

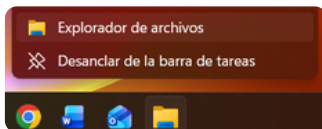
RECUPERACIÓN DE BITÁCORAS DEL SISTEMA EN WINDOWS

Para que el UNAM-CERT pueda realizar el análisis correspondiente después de un incidente de seguridad en un dispositivo con sistema operativo Windows, es necesario recuperar las bitácoras del sistema.

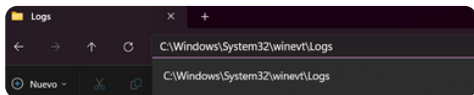


Para recuperar estas bitácoras puedes seguir los siguientes pasos:

1. Desde tu computadora Windows abre un Explorador de Archivos:

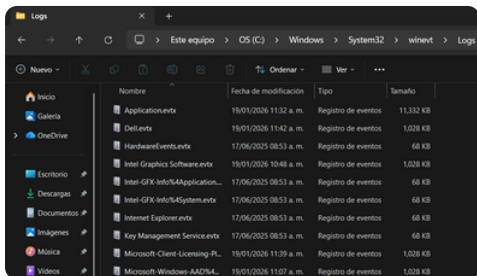


2. En la barra de Ubicaciones coloca la ruta **C:\Windows\System32\winevt\Logs** (Windows Vista, 7, 8, 10, 11 y Windows Server).



Para Windows XP y versiones anteriores, coloca la ruta **C:\Windows\System32\config**

3. Dentro del directorio se encuentran archivos (.evtx), cada uno corresponde a una bitácora del sistema.



4. Es necesario enviar todos las bitácoras de este directorio en un archivo comprimido al correo:

csi.incidentes@unam.mx