

UNAM ADMIN UNAM 2016

Certificados Digitales SSL para la UNAM

Mtra. Lizbeth Angélica Barreto Zúñiga

Mtro. Alejandro Gerbacio Gerbacio



Funciones DGTIC

“Orientar a las entidades y dependencias universitarias en la gestión de infraestructura y soluciones de cómputo y telecomunicaciones”.

noviembre 2015

Problemática de los certificados SSL

- No existen criterios uniformes para adquisición.
- Diversidad de proveedores, niveles de cifrado y características.
- Es común encontrar sitios con:
 - Certificados SSL autofirmados
 - Escasa protección
 - Validez nula al exterior
- Escasos certificados SSL.

Causas

- Regularmente los certificados SSL son “caros”.
- Limitados o nulos recursos para adquirirlos.
- Complicada justificación de compra.
- Desconocimiento de uso, configuración, beneficios y relevancia de los certificados.
- Priorización a otros gastos.



¿Qué servicios o páginas deben tener un SSL?

- Manejo de **información sensible o crítica** (datos personales privados, dinero, documentos confidenciales).
- Requieren garantizar la **integridad de los datos** evitando que se intercepte la información.
- Deben garantizar a los usuarios la **autenticidad** de su **identidad** y evitar la **suplantación**.
- Por **normatividad** UNAM, nacionales e internacionales en materia de privacidad, seguridad e integridad de los datos.

Gestor central de certificados SSL

- DGTIC como gestor central de certificados SSL para la UNAM
 - Experiencia técnica.
 - Acorde a sus funciones.

Objetivo:

Establecer la norma y regularizar el proceso para la adquisición de certificados SSL en la UNAM.

RFP Certificados

UNAM CERT y Firma Electrónica Avanzada elaboraron un RFP con:

- Criterios mínimos de aceptación.
- Bajo costo operativo para la UNAM.
- Mayor cobertura.
- Tecnología de última generación.
- Administración centralizada.

Características de los certificados

- Nivel de Validación Organizacional.
- Soporte para el algoritmo SHA-1 y SHA-256.
- Cifrado de Raíz de 2048 bit (RSA y ECC).
- Potencia de cifrado mínimo de 128 bits y máximo de 256 bits.
- Autenticación de organización completa .
- Soporte a multiplataforma.
- Compatibilidad universal con principales navegadores.
- Dispositivos móviles.

Esquema de operación

1. Entidad o dependencia solicita por oficio a DGTIC los certificados con justificación técnica.
2. DGTIC analiza justificación y, en su caso, autoriza certificado.
3. El costo de los certificados será de **recuperación**.
 - **DGTIC** realizó negociación a un precio preferente
 - No existe presupuesto asignado previamente para tal efecto
4. DGTIC proveerá soporte remoto para la instalación.
5. Certificados serán entregados de **3 a 5 días hábiles** a partir de la transferencia de recursos.
6. Entidad o dependencia debe considerar que la renovación del certificado es ANUAL.

Mtra. Lizbeth Angélica Barreto Zúñiga

Mtro. Alejandro Gerbacio Gerbacio

DGTIC – UNAM

dudas_firma@unam.mx



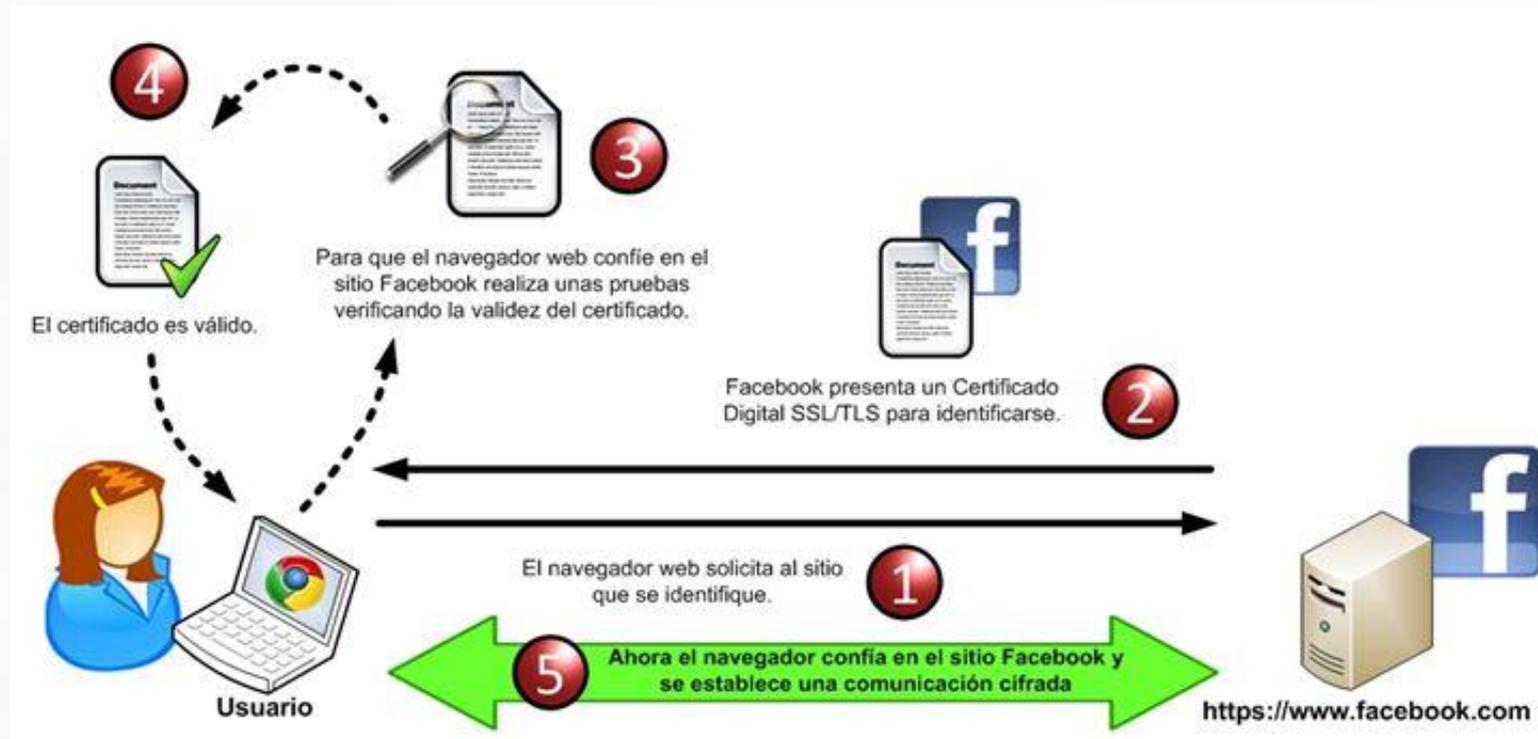
@feaunam

56 22 35 99

¿Quién es el proveedor?

- Acreditación mundial Webtrust.
- Miembro de Trust Alliance Online y de Grupo de trabajo Anti – phishing.
- Premio Oro al Auto Registro Corporativo como Producto de seguridad más innovador en RSA 2016 emitido por Info Security.

Como funciona un SSL



fuelle: <http://revista.seguridad.unam.mx/numero-10/el-cifrado-web-sslts>