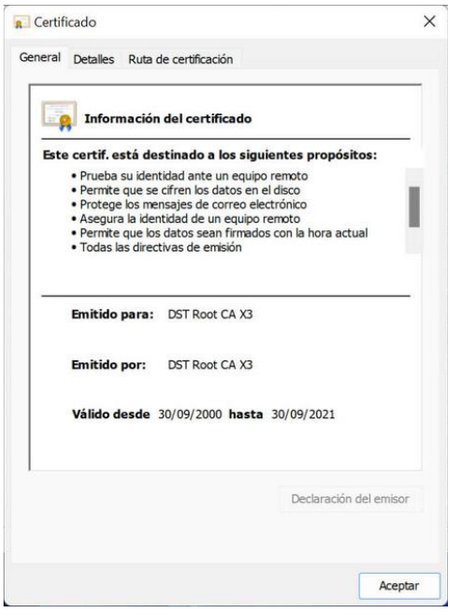
Gran número de dispositivos no podrán conectarse a internet este 30 de septiembre cuando caduque uno de los primeros certificados SSL emitidos

Let's Encrypt es una organización sin fines de lucro que emite certificados que **encriptan las conexiones** de los dispositivos con internet, garantizando que en este diálogo los datos del usuario no puedan ser interceptados ni robados.

Los certificados de *Let´s Encryt* se encuentran en el 30% de todos los dominios existentes. Uno de sus certificados más antigüos, el **CA de DST Root CA X3,** vence este 30 de septiembre por lo que ocasionará errores tan sencillos como que el navegador reciba una advertencia por la falta o incompatibilidad del certificado hasta problemas tan complejos como que los dispositivos que lo utilizan sean incapaces de conectarse al internet.

Muchos de los dispositivos que usamos habitualmente no deben tener problema si los hemos actualizado de manera regular. Sin embargo existen otros que pueden requerir mayor atención para evitar que terminen como pisapapeles.

Para ello será necesario realizar una actualización de software y firmware de los dispositivos:



- Windows menores a XP SP3
- MacOS menores a 10.12.1
- iOS menores al sistema 10 (el iPhone 5 como modelo más antiguo puede actualizarse hasta el iOS 10)
- Android menores a 7.1.1 (aunque los inferiores a 2.3.6 continuarán funcionando con certificado ISRG Root X1 con señal cruzada)
- Mozilla Firefox menor a la versión 50
- Java por debajo de versión 8

Según el experto Scott Helme, los clientes que seguirán afectados por esta caducidad son "todos lo que dependan de la librería OpenSSL 1.0.2 o anterior, lanzada el 22 de enero de 2015 y actualizada por última vez como OpenSSL 1.0.2u el 20 de diciembre de 2019", advierte el experto en su post.

Entre los posibles aparatos afectados se encuentran:

- El teléfono móvil Blackberry, con versiones menores a 10.3.3
- El sistema operativo Jolla Sailfish OS, inferior a 1.1.2.16
- La consola PS 4 con 'firmware' o inferior, etc. (más consolas de generaciones previas que no fueron actualizadas a los 'firmware' recientes)

Hay que considerar que "como los dispositivos Android antiguos no comprueban la fecha de caducidad de un certificado raíz cuando lo utilizan, **Let's Encrypt** puede seguir encadenándolos hasta el certificado raíz caducado, sin ningún problema en esos dispositivos antiguos", según explica Helme.

En lo que refiere al nuevo certificado, se denomina ISRG Root X1 con firma cruzada y tendrá vigencia hasta el **30 de septiembre de 2024**. Para volver a establecer conexiones seguras a Internet, hará falta actualizarlo en dispositivos antiguos.

La principal herramienta para protegernos y a nuestras organizaciones es el conocimiento y la prevención.

Mantener nuestros equipos actualizados, capacitar a nuestro personal, contar con una estrategia de Ciberseguridad, y tener una asesoría adecuada por especialistas es esencial para una operación adecuada, sin intrusos en nuestros sistemas.