1) El sitio que puede usar este certificado es ***.mercadolibre.com***. El ***** implica que puede haber cualquier palabra detrás del resto de la URL.

2) La **digital signature** es un mecanismo para soportar servicios de seguridad que no sean **Certificate signing** (bit 5) o **CRL signing** (bit 6). El **key encipherment** es asegurado cuando la key pública del sujeto es usada para el tráfico de otras key.

3) Las fechas del certificado son las siguientes:
   No valido antes de: 2020-02-18
   No válido después de: 2022-02-22
   Cuando un certificado SSL expira, esto implica que a partir de ese momento se empieza a mostrar una advertencia cuando un usuario quiere entrar en la pagina web, que dice que el tráfico en este sitio no es seguro. Esto genera un gran impacto en sitios que son de empresas importantes, como lo sería en nuestro caso Mercado Libre.

4) El algoritmo que usa este certificado es el **RSA**, que es un algoritmo **asimétrico**. Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto