



Manual: Guía de instalación del certificado *Fortinet* para navegación web segura en dispositivos *Windows, Mac, Android, iOS*

**Karen Lucero Roldán Serrato
Alethia Patricia Estrella Ruiz
Emmanuel Gómez Cantoya
2022**

Financiamiento (interno)

Manual: Manual: Guía de instalación del certificado Fortinet para navegación web segura en dispositivos Windows, Mac, Android, iOS

Karen Lucero Roldán Serrato, Alethia Patricia Estrella Ruiz, Emmanuel Gómez Cantoya

Instituto de Ciencias Aplicadas y Tecnología, Circuito Exterior S/N, C.P. 04510,
A.P.70- 186, Universidad Nacional Autónoma de México, CDMX, México.

Resumen

Este documento presenta el procedimiento para la instalación y configuración del certificado Fortinet para navegación web segura en dispositivos Windows, Mac, Android, iOS para conexiones inalámbricas (WLAN), la cual es una herramienta asociada a la seguridad perimetral de la red local de datos. La finalidad de la configuración del certificado en los dispositivos móviles es realizar la validación correcta de la navegación de los usuarios sobre las visitas sobre los sitios web con el fin de brindar protección contra amenazas en la red (*Phishing, Man in the middle* y etc.), así como, para garantizar la conexión y navegación segura.

Índice

Resumen	1
Nomenclatura	3
Introducción	4
Especificaciones	4
1. Guía de instalación del certificado Fortinet para navegación web segura en dispositivos Android	6
2. Guía de instalación del certificado Fortinet para navegación web segura en dispositivos iOS.....	8
3. Guía de instalación del certificado Fortinet para navegación web segura en dispositivos Mac OS	113
4. Guía de instalación del certificado Fortinet para navegación web segura en dispositivos Windows	146
Anexo. Instalación alternativa de forma directa	21
Referencias.....	26

Nomenclatura

Android	Es un sistema operativo que se emplea en dispositivos móviles, por lo general con pantalla táctil (GOOGLE, 2021).
Autoridad de certificación	Empresa u organización que actúa para validar las identidades de sitios web y etc., vincularlas a claves criptográficas mediante la emisión de Certificados digitales (DESCOM, 2002).
BYOD	<i>Bring Your Own Device, Conexión sobre traer tu propio dispositivo [Rouse, 2017].</i>
Certificado SSL	Es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada entre un servidor web y un navegador web. (<i>Secure Sockets Layer</i>) [DESCOM, 2002].
Cifrado	Es la conversión de datos de un formato legible a un formato codificado. Los datos cifrados solo se pueden leer o procesar luego de descifrarlos permitiendo garantizar que la seguridad en la información [KASPERSKY, 2022].
Dirección MAC	es un identificador de 48 bits (6 bloques de dos caracteres hexadecimales [8 bits]) (Rouse, 2017)
Fortinet	Plataforma de seguridad perimetral para redes de voz y datos, a través de firewalls, antivirus, prevención de intrusiones y seguridad en dispositivos y etc [FORTINET, 2022].
GUEST	Conexiones tipo invitado son las que tienen un tiempo limitado y es para visitantes que requieran conexión a internet temporal (Rouse, 2017).
https	Protocolo seguro de transferencia de hipertexto, es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus dispositivos y el sitio web [GOOGLE, 2022].
iOS	Es un sistema operativo para dispositivos móviles de la multinacional Apple Inc [GOOGLE, 2021].
Internet	<i>Es una conexión entre equipos para comunicación y ofrecer servicios [Rouse, 2017]</i>
MacOS	Es una serie de sistemas operativos gráficos para computadoras desarrollados y comercializados por Apple Inc [GOOGLE, 2021].
Man in the middle	<i>Es la técnica de robo de información valiosa para los usuarios a través de páginas Web o acceso a bases de datos en los sitios de almacenamiento [Malekovich, 2013]</i>
OCSP	<i>(Online Certificate Status Protocol) Es un protocolo que permite validar el estado de un certificado en su entidad certificadora. Comprobando que es correcto y que no está revocado, garantizando una mayor seguridad en las transacciones. Este estado es útil tanto en certificados SSL como certificados de firma digital [DESCOM, 2002].</i>
Phishing	<i>Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con la intención de debilitar su buen juicio al infundirle miedo. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia [Malwarebytes, 2022].</i>
VLAN	<i>Es una red virtual local la cual nos permite segmentar o distribuir el tráfico por líneas virtuales de comunicación (CISCO, 2006).</i>
Windows	Es el nombre de una familia de distribuciones de software para PC, servidores, sistemas empujados y antiguamente teléfonos inteligentes desarrollados y vendidos por Microsoft [GOOGLE, 2021].

Introducción

Al acceder a una página segura (*https*) o cuando recibimos una firma digital por correo, nuestro navegador o cliente de correo verifica cual es el servidor *OCSP* que debe responder para validar el certificado [SSL, 2021]. Por lo que, los certificados son documentos digitales que se vinculan a una clave pública para un sujeto individual. El enlace se asegura al tener una autoridad de certificación (CA) confiable como SSL.com que verifica la identidad de los posibles propietarios de certificados, a través de validaciones automáticas y manuales contra bases de datos calificadas, donde se establece una conexión remota y se verifica la validez del certificado. Con ello conseguimos un método que valida que el sitio o remitente de correo son los que dicen ser y que la transacción segura es realmente segura [KASPERSKY, 2022].

Cuando una página Web este cifrada es con el fin de ofrecer una infraestructura digital para el comercio electrónico o intercambio de información sensible, la velocidad de esta se ve afecta por la conexión que se establece mediante el protocolo *OCSP*, por lo cual el tiempo medio de respuesta de los *OCSP* tiene un valor importante en la respuesta de nuestra página web. El protocolo *OCSP*, nos permite validar el estado de un certificado en su entidad certificadora, comprobando que es correcto y que no está revocado, permitiendo una mayor seguridad en las transacciones. Este estado es útil tanto en certificados SSL como certificados de firma digital (Figura 1). El funcionamiento de este protocolo se describe a través del protocolo RFC 2560 [SSL, 2021; KASPERSKY, 2022].

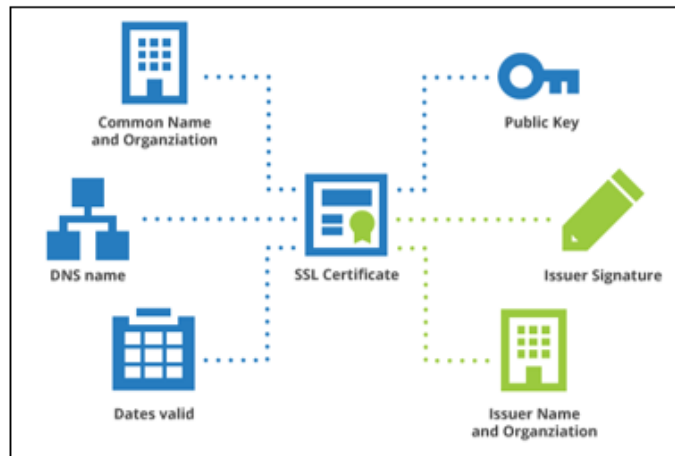


Figura 1. Diagrama de flujo de un certificado SSL. (SSL, 2021).

La intención de la instalación de este certificado de seguridad es crear compatibilidad de la seguridad perimetral y la navegación del dispositivo creando un canal seguro y estable de monitoreo y validación de tráfico de cada dispositivo.

La intención de este manual es dar la pauta al usuario para la instalación del certificado de seguridad con el fin de lograr una navegación en el dispositivo de la conexión local.

Especificaciones

1. Guía de instalación del certificado Fortinet para navegación web segura en dispositivos Android

- a. Ingresar al sitio <https://www.icat.unam.mx/> dar clic en la sección **Utilería** para descargar y guardar el certificado de navegación segura **Fortinet_CA_SSL.cer** (Figura 2).

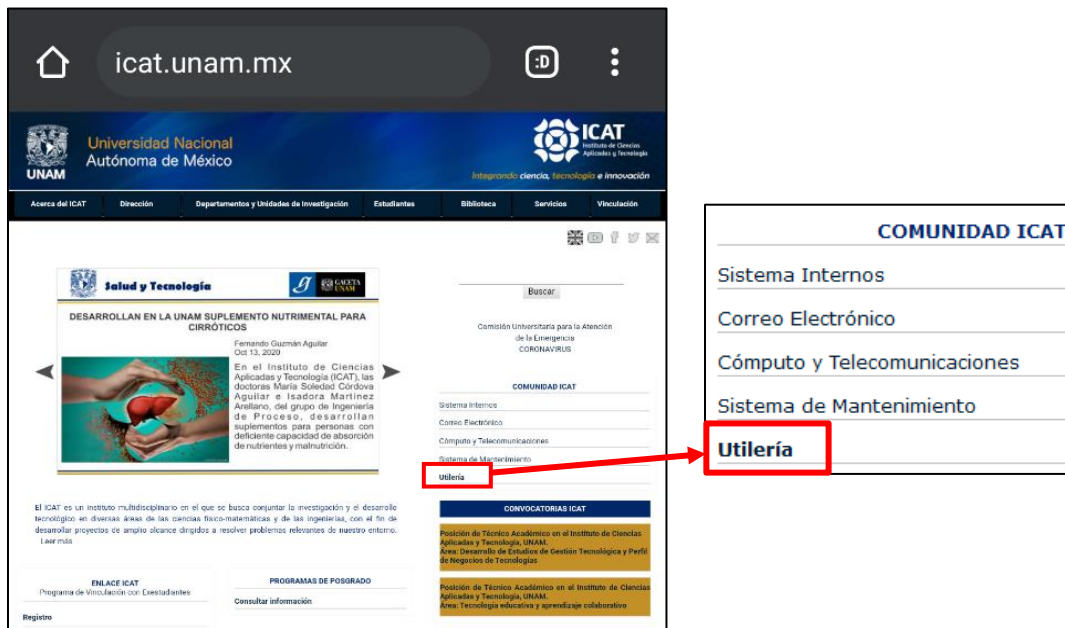


Figura 2. Localización del área de descarga. Elaboración propia.

- b. Una vez finalizada la descarga, el dispositivo enviará una notificación de **descarga completa**, dar clic sobre **Fortinet_CA_SSL.cer** (Figura 3):

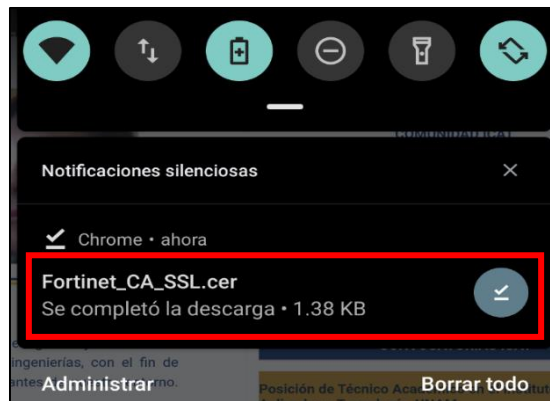


Figura 3. Descarga exitosa del certificado. Elaboración propia.

- c. Instalación y configuración de certificado. A continuación, se abrirá una ventana flotante donde deberá llenar los siguientes datos y después dar clic en Aceptar (Figura 4):

Nombre del certificado: ICAT

Uso de credenciales: Seleccionar Wi-Fi

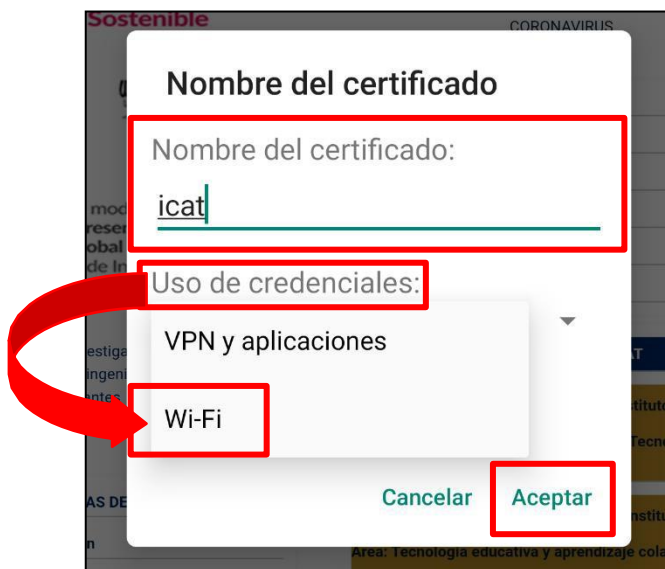


Figura 4. Instalación de certificado en sistema Android. Elaboración propia.

Daremos doble clic en él para abrir las opciones de configuración y en la sección **Tipo de inicio** seleccionaremos **Automático**.

2. Guía de instalación del certificado Fortinet para navegación web segura en dispositivos iOS

Ingresa al sitio <https://www.icat.unam.mx/> y da clic en la sección **Utilería** para descargar y guardar el certificado de navegación segura Fortinet_CA_SSL.cer.

Se abrirá una ventana para confirmar la descarga del certificado de seguridad, da clic en **Permitir** (Figura 5).

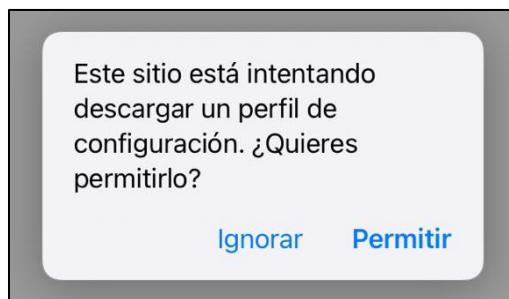


Figura 5. Confirmación de descarga del certificado. Elaboración propia.

2.- Instalación y configuración del certificado de seguridad

Al finalizar la descarga aparecerá una ventana de notificación, da clic en **Cerrar** (Figura 6).

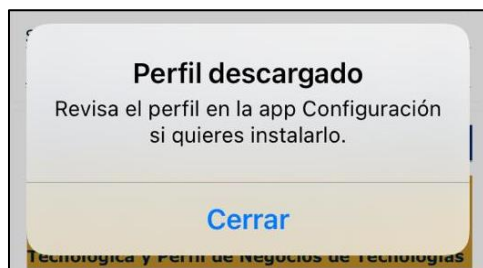


Figura 6. Confirmación de descarga exitosa. Elaboración propia.

A continuación, deberá abrir el menú **Ajustes del teléfono**, entrar al submenú **General** y seleccionar **Perfil** (Figura 7).



Figura 7. Localización de la sección Perfil en el submenú General. Elaboración propia.

En seguida se mostrará información del certificado de seguridad bajo la pestaña Perfil descargado y el nombre del certificado **FG1KDT918801453** (dependiendo de la versión de iOS instalada el nombre del certificado podría variar un poco), dar clic sobre el mismo (Figura 8).



Figura 8. Certificado descargado bajo la pestaña Perfil. Elaboración propia.

Se abrirá el asistente de instalación del perfil de seguridad, daremos clic en **Instalar** (Figura 9).



Figura 9. Instalación del perfil de seguridad. Elaboración propia.

Se abrirá una ventana de confirmación solicitando el **código de acceso o desbloqueo** del dispositivo, lo ingresaremos para continuar con la instalación (Figura 10).



Figura 10. Ventana de ingreso de código de desbloqueo del dispositivo. Elaboración propia.

A continuación, se mostrará una notificación de advertencia ya que estamos a punto de agregar el certificado de seguridad a la lista de confianza del dispositivo, ya que el certificado pertenece al equipo de seguridad informática **Fortinet**, de la red del ICAT, podemos estar seguros de la validez y veracidad de dicho certificado, por lo que daremos clic en **Instalar** (Figura 11).



Figura 11. Instalación del certificado de seguridad. Elaboración propia.

Deberemos confirmar una vez más dando clic en **Instalar** (Figura 12).



Figura 12. Localización del área de descarga. Elaboración propia.

Se mostrará la ventana de **Perfil instalado** con información del proceso que acabamos de realizar y la leyenda en verde **Verificado**, confirmando que el certificado de seguridad ha sido correctamente instalado, daremos clic en **Listo** para terminar el proceso (Figura 13).



Figura 13. Instalación exitosa del certificado de seguridad. Elaboración propia.

Nota final: Es necesario cerrar y volver a abrir el navegador web para aplicar los cambios

3. Guía de instalación del certificado Fortinet para navegación web segura en dispositivos Mac OS

Ingresar al sitio <https://www.icat.unam.mx/> y dar clic en la sección **Utilería** para descargar y guardar el certificado de navegación segura **Fortinet_CA_SSL.cer** (Figura 14).

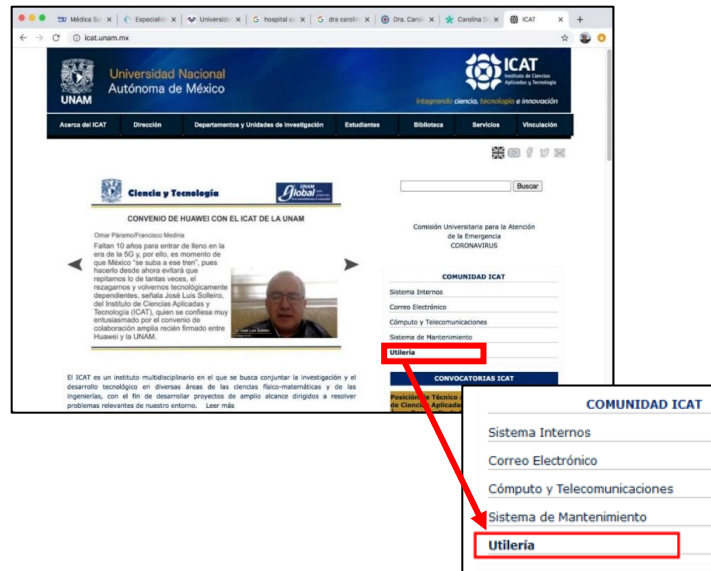


Figura 14. Localización del área de descarga. Elaboración propia.

Se abrirá una ventana preguntando en qué lugar se desea guardar el certificado **Fortinet_CA_SSL.cer**, lo guardaremos en el escritorio para su fácil localización posterior (Figura 15).

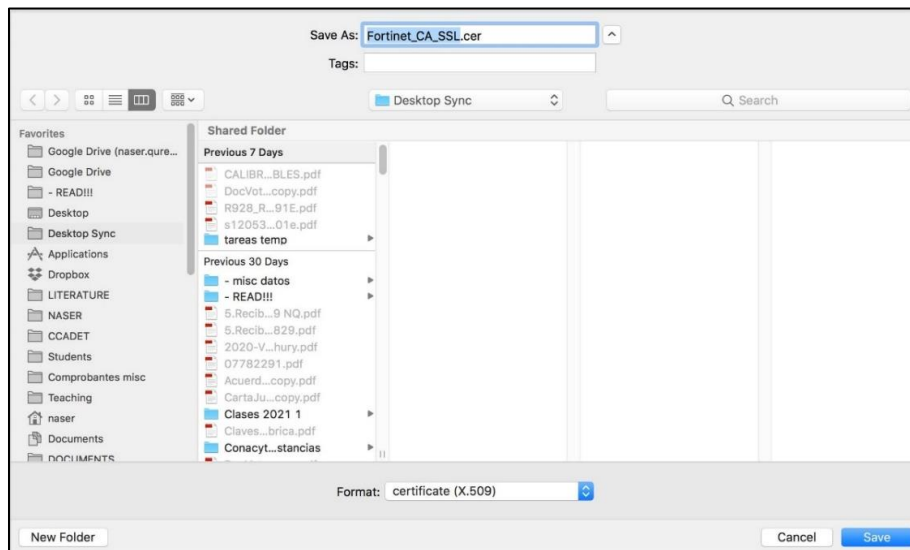


Figura 15. Guardado del certificado en la carpeta de Descargas. Elaboración propia.

2.- Instalación y configuración

Una vez finalizada la descarga, ejecutaremos el archivo **Fortinet_CA_SSL.cer** para iniciar la instalación (Figura 16).

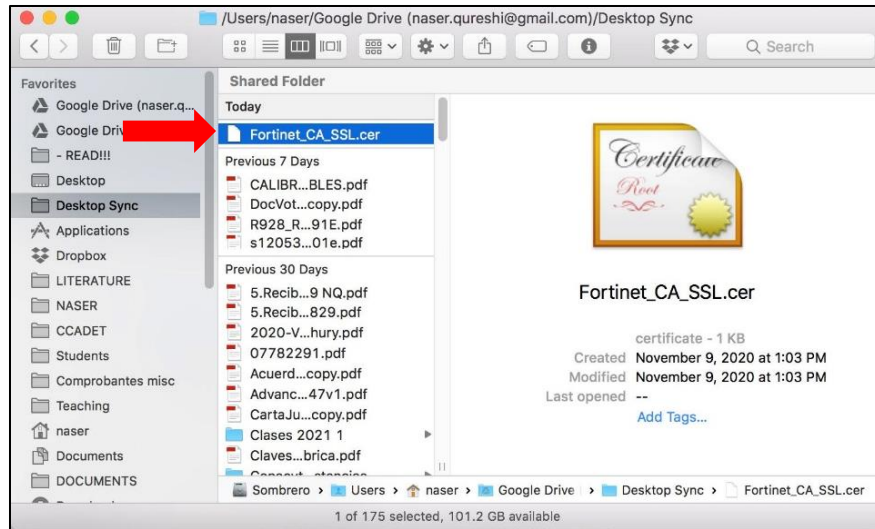


Figura 16. Ubicación de la descarga del Certificado. Elaboración propia.

A continuación, se abrirá la aplicación de administración **“Llaveros”** o **“Keychain Access”** según la configuración de idioma del dispositivo Mac OS.

Dentro de esta aplicación nos ubicaremos en el directorio **System** o **Sistema** dando clic sobre él y después de encontrar el certificado **FG1K2DT918801453** daremos clic sobre él nuevamente para configurarlo. (Figura 17).

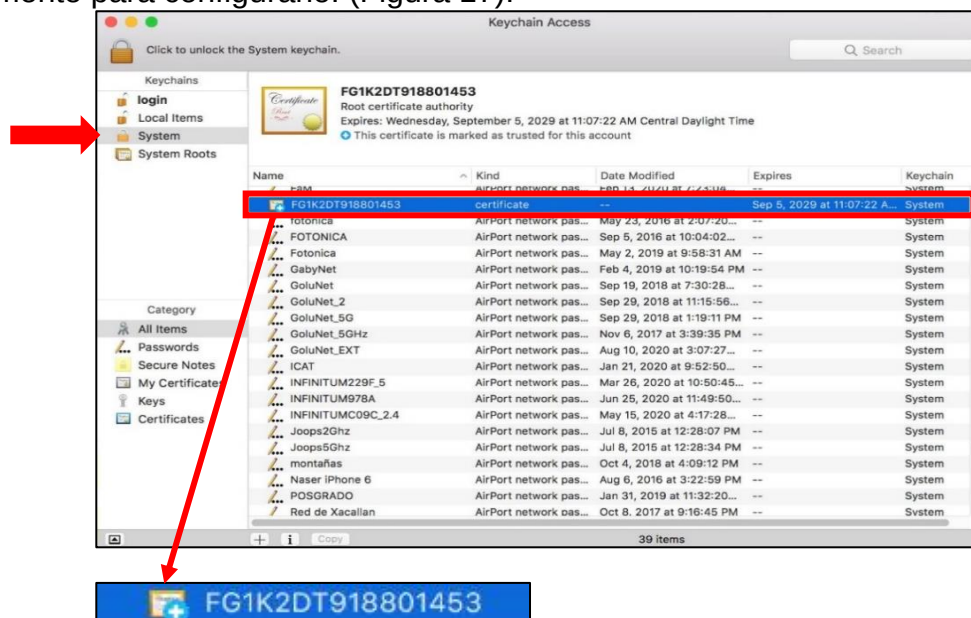


Figura 17. Aplicación Keychain Access o Llaveros. Elaboración propia.

Se le pedirá la **clave o contraseña de usuario** para poder continuar, la ingresaremos para proseguir con la configuración del certificado.

En seguida se mostrará la ventana de información y administración de permisos del certificado de seguridad **FG1K2DT918801453**, en la sección **“Trust”** o **“De confianza”** elegiremos en todas las opciones **“Always Trust”** o **“Siempre confiar”** y daremos clic en **Finalizar** o **Aceptar** para concluir el proceso (Figura 18).

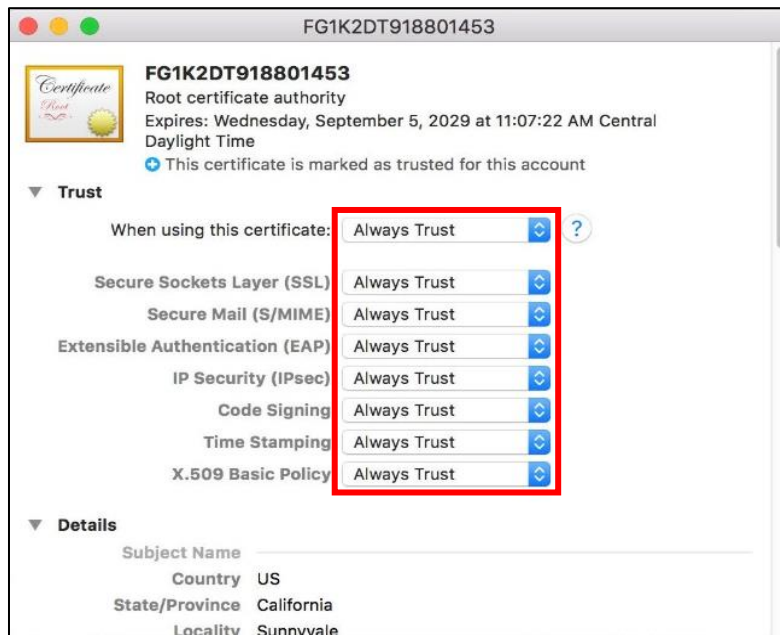


Figura 18. Administración de permisos del certificado de seguridad. Elaboración propia.

Nota final: Es necesario cerrar y volver a abrir el navegador web para aplicar los cambios.

4. Guía de instalación del certificado Fortinet para navegación web segura en dispositivos Windows

Ingresar al sitio <https://www.icat.unam.mx/> y dar clic en la sección **Utilería** para descargar y guardar el certificado de navegación segura **Fortinet_CA_SSL.cer** (Figura 19).

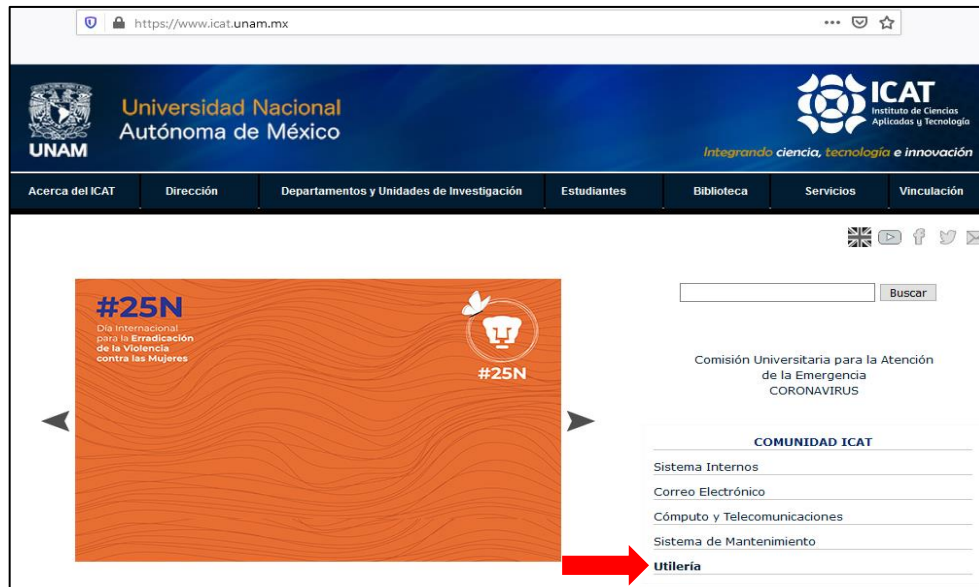


Figura 19. Localización del área de descarga Elaboración propia.

2.- Instalación y configuración

Una vez descargado, al ejecutar el archivo **Fortinet_CA_SSL.cer**, se abrirá una ventana de confirmación, daremos clic en **Aceptar** (Figura 20).

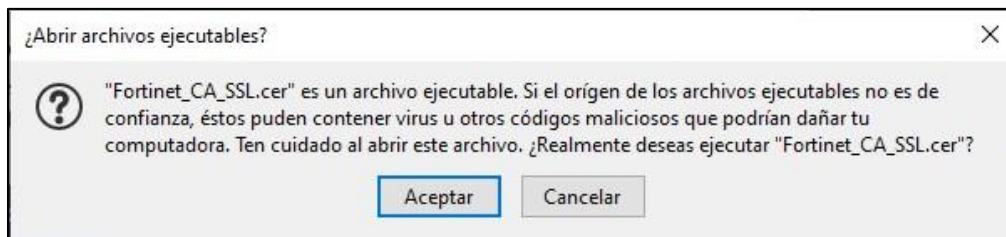


Figura 20. Confirmación de la instalación.

Si se solicita alguna otra confirmación le daremos clic en **Abrir/Aceptar** (Figura 21).

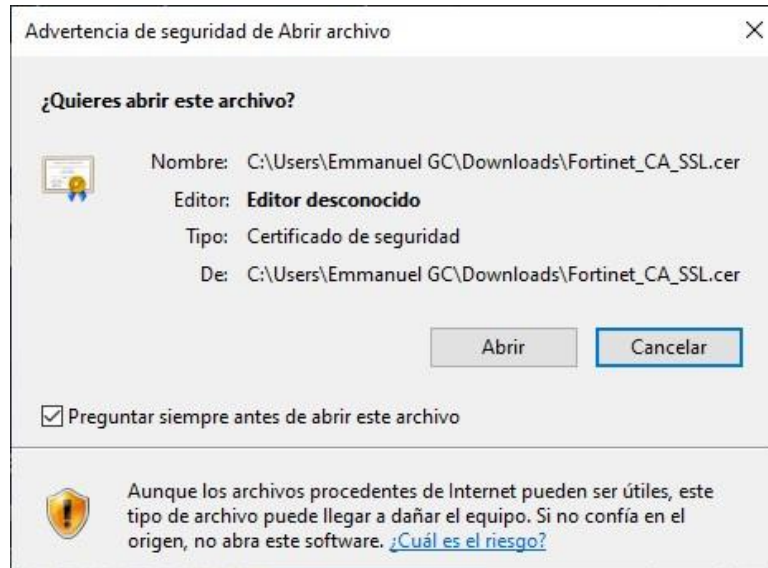


Figura 21. Confirmación de descarga. Elaboración propia.

A continuación, se abrirá una ventana donde podremos observar la información respecto al certificado, daremos clic en **Instalar Certificado** (Figura 22).

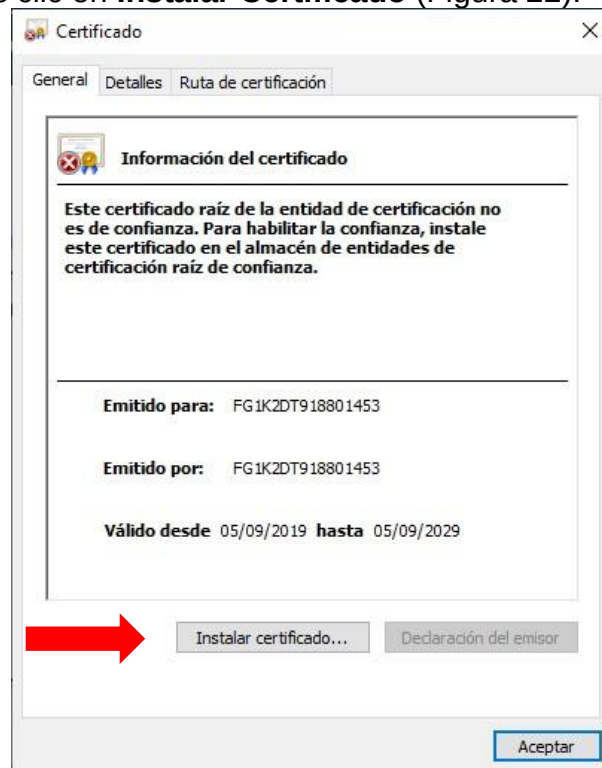


Figura 22. Instalación del certificado. Elaboración propia.

Se abrirá el Asistente para importar certificados, en **Ubicación del Almacén** seleccionaremos **Equipo local** y daremos clic en **Siguiente** (Figura 23).

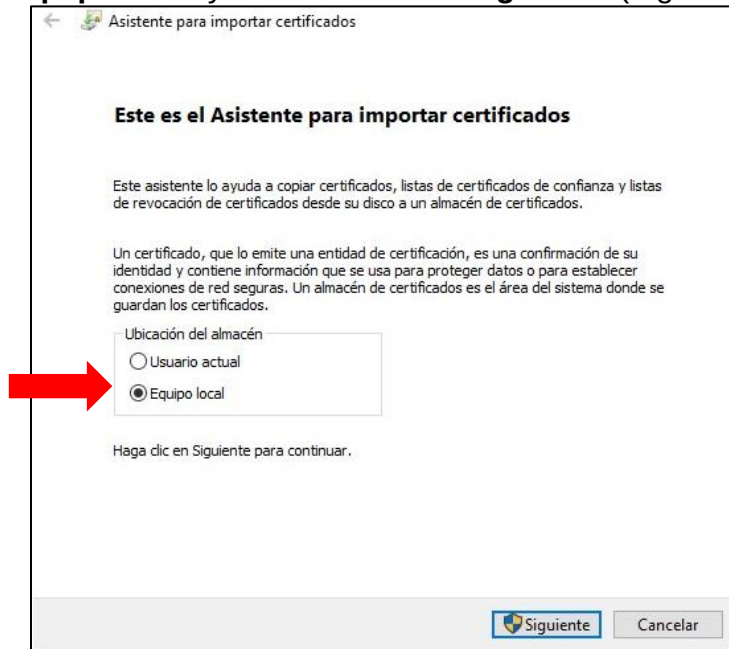


Figura 23. Asistente para importar certificados. Elaboración propia.

En la siguiente ventana seleccionaremos **Colocar todos los certificados en el siguiente almacén** y daremos clic en **Examinar** (Figura 24).

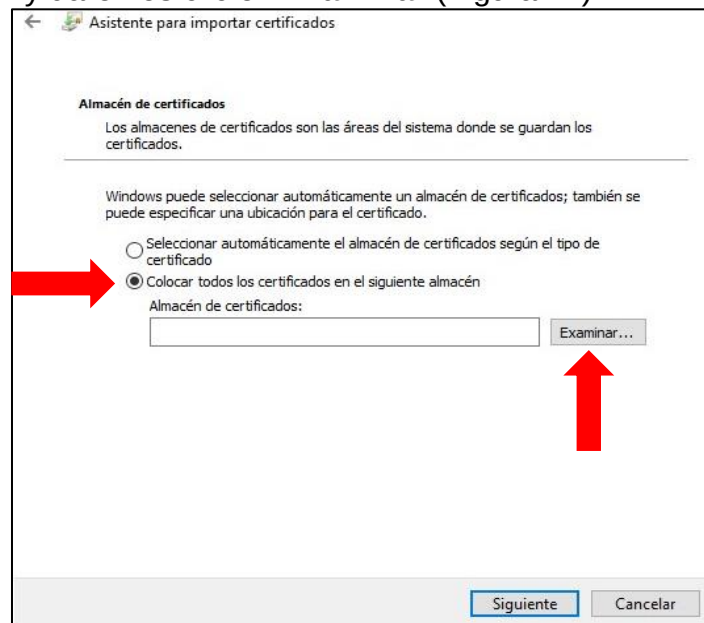


Figura 24. Almacén de certificados. Elaboración propia.

Se abrirá una ventana en la que seleccionaremos la carpeta con el nombre **Entidades de certificación de raíz de confianza** y daremos clic en **Aceptar** (Figura 25).

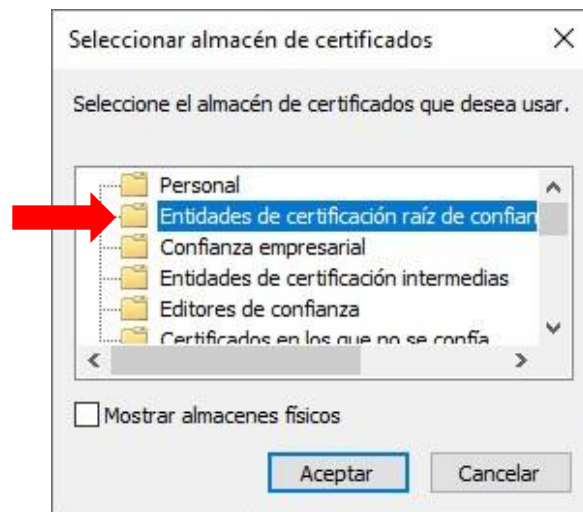


Figura 25. Localización de la carpeta para guardar el certificado. Elaboración propia.

A continuación, se mostrará la ventana anterior del **Asistente para importar certificados** con la ubicación que acabamos de seleccionar, daremos clic en **Siguiente** (Figura 26).

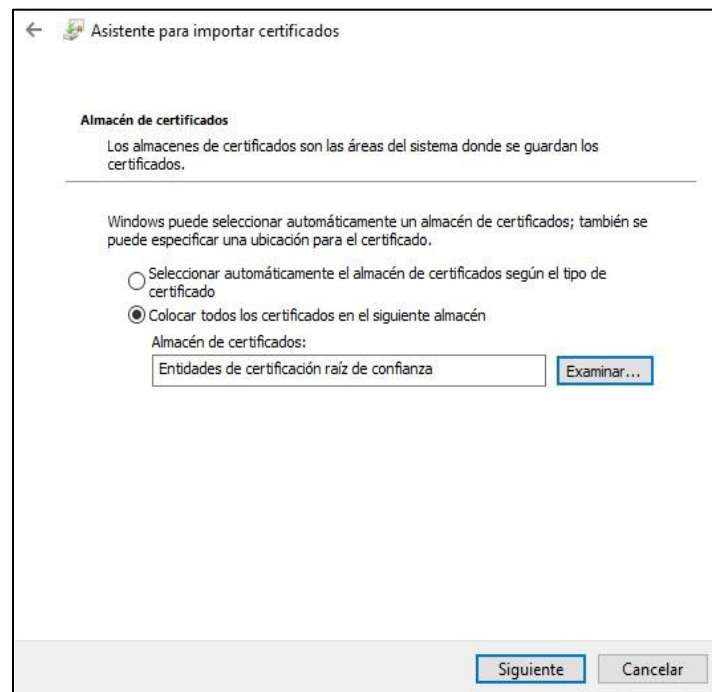


Figura 26. Confirmación de la importación del certificado. Elaboración propia.

Se abrirá una ventana para confirmar la importación del certificado, daremos clic en **Finalizar** (Figura 27).

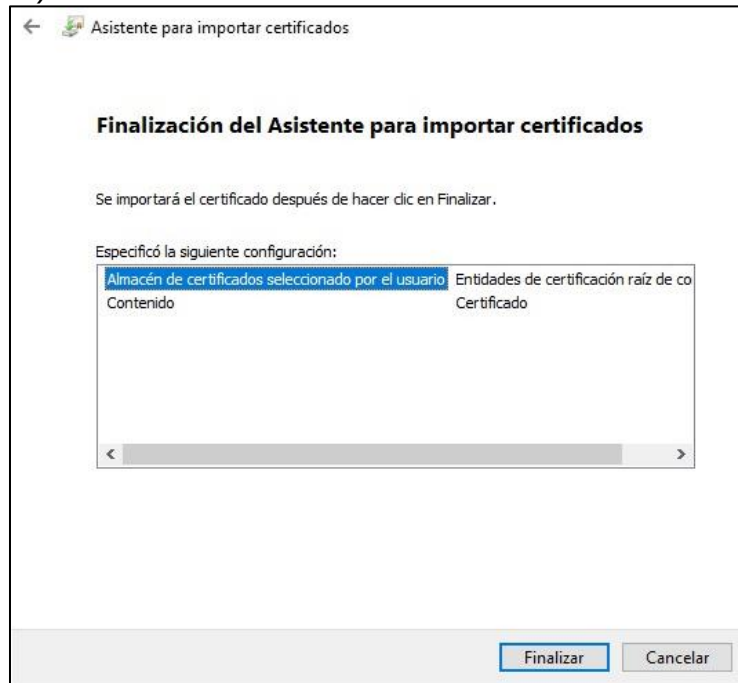


Figura 27. Localización del área de descarga. Elaboración propia.

Si los pasos se efectuaron correctamente, recibiremos una notificación exitosa, daremos clic en **Aceptar** (Figura 28).

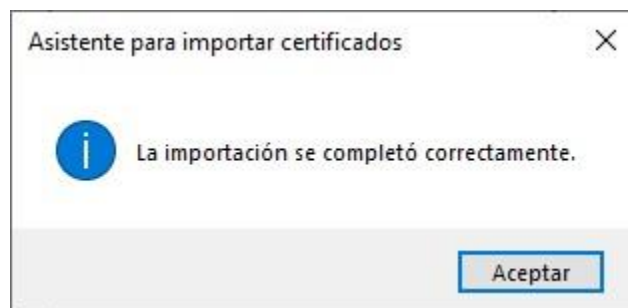


Figura 28. Importación exitosa. Elaboración propia.

Nota. Es necesario cerrar y volver a abrir el navegador web para aplicar los cambios.

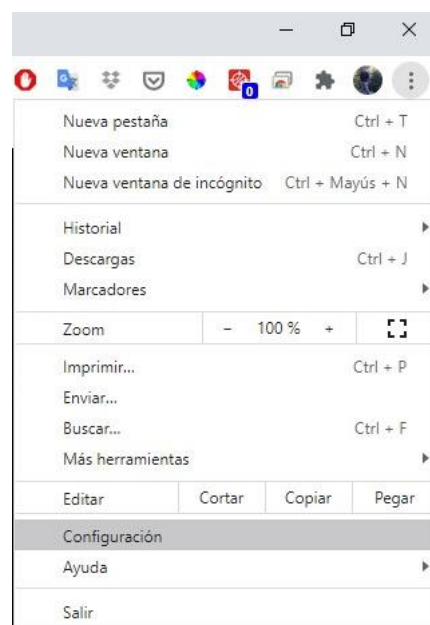
Anexo. Instalación alternativa de forma directa

Si tiene algún problema con la instalación estándar explicada anteriormente, puede utilizar los pasos alternativos explicados a continuación (Figuras 29 – 40):



Firefox

Figura 29. Menú principal, submenú Opciones configuración



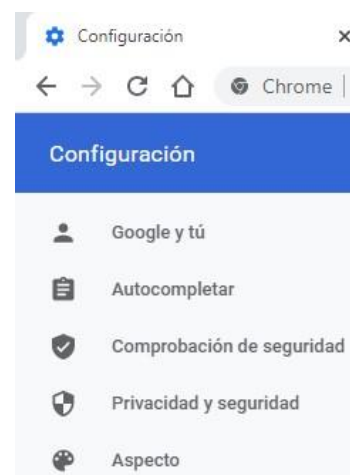
Chrome

Figura 30. Menú principal, submenú



Firefox

Figura 31. Submenú Privacidad y Seguridad



Chrome

Figura 32. Submenú Privacidad y Seguridad

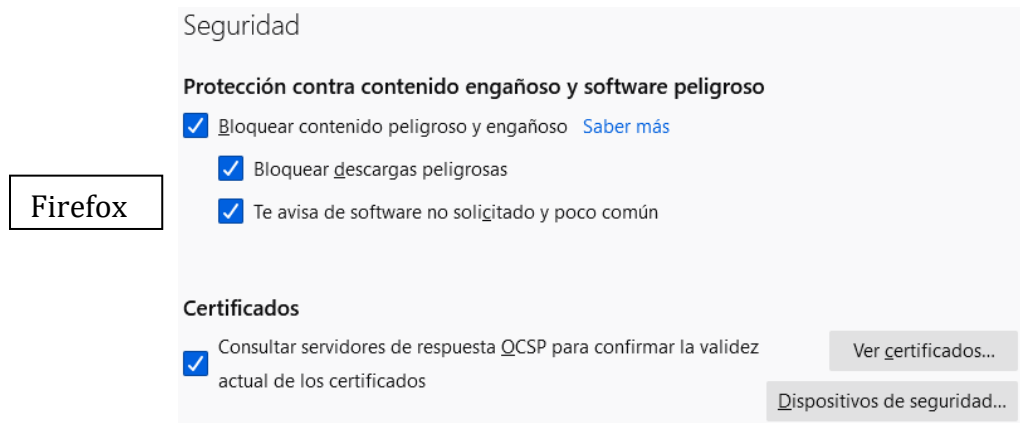


Figura 33. Ubicación del área de administración de Certificados en la sección de Seguridad

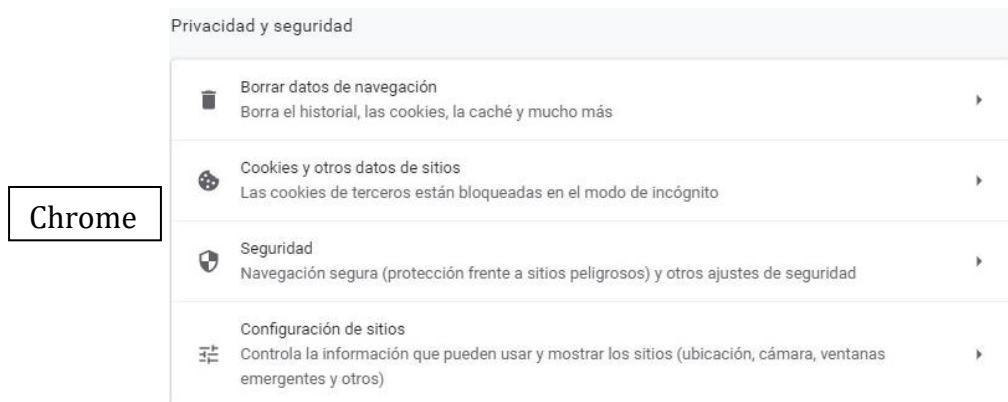


Figura 34. Ubicación del área de administración de Certificados de la sección de Seguridad.
Elaboración propia.

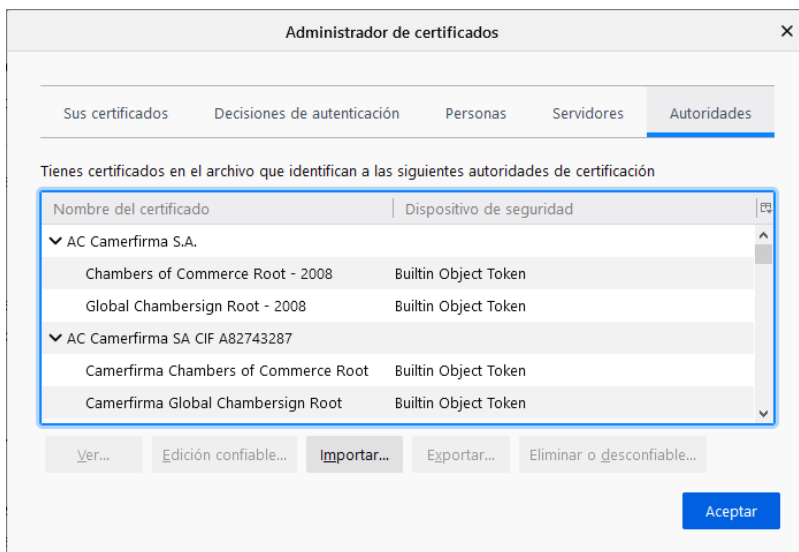


Figura 35. Administrador de Certificados. Elaboración propia.

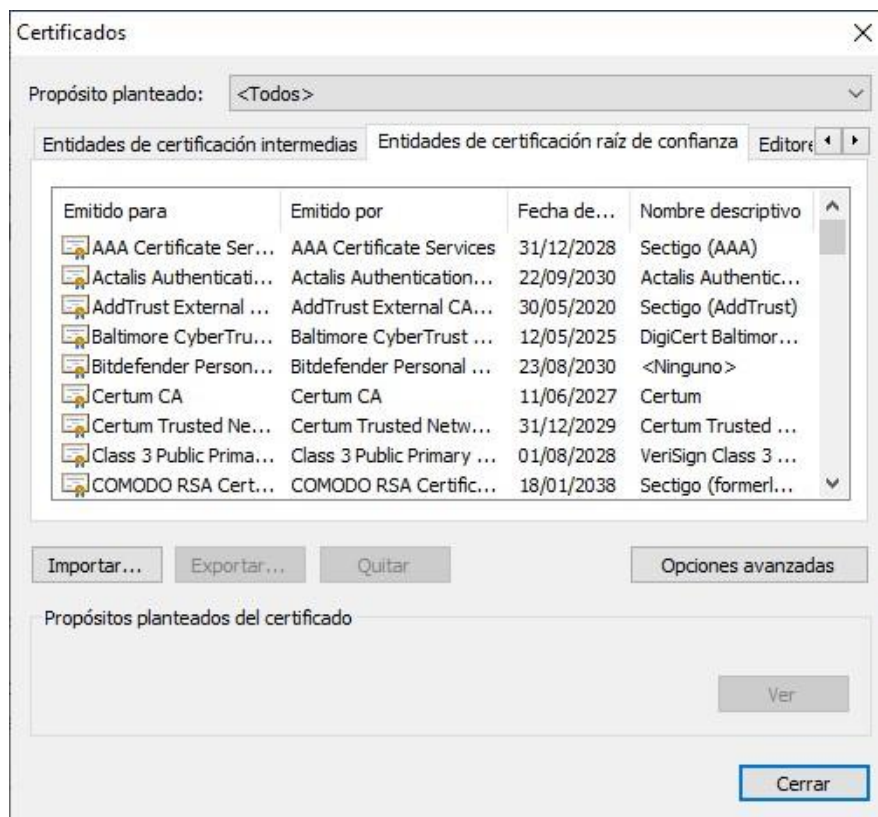


Figura 36. Administrador de Certificados. Elaboración propia.

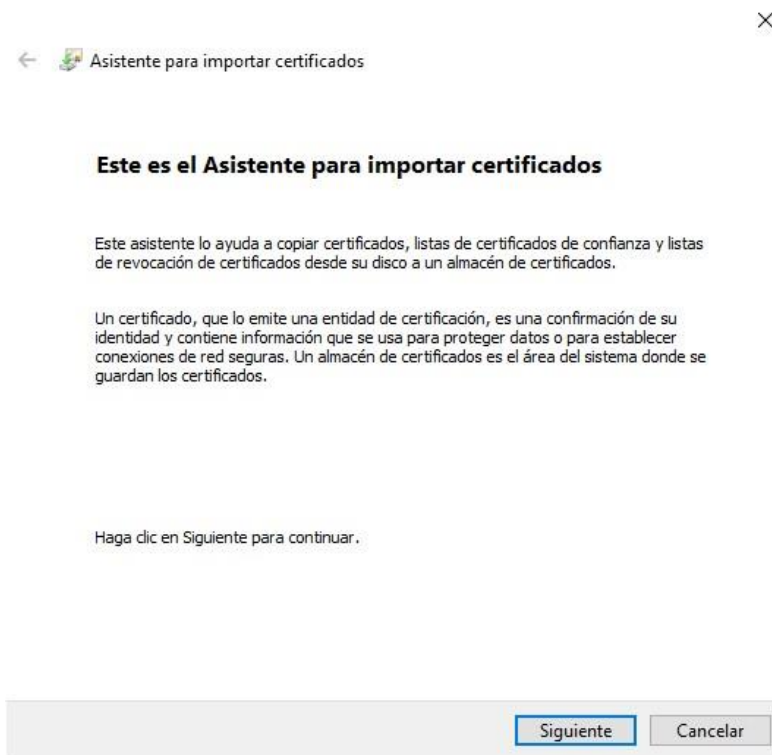


Figura 37. Asistente para la importación de Certificados. Elaboración propia.

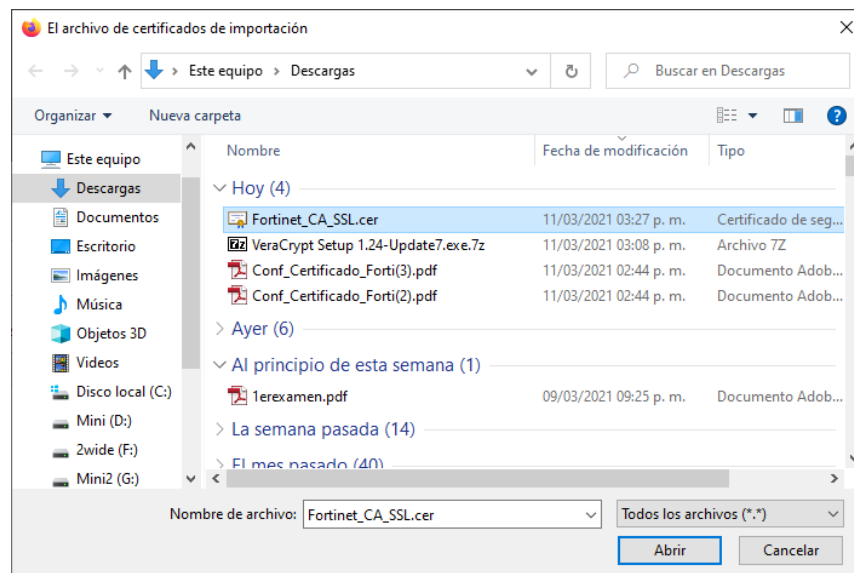


Figura 38. Ubicación del certificado Fortinet_CA_SSL.cer en Descargas. Elaboración propia.

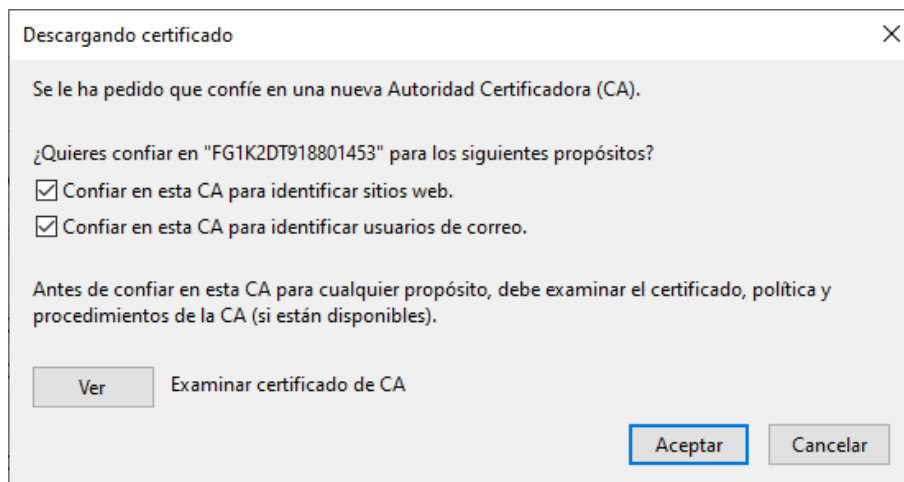


Figura 39. Configuración e instalación del certificado. Elaboración propia.

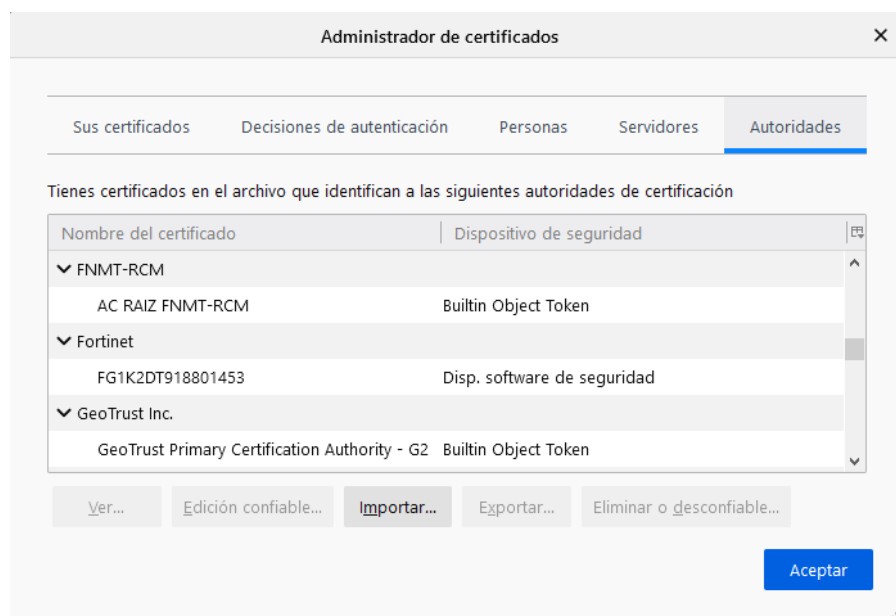


Figura 40. Importación exitosa. Elaboración propia.

NOTA. En general el proceso de importación de certificados es similar, puede variar un poco dependiendo del navegador web en cuestión (Chrome, Firefox, Edge, etc.), si después de realizar la instalación aún tiene problemas para navegar en internet, por favor contacte a la Unidad de Cómputo del ICAT.

Referencias

- ALEPH, 2021. ¿Qué es un *trunk* de red?. [En línea]. Disponible desde <https://aleph.org.mx/que-es-un-trunk-en-red#:~:text=Trunk%20es%20una%20configuraci%C3%B3n%20de,m%C3%A1s%20de%20una%20VLAN.%3B%20as%C3%AD> [Fecha de recuperación 19 de enero de 2022].
- CEPAL-UNESCO, 2020. La educación en tiempos de la pandemia de COVID-19. Publicado en agosto de 2020. [En línea]. Disponible desde https://repositorio.cepal.org/bitstream/handle/11362/45904/1/S2000510_es.pdf [Fecha de recuperación 12 de enero de 2022].
- CISCO, 2006. Inter-Switch Link y Formato de Trama IEEE 802.1Q. [En línea]. Disponible desde https://www.cisco.com/c/es_mx/support/docs/lan-switching/8021q/17056-741-4.html [Fecha de recuperación 13 de enero de 2022].
- CISCO, 2022. ¿What is WIFI?. [En línea]. Disponible desde https://www.cisco.com/c/es_mx/products/wireless/what-is-wifi.html [Fecha de recuperación 19 de enero de 2022].
- DESCOM, 2002. Protocolo OCSP y certificados. [En línea]. Disponible desde <https://www.descom.es/blog/alojamiento-web/certificados-ssl/protocolo-ocsp.html> [Fecha de recuperación 15 de enero de 2022]
- FORTINET, 2018. Fortinet es el proveedor mundial líder en dispositivos de seguridad de red y líder en Gestión Unificada de Amenazas (UTM). [En línea]. Disponible desde <http://fortinet.globalgate.com.ar/ver.php/mod/contenido/> [Fecha de recuperación 13 de enero de 2022].
- FORTINET DOCUMENT LIBRARY, Certificate-based authentication, [En línea]. Disponible desde <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/943479/certificate-based-authentication> [Fecha de recuperación 13 de enero de 2022].
- GOOGLE, 2021. Proteger sitios con el protocolo HTTPS. [En línea]. Disponible desde <https://developers.google.com/search/docs/advanced/security/https?hl=es> [Fecha de recuperación 14 de enero de 2022].

KASPERSKY, 2022. ¿Qué es el cifrado de datos? Definición y explicación. [En línea]. Disponible desde <<https://latam.kaspersky.com/resource-center/definitions/encryption>> [Fecha de recuperación 17 de enero de 2022].

KASPERSKY, 2022. Qué es un certificado SSL: definición y explicación. [En línea]. Disponible desde <<https://latam.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate>> [Fecha de recuperación 17 de enero de 2022].

Malenkovich S., 2013. ¿Qué es un ataque *man-in-the-middle*?. [En línea]. Disponible desde <<https://latam.kaspersky.com/blog/que-es-un-ataque-man-in-the-middle/469/>> [Fecha de recuperación 10 de abril de 2013].

Malwarebytes, 2022. Suplantación de identidad (*phishing*). [En línea]. Disponibles desde <[https://es.malwarebytes.com/phishing/#:~:text=Suplantaci%C3%B3n%20de%20identidad%20\(phishing\),correo%20electr%C3%B3nico%20o%20llamada%20telef%C3%B3nica](https://es.malwarebytes.com/phishing/#:~:text=Suplantaci%C3%B3n%20de%20identidad%20(phishing),correo%20electr%C3%B3nico%20o%20llamada%20telef%C3%B3nica)> [Fecha de recuperación 25 de enero de 2022].

Rouse M., 2017. BYOD traiga su propio dispositivo. [En línea]. Disponible desde <<https://www.computerweekly.com/es/definicion/BYOD-traiga-su-propio-dispositivo>> [Fecha de recuperación 13 de enero de 2022].

SSL, 2021. ¿Qué es una autoridad de certificación (CA)?. [En línea]. Disponible desde <<https://www.ssl.com/es/preguntas-frecuentes/%C2%BFQu%C3%A9-es-una-autoridad-de-certificaci%C3%B3n%3F/>> [Fecha de recuperación 13 de enero de 2022].

SSL, 2021. Navegadores y validación de certificados. [En línea]. Disponibles desde <<https://www.ssl.com/es/art%C3%ADculo/navegadores-y-validaci%C3%B3n-de-certificados>>. [Fecha de recuperación 13 de enero de 2022].