**Actividad Evaluable Herramientas DLP**



Daniel Escaño Hernández CET Ciberseguridad

# **Índice**

[**Índice**](#_u3m2w22qmzkq) **1**

[**1. Tabla Comparativa**](#_yby49ic4bcux) **2**

[**2. Instalación Herramienta DLP**](#_z6v250u8eg2k) **4**

[**2.1 Instalación**](#_i92etluu9ojk) **4**

[**2.2 Bloqueo USB**](#_1t4f9z8i9xbn) **5**

[**2.3 Regla HTTP y Navegación por Internet**](#_c56aua9tk0gb) **6**

# **1. Tabla Comparativa**

**Busca información acerca de diferentes programas DLP, documenta sus características, y haz una tabla comparativa entre ellos.**

Compararemos las características, ventajas y desventajas de 4 softwares seleccionados, siendo “Kickidler”, “Endpoint Protector DLP”, “Safetica DLP” y “McAfee Total Protection for DLP”.

|  | **Kickidler** | **Endpoint Protector DLP** |
| --- | --- | --- |
| **Características** | Potentes herramientas de análisis e informes que ayudan a supervisar el comportamiento digital de los empleados en el trabajo.  Seguimiento de las horas de trabajo de los empleados  Visión general de los procesos internos y de las estadísticas importantes en forma de cómodos gráficos y tablas.  Exportación de informes. | Protección basada en el contenido (escaneo contextual en tiempo real de los datos de los dispositivos multimedia extraíbles, capturas de pantalla, contenido de Outlook, conversaciones de Skype y archivos de Dropbox).  Gestión de USB y periféricos |
| **Ventajas** | Increíblemente rentable. Diseñado con procedimientos que cumplen con los estándares de privacidad de datos del Reglamento General de Protección de Datos | Disponible como servicio en la nube y como aplicación virtual. Tiene un bajo uso de recursos |
| **Desventajas** | No hay versión móvil. La versión en la nube no está disponible por ahora. | No hay versión gratuita. Políticas de precios imprecisas. |

|  | **Safetica DLP** | **McAfee Total Protection for DLP** |
| --- | --- | --- |
| **Características** | Análisis de contenido mediante palabras clave específicas.  Auditoría de seguridad.  Protección de datos en la nube.  Un conjunto de modos informativos y alertas a los empleados que proporcionan un control total del entorno de la empresa y crean conciencia por parte del usuario. | Poderosa función de clasificación de datos que ayuda a identificar y clasificar los datos.  Cifrado, redirección, cuarentena o bloqueo de las transmisiones de datos que infringen las políticas de la empresa.  Clasificación flexible de los usuarios finales.  Consola centralizada para la gestión de políticas e incidentes. |
| **Ventajas** | Interfaz fácil de usar. Versatilidad de los informes que ayudan a simplificar el análisis de los datos. Buena atención al cliente. | Seguimiento de datos en tiempo real. Buenas capacidades de detección. Configuración de políticas fácil y sencilla. |
| **Desventajas** | La interfaz es mejorable, ya que al principio puede resultar difícil utilizar la consola con sus numerosos módulos. Un poco caro. Sólo ofrece soporte en línea. | Puede ser un poco complejo y poco intuitivo para algunos usuarios. Los bloqueadores de pops pueden ser molestos. |

# **2. Instalación Herramienta DLP**

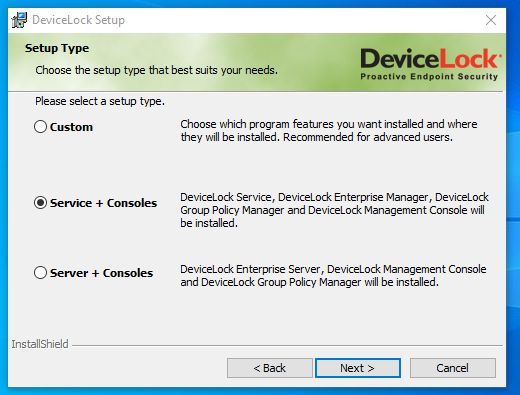
**Indica cuál escogerías para una PYME, instala el software en una máquina virtual y prueba su funcionalidad.**

### **2.1 Instalación**

Para el caso de una PYME escogería el software “Acronis DeviceLock DLP”, procederemos a su instalación.

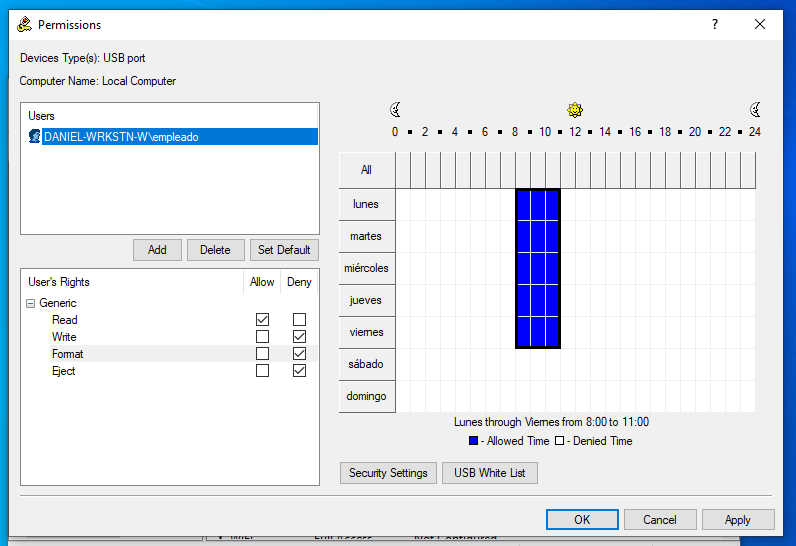
Principalmente porque ofrece muchas utilidades interesantes que podemos aplicar a nuestra empresa para mejorar su rendimiento general.

En mi opinión, se trata de una buena elección ya que entre otras ventajas que comparte con otras opciones antes mencionadas, el software resulta en líneas generales, completo, intuitivo, eficaz y económico.

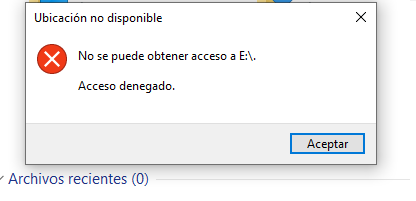


### **2.2 Bloqueo USB**

Crearemos una regla que impida la escritura y formateo de los dispositivos USB en un horario limitado, en este caso únicamente se permitirá el uso de estos dispositivos de Lunes a Viernes de 8:00 a 11:00, que son las horas que hipotéticamente se encontraba presente el supervisor.



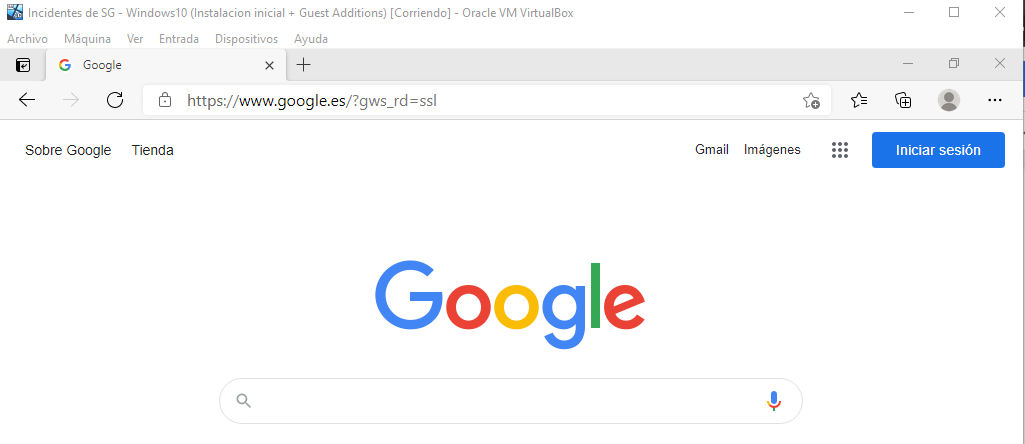
Comprobamos que funciona:

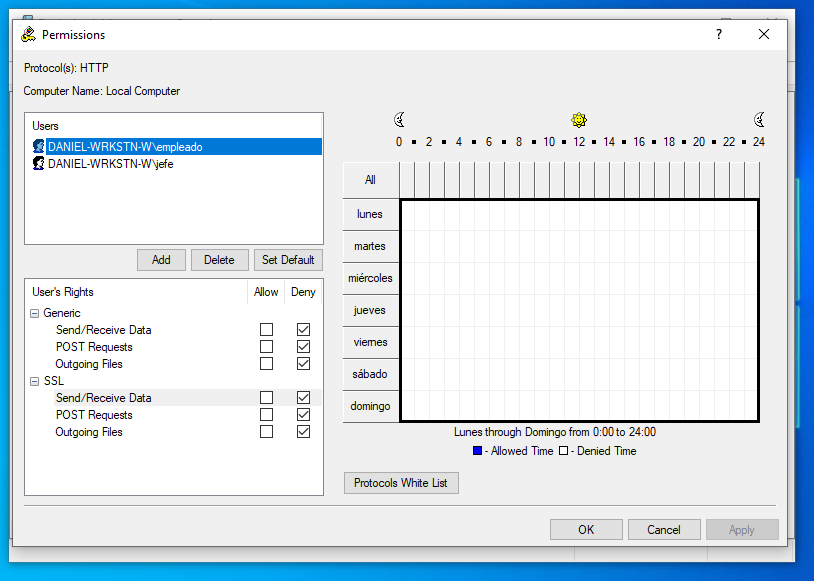


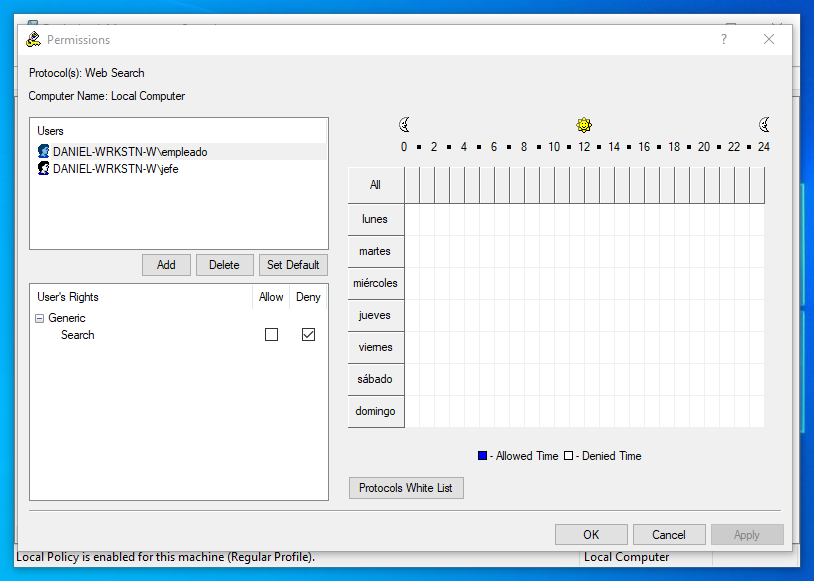
### **2.3 Regla HTTP y Navegación por Internet**

Ahora, instauramos un bloqueo de protocolo HTTP, impidiendo así a los empleados recibir malware a través de este protocolo ni navegar por internet, para evitar un riesgo o exposición.

Comprobamos que podemos navegar:







Finalmente comprobamos su funcionamiento:

