pero se configura como un entorno controlado, en el que solo se permite el uso de aplicaciones previamente autorizadas y configuradas.

En esta configuración se permite únicamente el uso de aplicaciones que puedan ser controladas de forma fiable. En concreto, se ha optado por:

- **Firefox:** se utiliza como navegador principal, ya que permite restringir el acceso a los recursos web mediante listas de URLs autorizadas, bloquear la instalación de extensiones y desactivar funciones avanzadas no necesarias durante el examen. Para la aplicación de estas restricciones se emplea el programa **Sc_mandar_policies.bat**, junto con el archivo JSON generado específicamente para cada escenario mediante el programa **Generar_Json_Firefox.py**, cuyo funcionamiento se describe en la sección *Uso del programa Generar_Json_Firefox.py*. Dicho archivo JSON incorpora tanto las restricciones asociadas a la instalación y uso de extensiones como el listado de direcciones web permitidas.
- **Visual Studio Code**: se utiliza como entorno de programación, configurado para impedir la instalación de nuevas extensiones y deshabilitar los mecanismos de sincronización online. Previamente al examen, el profesorado instala las extensiones necesarias para el desarrollo de la prueba. Posteriormente, se bloquea la posibilidad de añadir nuevas extensiones mediante la modificación de los permisos de la carpeta correspondiente, tal y como se describe en la sección *Configuración de la MV para no poder añadir extensiones en Visual Studio Code*, evitando así la incorporación de funcionalidades no permitidas durante el examen.

Todos los demás programas con capacidad de acceso a red (navegadores alternativos, clientes de mensajería, herramientas cloud, etc.) deben permanecer bloqueados o no instalados en la máquina virtual.

Configuración de "SEB Configuration Tool"

En los siguientes apartados se describe la configuración pestaña a pestaña de la ***SEB Configuration Tool***. Cada subsección incluye una captura de pantalla y una explicación de los parámetros que deben ajustarse para este nivel de seguridad.

General

En esta pestaña General (Fig. 5) se configura si el alumno puede cerrar SEB y, en caso afirmativo, bajo qué condiciones.

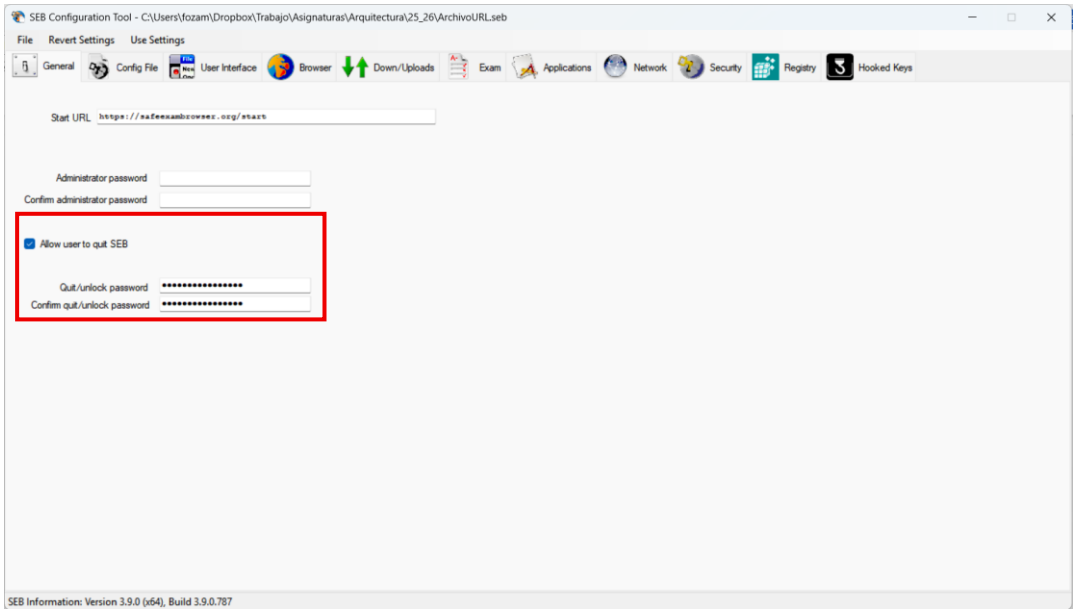

Fig. 5 Pestaña General de SEB Configuration Tool.

Configuración recomendada para el Nivel 3:

- Activar la opción ***Allow user to quit SEB*** únicamente para permitir la salida controlada mediante contraseña.
- Definir una ***Quit/unlock password*** y su confirmación. Esta contraseña permite cerrar o desbloquear SEB exclusivamente bajo supervisión del profesorado, por ejemplo, en caso de incidencias técnicas.

Config File

La pestaña Config File, que se observa en la Figura 6, define cómo y cuándo se utilizará el archivo de configuración SEB (.seb), así como el nivel de protección aplicado a dicho archivo. Esta configuración es especialmente importante en el Nivel 3, ya que el archivo .seb es el elemento que garantiza que el examen se ejecute siempre bajo las condiciones establecidas.

En el apartado ***Use SEB settings file for…*** se debe seleccionar la opción: ***Starting an exam***

Esta opción indica que el archivo .seb se utilizará exclusivamente para iniciar un examen, impidiendo que el alumnado pueda modificar la configuración o acceder a preferencias avanzadas de SEB.

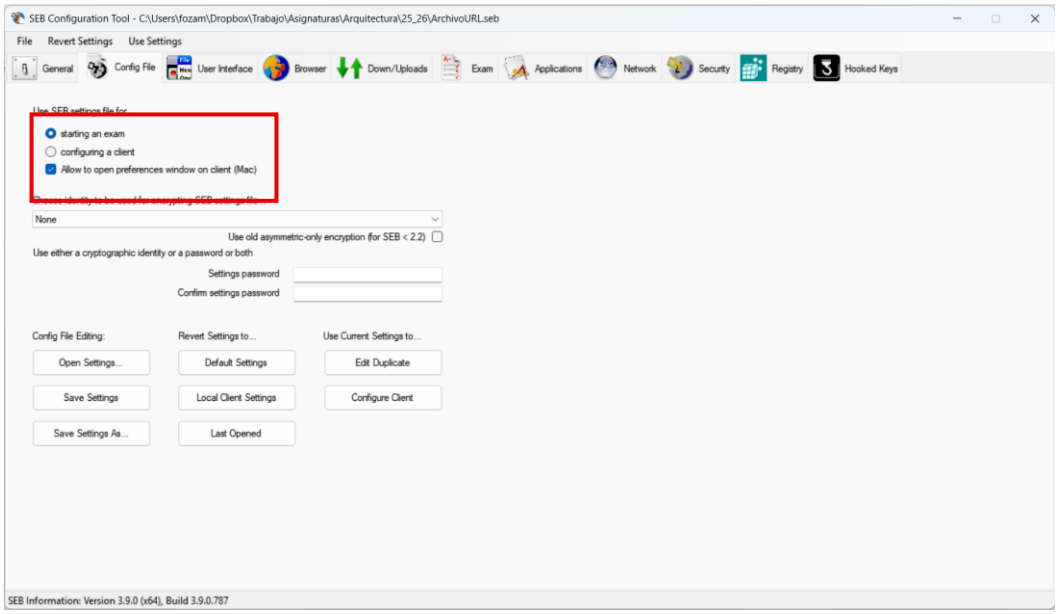

Fig. 6 Pestaña Config File de SEB Configuration Tool.

User Interface

La pestaña User Interface (Fig. 7) permite definir cómo se presenta SEB al alumnado durante el examen y qué elementos de la interfaz están visibles o accesibles. En el Nivel 3, el objetivo principal es minimizar distracciones, evitar accesos innecesarios y mantener una experiencia de uso clara pero controlada.

En esta configuración se mantiene el navegador en una ventana que ocupa toda la pantalla, con los elementos informativos básicos visibles (hora, recarga y distribución del teclado), y sin acceso a barras de herramientas, menús ni opciones avanzadas del navegador. No se habilitan ayudas adicionales como el corrector ortográfico o diccionarios. Para este nivel, **se recomienda mantener las opciones por defecto**, ya que ofrecen un equilibrio adecuado entre usabilidad y control, sin introducir riesgos adicionales en la seguridad del examen.

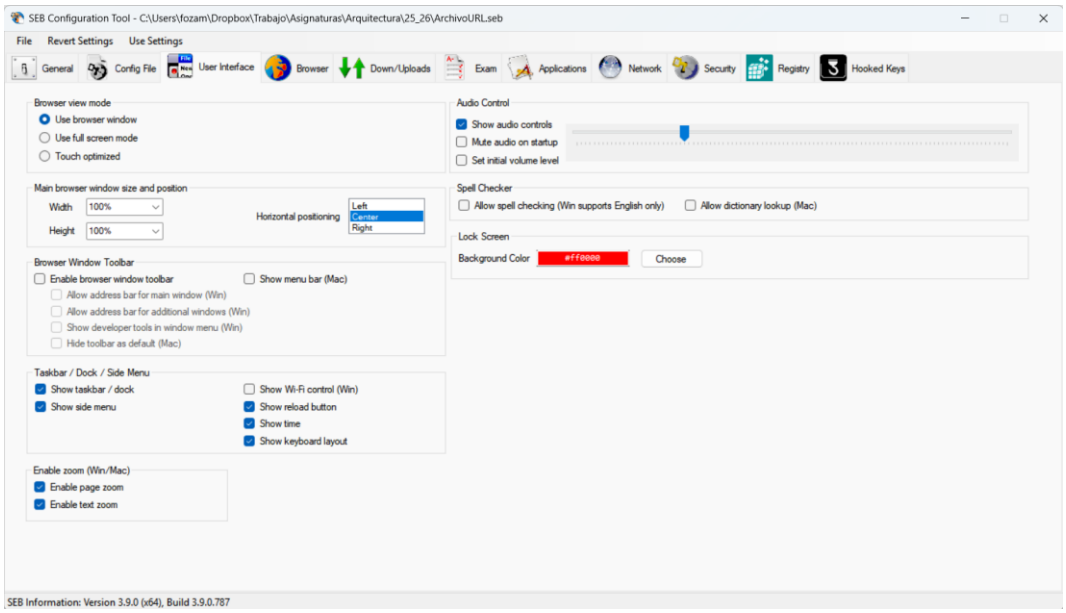

Fig. 7 Pestaña User Interface de SEB Configuration Tool.

Browser

La pestaña Browser define cómo se abren los enlaces y cómo se controla la navegación durante el examen. En el Nivel 3, estas opciones son clave para evitar que el alumnado quede bloqueado en un recurso y para mantener un flujo de navegación controlado.

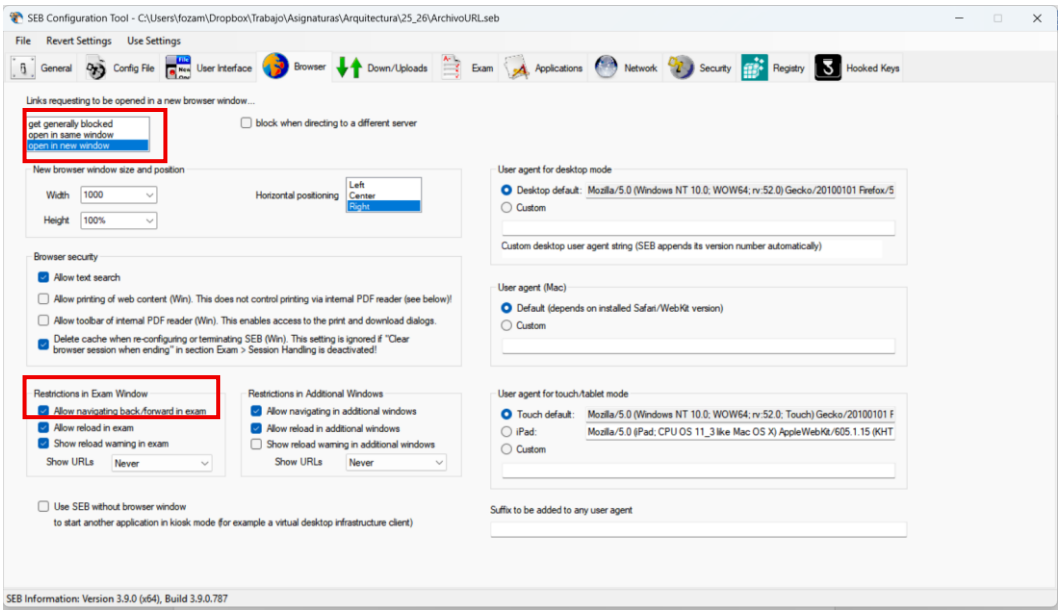

Fig. 8 Pestaña Browser de SEB Configuration Tool.

En esta configuración se selecciona la opción ***Open links in new window***, de modo que todos los enlaces se abran siempre en una ventana nueva del navegador. Esta opción resulta especialmente importante cuando se utilizan documentos PDF u otros recursos externos, ya que evita que el alumnado quede bloqueado en un contenido sin posibilidad de regresar al examen.

Asimismo, en el apartado ***Restrictions in Exam Window*** se activa la opción ***Allow navigating back/forward in exam,*** lo que habilita la navegación hacia adelante y atrás dentro del examen. De forma complementaria, se permite también la recarga de páginas, facilitando la recuperación del estado del examen ante posibles incidencias sin comprometer la seguridad del entorno.

Para el Nivel 3, se recomienda mantener estas opciones tal y como se muestran, ya que garantizan una navegación funcional sin comprometer la seguridad del entorno de examen.

Down/Uploads

En esta configuración se activa la opción ***Allow downloading files***, permitiendo la descarga de archivos durante el examen. Asimismo, se define un directorio específico de descarga mediante la opción Choose download / upload directory, que en este caso se establece en la carpeta Downloads del sistema.

En el apartado ***Allow uploading files*** se permite la subida de archivos cuando el examen lo requiera (por ejemplo, entrega de resultados o ficheros generados durante la prueba).

Se selecciona la opción ***manually with file request***, de modo que:

- La subida de archivos solo se realiza cuando el propio examen lo solicita.
- Se evita la subida accidental o no controlada de ficheros.

Además, se restringe la subida a archivos previamente descargados, garantizando que el alumnado solo pueda entregar documentos generados o facilitados dentro del propio entorno del examen.

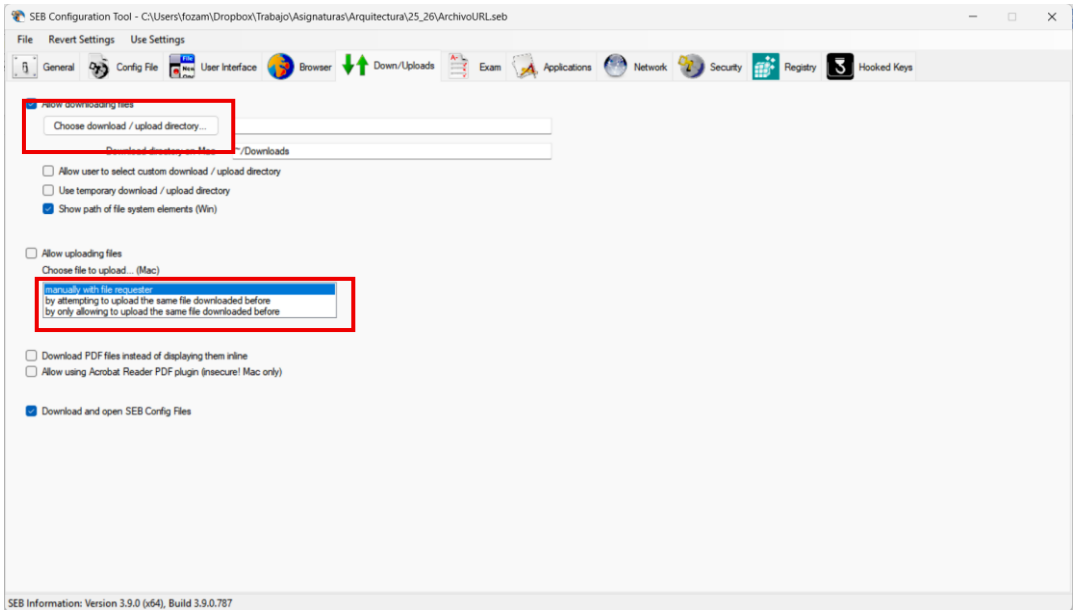

Fig. 9 Opciones de descarga y subida de archivos en SEB.

Exam

La pestaña Exam agrupa las opciones relacionadas con la integridad del examen y la gestión de la sesión en SEB.

Browser Exam Key / Configuration Key generan automáticamente dos type $env:USERPROF:

- Browser Exam Key (BEK): verifica la versión correcta de SEB y con la configuración.
- Configuration Key: comprueba el archivo de configuración definido.

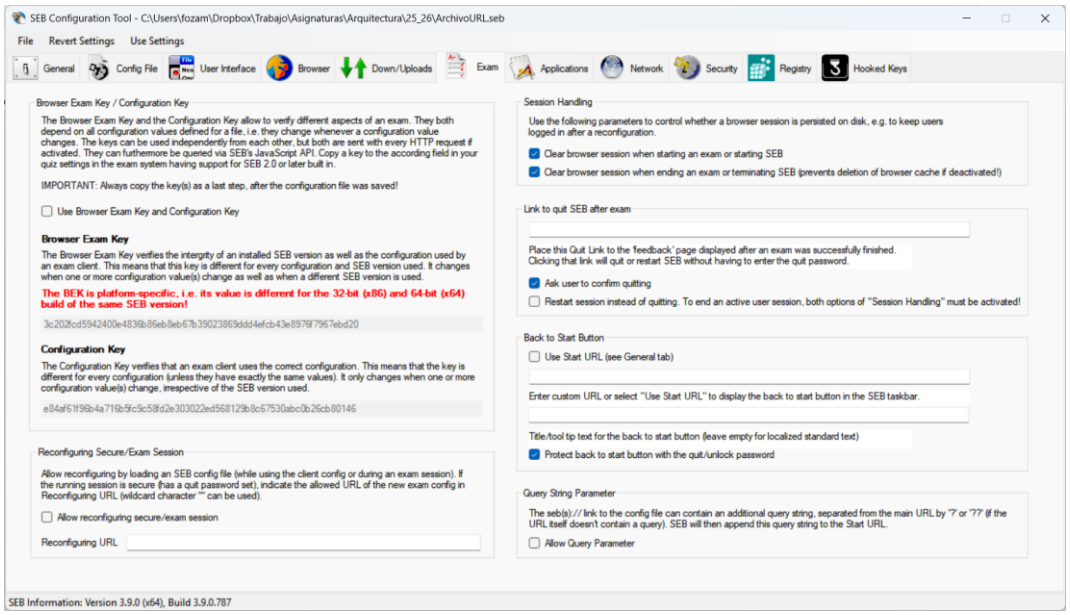

Fig. 10 Identificadores Browser Exam Key y Configuration Key.

En este nivel no es necesario modificar estos valores, ya que SEB los gestiona automáticamente.

La sección **Link to quit SEB after exam** permite definir un enlace para cerrar SEB al finalizar la prueba, pero en la configuración mostrada se mantiene el comportamiento estándar, solicitando confirmación al usuario antes de salir y protegiendo la salida con la contraseña definida en la pestaña *General*.

Applications

La pestaña Applications es una de las más importantes de toda la configuración de SEB, especialmente en el Nivel 3, ya que define qué aplicaciones y procesos pueden ejecutarse mientras SEB está activo y cuáles quedan bloqueados automáticamente.

La opción ***Monitor processes while SEB is running*** debe permanecer activada. Esto permite a SEB supervisar en tiempo real los procesos en ejecución y aplicar las restricciones definidas.

Para permitir la ejecución de nuevas aplicaciones durante el examen, estas deben añadirse explícitamente en la sección ***Permitted Processes*** de la pestaña *Applications*. SEB ofrece dos métodos para incorporar nuevos programas:

1. **Añadir manualmente** mediante el botón **"+"**, introduciendo los datos del proceso de forma manual.
2. **Seleccionar automáticamente** mediante la opción **"Choose Application…"**, que permite buscar la aplicación directamente en el sistema de archivos y rellena automáticamente los campos principales.

Al añadir una nueva aplicación, es necesario revisar y completar correctamente los siguientes campos:

- **Active:** Debe estar activado para que la aplicación esté permitida durante el examen.
- **OS:** Sistema operativo al que aplica la regla (por ejemplo, *Windows*).
- **Executable:** Ruta completa al ejecutable de la aplicación (por ejemplo, virtualbox.exe).
- **Original Name:** Nombre descriptivo de la aplicación (opcional, pero recomendable).
- **Signature:** Este campo permite especificar la firma digital del ejecutable. Obligatorio Dejarlo vacío.
- **Path:** Directorio donde se encuentra el ejecutable.
- **Arguments:** Parámetros opcionales de ejecución. Normalmente se deja vacío, excepto para lanzar la MV que se precisa para el examen)

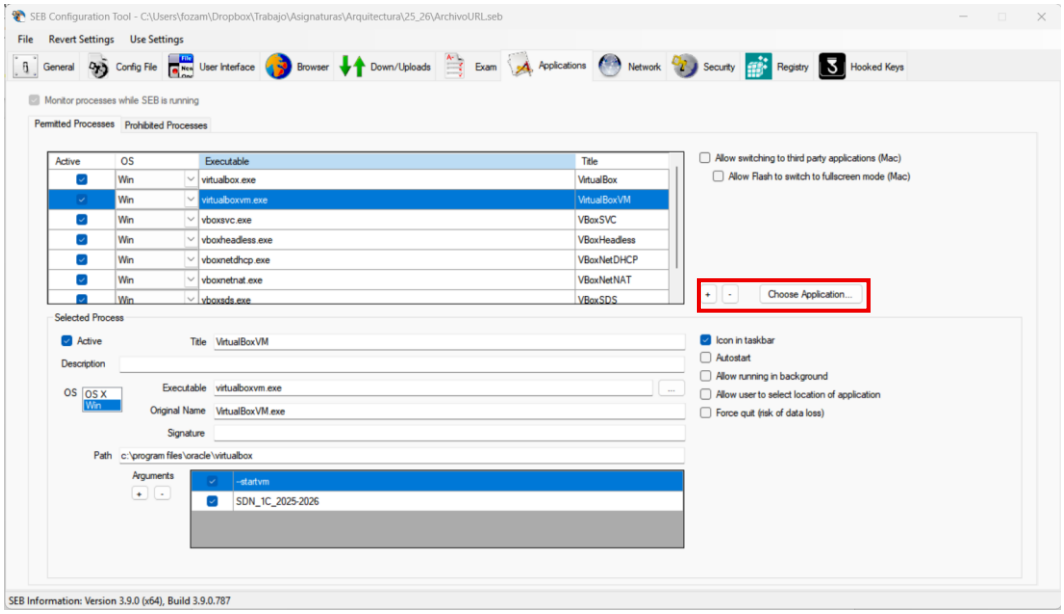

Fig. 11 Configuración de aplicaciones permitidas en SEB.

Configuración específica de VirtualBox en la pestaña *Applications*

Cuando el examen se realiza dentro de una máquina virtual, es imprescindible permitir explícitamente los procesos asociados a VirtualBox. De lo contrario, SEB puede bloquear su ejecución o cerrar el examen al detectar procesos no autorizados.

En la sección **Permitted Processes** deben añadirse, como mínimo, los siguientes ejecutables (en sistemas Windows):

- **virtualboxvm.exe:** Proceso encargado de la ejecución de la máquina virtual. Este proceso necesita marcar "*icon in taskbar*" para que esté disponible en el examen, además el campo Arguments ejecuta sólo la MV del examen.
  Para lanzar una MV concreta: **Arguments:** --startvm *NombreDeLaMaquina*
- **virtualbox.exe:** Interfaz gráfica principal de VirtualBox.
- **vboxsvc.exe:** Servicio interno de VirtualBox que gestiona la comunicación entre la interfaz gráfica y los componentes del sistema.
- **vboxheadless.exe:** Necesario si la MV se ejecuta sin interfaz gráfica completa.
- **vboxnetdhcp.exe:** Servicio DHCP de VirtualBox para redes NAT o internas.
- **vboxnetnat.exe:** Gestiona la traducción NAT de red (aunque la MV no tenga salida a Internet, el proceso debe estar permitido).
- **vboxsds.exe:** Servicio auxiliar interno utilizado por VirtualBox.
- **MV_BloqueoBarras.bat:** Script para quitar las barras del menú del VirtualBox para que no pueda acceder al menú de carpeta compartidas o USB (disponible en GitHub).
  Para lanzarlo sobre una MV concreta: **Arguments:** *NombreDeLaMaquina*

En la pestaña ***Applications***, dentro del apartado ***Prohibited Processes***, se definen las aplicaciones que no pueden ejecutarse mientras SEB está en funcionamiento. Esta lista actúa como una medida de refuerzo, impidiendo explícitamente la apertura de software que podría comprometer la integridad del examen.

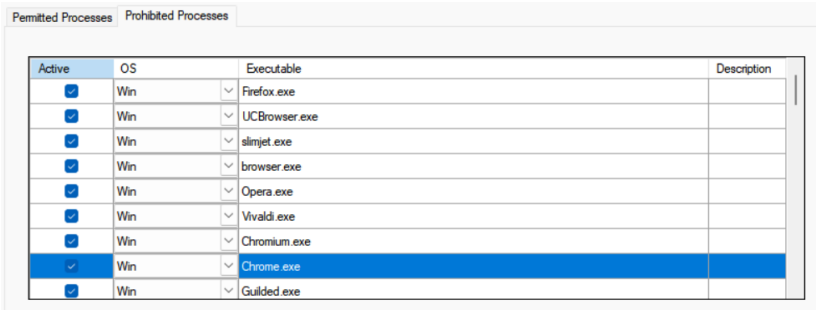

Fig. 12 Lista de procesos prohibidos en SEB.

SEB incluye, por defecto, una lista extensa de procesos prohibidos (aproximadamente 59 aplicaciones) en la pestaña **Prohibited Processes**. Esta lista contiene principalmente:

- Navegadores web alternativos.
- Aplicaciones de mensajería y comunicación.
- Herramientas habituales de captura, grabación o control remoto.
- Software que podría facilitar el acceso a recursos externos o la colaboración no autorizada.

Estas entradas están preconfiguradas por SEB para cubrir los casos más comunes y han sido definidas tras pruebas exhaustivas en distintos entornos.

Recomendación: Para el Nivel 3, se recomienda mantener íntegramente la lista de procesos prohibidos por defecto, sin eliminar ni modificar ninguna entrada. Además, se recomienda no añadir ninguna aplicación de lectura de archivos (word, acrobat) ya que estos dan acceso a todo el sistema de archivos

de la máquina nativa.

Network

La pestaña Network permite definir qué direcciones web pueden visitarse durante el examen y cuáles quedan bloqueadas.

En esta configuración se activa la opción Activate URL filtering, lo que habilita el uso de una lista blanca (allow list) de direcciones permitidas. De forma opcional, puede activarse Filter also embedded content si se desea que el filtrado se aplique también a contenido embebido, como iframes o recursos externos incluidos en una página.

En la tabla central se especifican las URLs autorizadas, marcadas con la acción Allow. Estas URLs pueden definirse como expresiones regulares o mediante patrones con comodines.

Es importante tener en cuenta que, debido al funcionamiento interno del filtrado de SEB, una URL permitida autoriza también todas las direcciones derivadas de ella (por ejemplo, subrutas, parámetros o recursos asociados), siempre que coincidan con el patrón definido. No obstante, cuando se requiere un control más estricto, es posible utilizar expresiones regulares más específicas (sin comodines) para limitar el acceso únicamente a URLs exactas.

Nota importante: Si no se desea permitir la navegación a ninguna URL adicional, es imprescindible incluir al menos las siguientes direcciones:

`*://<cv>.cv.uma.es/mod/assign/view.php*` URL para poder acceder a las tareas dentro de SEB.

`*://<cv>.cv.uma.es/pluginfile.php/*` URL para poder descargar ficheros dentro de la tarea.

En estas URLs, `<cv>` corresponde a la abreviatura del Campus Virtual específico de cada materia, (informatica,esit,mop,..).

Recomendación: Para facilitar y acelerar la configuración del filtrado de URLs, se recomienda utilizar el programa ***Generar_Seb.py***, que permite importar automáticamente listas de URLs desde un archivo .txt y añadirlas directamente a la pestaña ***Network*** de SEB Configuration Tool. De este modo se evita la introducción manual de enlaces, reduciendo errores y tiempo de configuración.

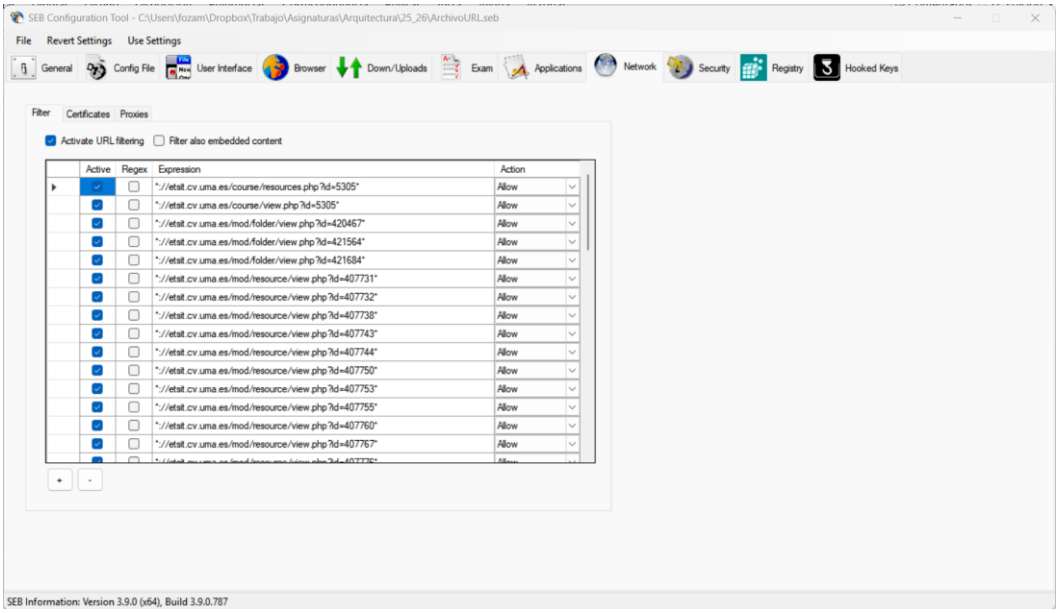

Fig. 13 Configuración del filtrado de URLs en SEB.

Asimismo, con la ayuda del programa ***Generar_URL.py*** es posible extraer automáticamente todas las URLs asociadas a una asignatura del Campus Virtual y generar el archivo .txt correspondiente.

Security

La pestaña Security es una de las más relevantes en el Nivel 3, ya que permite reforzar el aislamiento del entorno del examen mediante restricciones directas sobre el **sistema operativo**. En esta pestaña se configuran aspectos críticos como el modo quiosco, el uso del portapapeles y determinadas acciones del usuario.

A continuación, se describen los bloques más importantes señalados en la Figura 14.

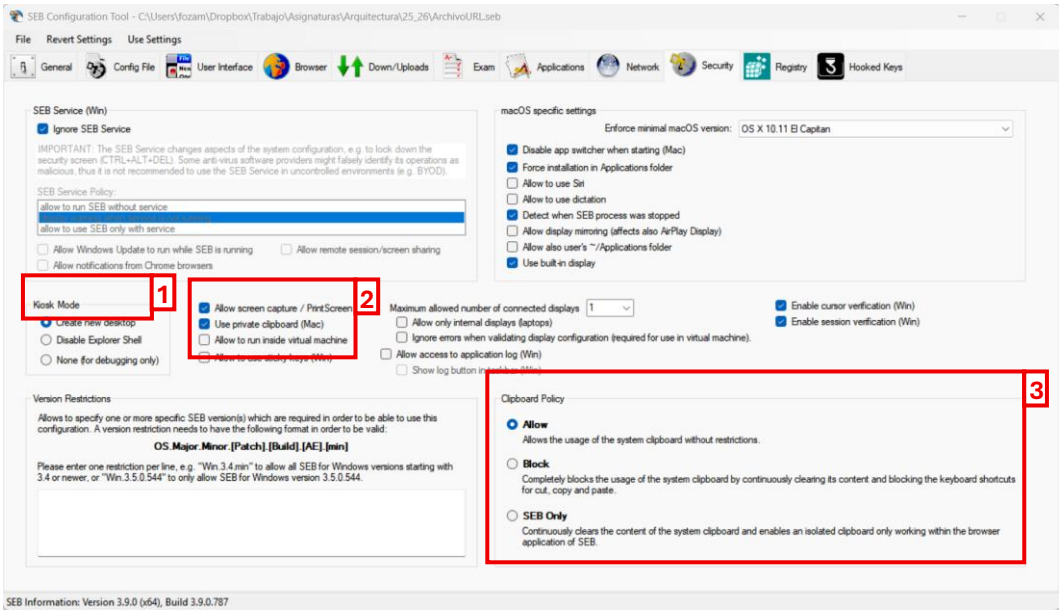

Fig. 14 Opciones de seguridad del sistema en SEB.

Para un correcto funcionamiento del examen, se recomienda la siguiente configuración en la pestaña Security:

1) ***Kiosk Mode:*** En este apartado se define el nivel de aislamiento del escritorio mientras SEB está activo. Se recomienda seleccionar **Create new desktop**, de modo que SEB se ejecute en un escritorio independiente, aislado del escritorio principal del sistema operativo. Esta configuración impide el acceso directo a ventanas, aplicaciones o notificaciones externas, garantizando que el examen se desarrolle dentro de un entorno controlado.

2) ***Restricciones de captura y combinaciones de teclas:*** En el bloque central se controlan acciones que podrían utilizarse para copiar o extraer información durante el examen. Se recomienda activar la opción **Allow screen capture / PrintScreen** para permitir la realización de capturas de pantalla durante la prueba. Aunque esta opción puede facilitar un posible envío de información fuera del examen, se considera adecuada en este contexto porque facilita la realización del examen, especialmente en pruebas técnicas. Asimismo, se activa Use private clipboard, lo que habilita un portapapeles interno aislado dentro de SEB.

3) ***Clipboard Policy (política del portapapeles):*** En el apartado Clipboard Policy se define el comportamiento del portapapeles durante el examen. Se recomienda seleccionar la opción **Allow**, que permite el uso del portapapeles sin restricciones. Esta configuración facilita la copia y pegado de información durante la prueba, lo que puede resultar necesario en determinados tipos de examen, priorizando la usabilidad frente a un control más restrictivo.

Nota importante: Las opciones descritas en este apartado **priorizan la usabilidad y la correcta realización del examen** frente a un nivel máximo de restricción. La activación de capturas de pantalla y el uso del portapapeles puede facilitar determinadas acciones fuera del entorno del

examen, por lo que esta configuración debe utilizarse únicamente cuando el tipo de prueba lo requiera.

Registry

Esta pestaña permite controlar qué opciones del menú de seguridad de Windows (invocado mediante la combinación Ctrl+Alt+Supr) están disponibles mientras SEB está en ejecución.

En esta sección se pueden habilitar o deshabilitar acciones del sistema que podrían permitir al alumnado interrumpir el examen o acceder a funciones no deseadas Se recomienda mantener todas las opciones desactivadas, es decir, dejar todos los campos sin marcar, tal y como se muestra en la figura 15.

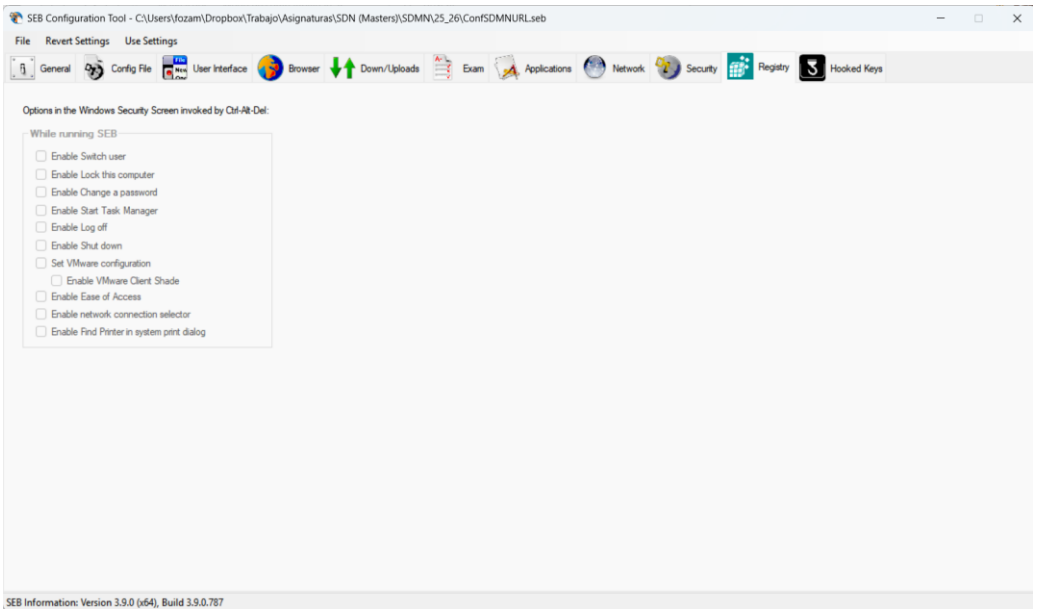

Fig. 15 Pestaña Registry con restricciones del menú de seguridad.

Hooked Keys

La pestaña Hooked Keys permite definir qué teclas especiales y teclas de función están habilitadas mientras SEB se encuentra en ejecución. Estas opciones controlan combinaciones de teclado y acciones del ratón que podrían utilizarse para cambiar de aplicación o interactuar con el sistema operativo. Se recomienda mantener esta pestaña con los valores por defecto, tal y como se muestra en la figura.

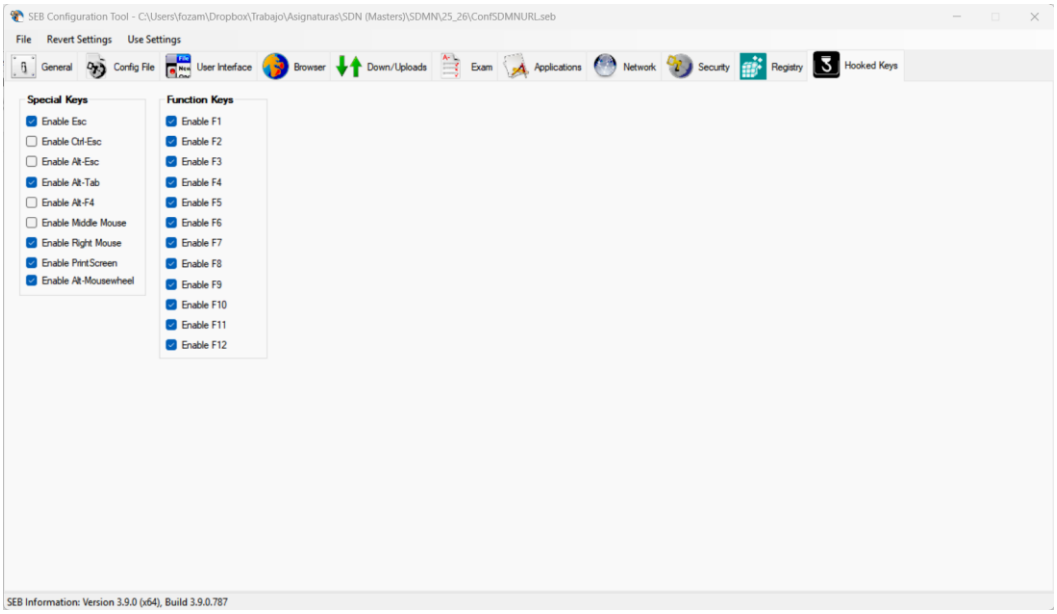

Fig. 16 Pestaña Hooked Keys con configuración por defecto.

Configuración de la MV para poner/quitar Internet al usuario sin permiso de sudo

El entorno seguro para realizar el examen se realiza dentro de una máquina virtual (MV) con Linux, configurada para controlar el acceso de los usuarios. La seguridad se basa en dos ideas:

- Separar usuarios (profesor / alumno) para controlar permisos en el sistema.
- Bloquear la salida a Internet del usuario alumno usando iptables por UID, de forma que el resto del sistema (usuario profesor) no se vea afectado.

Paso 1. Crear los usuarios de trabajo

- Usuario profesor (administrador). Debe disponer de permisos de administración (sudo/root) para preparar la MV y gestionar incidencias.
- Usuario alumno (sin administración). Debe ser un usuario normal, sin permisos de sudo, que será el que utilice el alumnado durante el examen.

Paso 2. Identificar el UID del usuario alumno

- Las reglas se aplican por UID. Para conocerlo: `$ id -u alumno`

  (**NOTA:** En los ejemplos siguientes se asume que el UID del usuario alumno es 1000. Si tu usuario tiene otro UID, sustituye 1000 por el valor correspondiente.)

Paso 3. Revisar reglas actuales de OUTPUT

Antes de modificar nada, visualizar la cadena OUTPUT con números de línea:

```
$ sudo iptables -L OUTPUT -v -n --line-numbers
```

Esto permite comprobar el orden de reglas y facilitar borrados posteriores.

Paso 4. Aplicar reglas de red (bloqueo por UID)

Las siguientes reglas se aplican solo al usuario alumno (UID 1000) y controlan su tráfico saliente (OUTPUT).

1. Permitir tráfico local (loopback)

   Esta regla es obligatoria para que funcionen correctamente servicios locales:

   ```
   $ sudo iptables -I OUTPUT 1 -m owner --uid-owner 1000 -o lo -j ACCEPT
   ```

2. Permisos opcionales (solo si se necesitan)

   a) Permitir proxy (puerto 3128):

   ```
   $ sudo iptables -A OUTPUT -m owner --uid-owner 1000 -p tcp --dport 3128 -j ACCEPT
   ```

   b) Permitir solo HTTP/HTTPS (80,443):

   ```
   $ sudo iptables -A OUTPUT -m owner --uid-owner 1000 \
   -p tcp -m multiport --dports 80,443 -j ACCEPT
   ```

   c) Permitir puertos TCP usados en prácticas

   ```
   $ sudo iptables -A OUTPUT -m owner --uid-owner 1000\
    -p tcp -m multiport --dports 5000,7000,8000,8181 -j ACCEPT
   ```

3. Permitir DNS (53/udp):

   ```
   $ sudo iptables -A OUTPUT -m owner --uid-owner 1000 -p udp --dport 53 -j ACCEPT
   ```

4. Bloquear todo lo demás (regla final)

   Esta regla debe ir al final para que bloquee cualquier tráfico no contemplado:

   ```
   $ sudo iptables -A OUTPUT -m owner --uid-owner 1000 -j REJECT
   ```

Resultado: el usuario alumno solo podrá usar los puertos permitidos (y siempre podrá usar loopback). Todo lo demás quedará bloqueado.

Paso 5. Guardar reglas (persistencia)

Para mantener las reglas tras reiniciar la MV (si se usa iptables-persistent o reglas persistentes), guardar:

```
$ sudo sh -c 'iptables-save > /etc/iptables/rules.v4'
```

Paso 6. Mantenimiento de reglas

1. Borrar una regla por número de línea (Ejemplo: borrar la regla 2 de OUTPUT):

   ```
   $ sudo iptables -D OUTPUT 2
   ```

2. Insertar una regla en una posición concreta (Ejemplo: insertar en posición 2):

   ```
   $ sudo iptables -I OUTPUT 2 -m owner --uid-owner 1000 \
   -p tcp -m multiport --dports 80,443 -j ACCEPT
   ```

3. Guardar cambios, Tras modificar reglas, volver a guardar:

   ```
   $ sudo sh -c 'iptables-save > /etc/iptables/rules.v4'
   ```

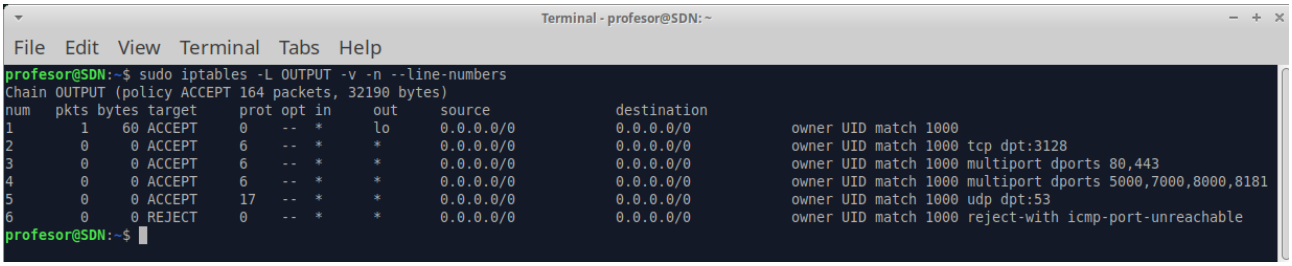

Fig. 17 Reglas iptables aplicadas al tráfico de salida del usuario alumno (UID 1000).

Paso 7. Configuración de permisos con **visudo** para permitir herramientas con sudo

En este entorno de examen/prácticas, algunas herramientas necesitan privilegios de administrador para funcionar correctamente (por ejemplo, Mininet para crear interfaces, o Wireshark para capturar tráfico). Si el usuario que realiza la práctica (normalmente alumno) no conoce la contraseña de administrador, pero aun así debe poder ejecutar estas herramientas, es necesario autorizar su ejecución mediante sudo.

La autorización se realiza con visudo, permitiendo que el usuario ejecute solo los comandos necesarios con sudo y sin solicitar contraseña.

- Entra en el archivo visudo. En la MV, con un usuario administrador (por ejemplo, profesor).

  ```
  $ sudo visudo
  ```

- Añadir permisos NOPASSWD para el usuario alumno, los permisos serán en función de la necesidad de la asignatura:
  - alumno ALL=(ALL) NOPASSWD: /usr/bin/mn
  - alumno ALL=(ALL) NOPASSWD: /usr/bin/wireshark
  - …
- Se recomienda permitir solo las herramientas imprescindibles para el examen/práctica. Cuantos más comandos se incluyan en NOPASSWD, mayor es el riesgo de que el usuario pueda realizar acciones no deseadas en el sistema.

Configuración MV para poner/quitar Internet al usuario alumno mediante clave SSH (sin password)

Objetivo: desde el host Windows, ejecutar un script que active/desactive Internet del usuario alumno (UID 1000, sin sudo) dentro de una MV Ubuntu en VirtualBox, sin que se pida password ni para SSH ni para sudo.

Requisitos:

- MV: Ubuntu con un usuario de administración (por ejemplo, profesor) con sudo.
- Host: Windows con ssh disponible (PowerShell / CMD).
- VirtualBox con red NAT y reenvío de puertos para SSH.

Preparación dentro de la MV (Ubuntu)

1. Instalar y activar SSH. En la MV (como profesor):

```
$ sudo apt update
$ sudo apt install -y openssh-server
$ sudo systemctl enable ssh
$ sudo systemctl start ssh
```

2. VirtualBox: NAT + Port Forwarding (SSH)

   En VirtualBox → Propiedades de la MV → Red → Adaptador 1 → **NAT**

   Reenvío de puertos → añadir regla:

   - Nombre: ssh
   - Protocolo: TCP
   - IP anfitrión:
   - Puerto anfitrión: 2222
   - IP invitado: 10.0.2.15
   - Guest Port: 22

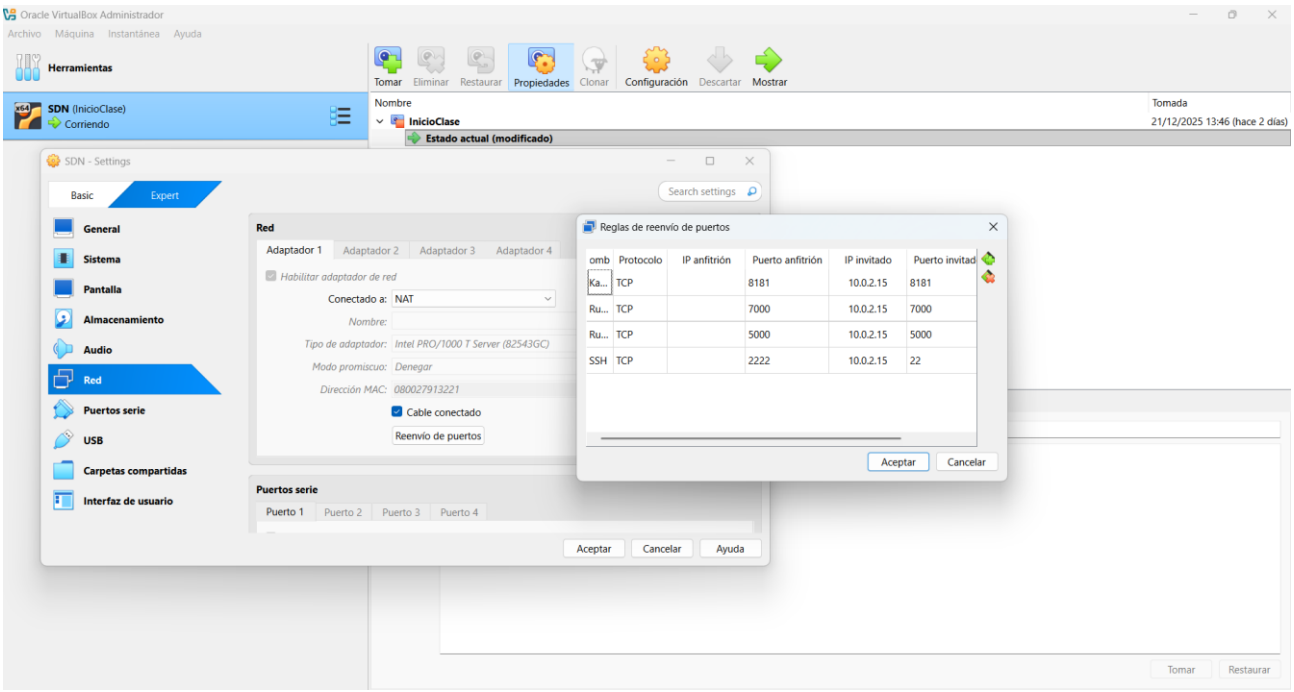

Fig. 18 Configuración de reenvío de puertos en VirtualBox para acceso a la máquina virtual.

3. Clave SSH en Windows (sin password)
    a) Generar clave en Windows. En PowerShell:

    ```
    $ ssh-keygen -t ed25519 -f $env:USERPROFILE\.ssh\Clave_MV_SDN
    ```

    (ENTER en las preguntas y no pongas passphrase si quieres 0 interacción.)

    Esto crea:

    - Clave_MV_SDN (clave privada)
    - Clave_MV_SDN.pub (clave pública)

    b) Copiar la clave pública a la MV

    - Primero, muestra la pública:

      ```
      $ type $env:USERPROFILE\.ssh\Clave_MV_SDN.pub
      ```

    - Copia toda la línea que empieza por ssh-ed25519.
    - En la MV, como profesor:
        - `$ mkdir -p ~/.ssh`
        - `$ chmod 700 ~/.ssh`
        - `$ nano ~/.ssh/authorized_keys`
        - Pega la línea de la clave publica, guarda, y luego:
        - `$ chmod 600 ~/.ssh/authorized_keys`
    - Probar SSH con clave (sin password). Desde Windows:
        - `$ ssh -i $env:USERPROFILE\.ssh\ Clave_MV_SDN -p 2222 profesor@127.0.0.1`

4. Evitar password también en sudo (NOPASSWD para iptables)

    Si ejecutas sudo iptables ... por SSH, Ubuntu pedirá password a menos que autorices esos comandos sin password.

    Crear regla sudoers dedicada (recomendado). En la MV, como ***"profesor":***

    - `$ sudo visudo`
    - Añade en el archivo:

      profesor ALL=(ALL) NOPASSWD: /usr/sbin/iptables, /bin/sh, /usr/bin/pkill
    - Guarda y sal. Esto permite a profesor ejecutar solo esos binarios con sudo sin password.

Configuración MV para no poder añadir Extensiones en Visual Studio Code

En el Nivel 4, cuando se permite el uso de Visual Studio Code como entorno de desarrollo, es necesario impedir que el alumnado pueda instalar nuevas extensiones, ya que estas podrían facilitar el acceso a recursos externos o introducir funcionalidades no autorizadas.

Para ello, la configuración se basa en dos pasos principales:

1. Instalación previa de las extensiones permitidas

   Antes del examen, deben instalarse manualmente todas las extensiones que vayan a ser necesarias para la prueba con el usuario con permisos sudo. Estas extensiones quedarán disponibles para el alumnado durante el examen. Una vez instaladas, no se permitirá añadir nuevas extensiones por parte del alumno

2. Bloqueo de la carpeta de extensiones

   Las extensiones de Visual Studio Code se almacenan en la carpeta:

   ```
   $ ~/.vscode/extensions
   ```

   Para impedir que el usuario del alumno pueda instalar, modificar o eliminar extensiones, es necesario:

   1. Cambiar el propietario del directorio a root.
   2. Eliminar los permisos de escritura.

      Este proceso se realiza mediante los siguientes comandos:

      ```
      $ sudo chown -R root:root ~/.vscode/extensions
      $ sudo chmod -R a-w ~/.vscode/extensions
      ```

Con estos pasos la configuración queda establecida como se muestra en la Fig. 19. Con esta configuración:

- Solo el administrador (root) puede modificar la carpeta.
- El usuario puede utilizar las extensiones ya instaladas.
- No puede instalar nuevas extensiones.
- No puede modificar ni eliminar las existentes.

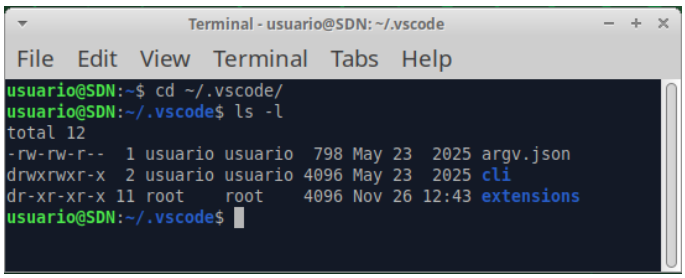

Fig. 19 Permisos de la carpeta de extensiones de Visual Studio Code tras su bloqueo.

Uso del programa *Generar_Urls_Asig.py*

El programa **Generar_Urls_Asig.py** es un script en Python cuyo objetivo es extraer automáticamente todas las URLs asociadas a una asignatura del Campus Virtual (incluyendo enlaces a recursos y actividades). El resultado se utiliza posteriormente para completar el listado de URLs permitidas en la configuración de SEB (ver Nivel 2).

El script puede ejecutarse tanto en Windows como en Linux desde una terminal (PowerShell, CMD o Terminal).

Parámetros de ejecución

El programa recibe dos parámetros:

1. Campus virtual (dominio): Se indica mediante una palabra clave, según el Campus virtual específico de la Escuela o Facultad. Los valores disponibles son múltiples, por ejemplo: mop, informática, etsit, …
- Código numérico de la asignatura: Es el identificador de la asignatura dentro del Campus Virtual.

Por ejemplo https://mop.cv.uma.es/course/view.php?id=21232&section=0 el campo 1 (dominio) es mop y para el campo 2 Código 21232

Ejecución del programa

Desde la carpeta donde se encuentre el script, debe ejecutarse el programa desde una terminal, utilizando el comando correspondiente según el sistema operativo:

- Windows (PowerShell o CMD):

  ```
  $ python .\Generar_Urls_Asig.py mop 21232
  ```

- Linux (Terminal):

  ```
  $ python3 ./Generar_Urls_Asig.py mop 21232
  ```

Al ejecutar el programa se observa en la Fig. 4 que se inicia el proceso de extracción. Antes de pulsar "Enter" para continuar hay que realizar el inicio de sesión de esa página para permitir el escaneo

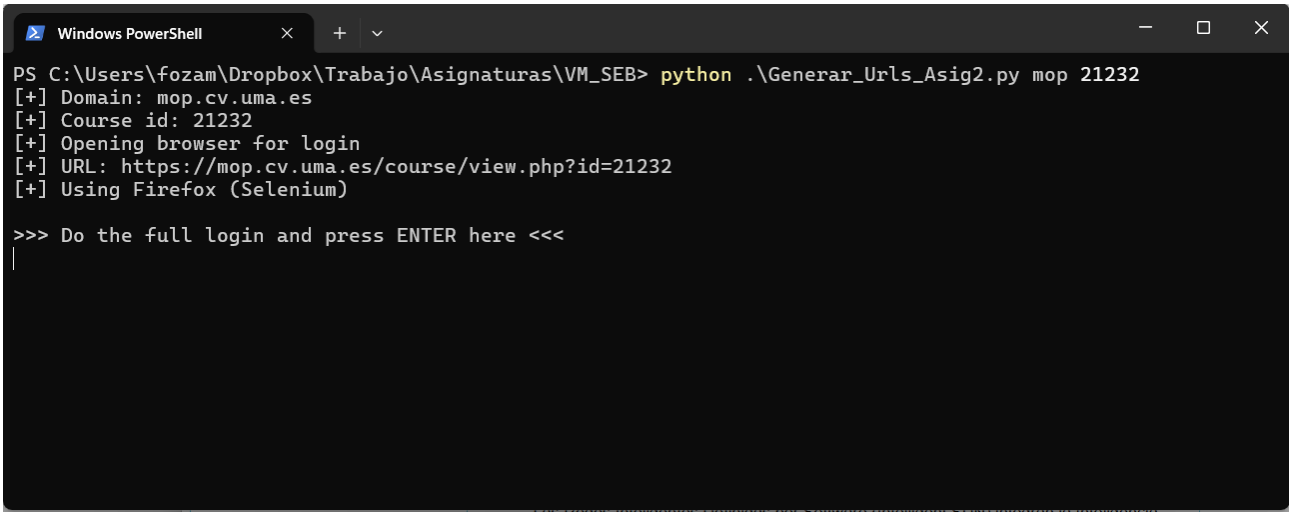

Fig. 20 Inicio del proceso de extracción de URLs.

Al comenzar la ejecución, el programa abre automáticamente una ventana del navegador para realizar el inicio de sesión en el Campus Virtual, como se muestra en la Figura 5. Una vez que el usuario ha completado el "login" manualmente en el navegador y la sesión ha quedado correctamente iniciada (Figura 6), debe volver a la terminal.

Tras completar el inicio de sesión, el usuario debe pulsar "*ENTER*" en la terminal para que el programa continúe con el proceso de extracción y analice todos los enlaces de la asignatura.

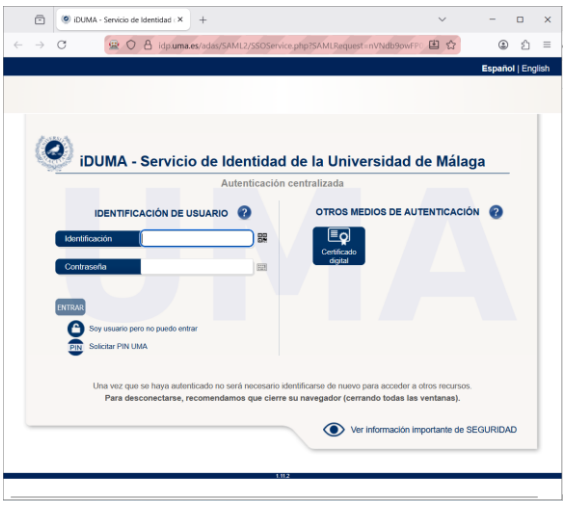

Fig. 21 Pantalla de inicio de sesión en el Campus Virtual.

Fig. 22 Inicio de sesión completado correctamente.

A continuación, el programa ejecuta automáticamente el escaneo completo de la asignatura. Durante este proceso, se debe esperar a que finalice la ejecución, tal y como se observa en la Figura 7.

Una vez finalizado el proceso, el programa genera un archivo de texto (.txt) que contiene todas las URLs detectadas exclusivamente de esa asignatura.

El archivo generado tiene el siguiente formato de nombre: URLs_<codigo>.txt

donde <codigo> corresponde al código numérico de la asignatura.

Este archivo .txt puede copiarse directamente en el apartado ***"URLs permitidas"*** de la configuración de SEB (paso 4 de la Figura 1), permitiendo al alumnado navegar por todos los contenidos de la asignatura dentro del Campus Virtual de forma controlada.

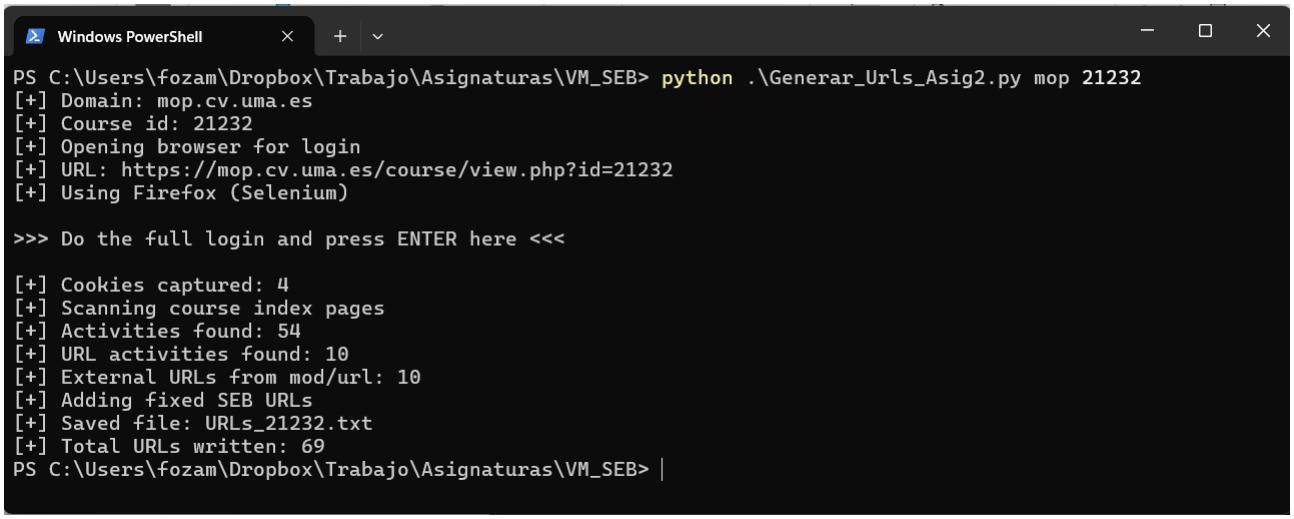

Fig. 23 Archivo de URLs generado por el programa.

Uso del programa *Generar_Seb.py*

El programa Generar_Seb.py permite automatizar la creación de un archivo de configuración SEB con las URLs permitidas del examen, evitando tener que copiarlas manualmente en la pestaña Network de la ***SEB Configuration Tool***.

A partir de un archivo de configuración base .seb (plantilla), el programa genera un nuevo archivo .seb que mantiene toda la configuración original (aplicaciones permitidas, restricciones, etc.) y añade automáticamente las URLs incluidas en uno o varios archivos de texto.

El archivo resultante se crea con el mismo nombre del archivo base, añadiendo el sufijo URL antes de la extensión:

- Entrada: *ConfSDMN.seb*
- Salida: *ConfSDMNURL.seb*

Tal como se muestra en la Figura 24, el programa confirma la creación del nuevo archivo.

Ejecución

El programa se ejecuta indicando:

1. El archivo .seb base (plantilla).
2. Uno o varios archivos .txt con URLs.

Ejemplo:

```
$ python .\Generar_Seb.py ConfSDMN.seb URLs_21232.txt URLs_21232_Ext.txt
```

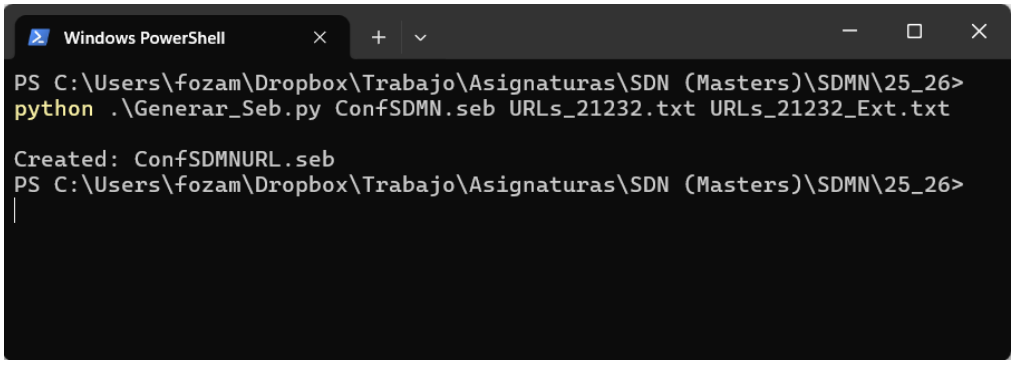

Fig. 24 Creación automática del archivo .seb con URLs incorporadas.

Tratamiento de URLs: comodines y coincidencia exacta

El programa inserta las URLs en el filtrado de SEB según el formato de cada línea del .txt:

- **URLs con asterisco *** Se insertan como "expresiones normales" (patrones). Esto permite la subnavegación, es decir, se autoriza la URL y también las rutas derivadas que coincidan con el patrón (por ejemplo, recursos internos asociados).
- **URLs sin asterisco.** Se insertan como "expresiones regulares" para que la navegación sea exacta. En este caso, solo se permitirá acceder a esa dirección concreta, evitando que se puedan visitar variantes derivadas o rutas adicionales.

Este comportamiento permite combinar, en una misma configuración, URLs amplias (con comodines) para permitir secciones completas del Campus Virtual, y URLs estrictas (sin comodines) cuando se necesita un control más restrictivo.

Uso del programa *Generar_Json_Firefox.py*

El programa **Generar_Json_Firefox.py** permite generar el archivo *policies.json* necesario para aplicar las políticas de control del navegador Firefox en las máquinas virtuales del aula. Dichas políticas incluyen el bloqueo de extensiones y la restricción del acceso a Internet según el modo seleccionado.

El programa debe ejecutarse desde un equipo de administración y el archivo generado debe copiarse posteriormente a las máquinas del aula.

Ejecución

El programa se ejecuta desde terminal mediante el siguiente formato general:

```
$ python3 Generar_Json_Firefox.py [opciones] [archivos_txt]
```

Dependiendo del modo seleccionado, se utilizarán distintas opciones.

- **Modo whitelist (permitir solo URLs específicas)**

  Este modo permite bloquear todo el acceso a Internet excepto las direcciones web indicadas en uno o varios archivos de texto. Cada archivo de texto debe contener una URL por línea.

  ```
  $ python3 Generar_Json_Firefox.py urls.txt
  ```

  El resultado es que se bloquea todo el tráfico web excepto el que se ha permitido en las URLs indicadas y además se bloquea la instalación de extensiones.

- **Modo permitir todo el acceso (-allow)**

  Este modo permite el acceso completo a Internet, manteniendo el bloqueo de extensiones.

  ```
  $ python3 Generar_Json_Firefox.py -allow
  ```

  El resultado es que se permite el acceso a todas las páginas web y se mantiene el bloqueo de extensiones (para uso "normal" en las clases prácticas).

- **Modo bloqueo total (-block)**

  Este modo bloquea completamente el acceso a Internet desde Firefox.

  ```
  python3 Generar_Json_Firefox.py -block
  ```

  El resultado es que se bloquea todo el tráfico web no permitiendo acceder a ninguna URL y además se mantiene el bloqueo de extensiones.

Tras la ejecución del programa, se genera el archivo *policies.json* (ver Fig 25) en el mismo directorio donde se ejecuta el script.

policies.json

```
{
    "policies": {
        "ExtensionSettings": {
            "*": {
                "installation_mode": "blocked"
            }
        },
        "DisablePrivateBrowsing": true,
        "DisableFirefoxAccounts": true,
        "DisableDeveloperTools": true,
        "WebsiteFilter": {
            "Block": [
                "<all_urls>"
            ],
            "Exceptions": [
                "https://auth.netacad.com/*"
            ]
        }
    }
}
```

Fig. 25. Configuración de políticas del navegador para bloqueo de extensiones y control de navegación