Para que Splunk pueda recibir eventos de auditoría de Windows Server, deberemos configurar las políticas de auditoría de una manera específica. La mejor forma de hacerlo es correr con el Administrador del servidor este script de la siguiente forma:

```
Invoke-Expression (Invoke-WebRequest -Uri "https://raw.githubusercontent.com/nipegun/ws-scripts/main/PostInst/CrearPoliticasParaAuditarConSplunk.ps1" -UseBasicParsing).Content
```

El script nos generará un CSV en el escritorio que deberemos importar en la sección «Configuración de seguridad >> Configuración de directiva de auditoría avanzada >> Directivas de auditoría del sistema», en la ventana de **secpol.msc**. Después de importarlo el servidor Windows enviará dichos eventos al servidor Splunk.

Pero antes, deberemos instalar en el WinServer el paquete Splunk Universal Forwarder.

Al momento de instalar marcaremos que aceptamos la licencia y nos aseguraremos de que la instalación sea de tipo on-premise. Luego procederemos con la personalización de opciones. Daremos Next hasta que lleguemos al tipo de instalación, donde nos aseguraremos que «Local System» esté marcado. En la ventana siguiente marcaremos, al menos:

- Application logs
- Security log
- System log
- Forwarded events log
- Setup log
- Enable AD monitoring

También, si queremos monitorizar la performance, podemos marcar algunas cosas de la derecha.

En la ventana siguiente creamos nuestro usuario y contraseña para, finalmente, en la ventana de «Receiving indexer», poner la IP y el puerto de escucha de nuestro Splunk.