

Manual de acceso a Conselleria de Sanitat Universal i Salut Pública mediante cliente VPN

Referencia MAN-COMM.040

Versión: 1.36

Estatus: Publicado

Fecha: 02/05/2023

AUDITORÍA DEL DOCUMENTO

Responsabilidades

Propietario	Organización	Fecha
Servicio de Infraestructuras de Tecnologías de la Información y la Comunicación / Telecomunicaciones	CSUiSP	02/05/2023

Versión

Versión	Fecha	Editores	Descripción de la Versión/Cambios Realizados
1.0	16/12/2004	Isabel Sánchez	Versión inicial
1.1	16/12/2004	Isabel Sánchez	Inclusión del Formulario de Acceso como Anexo (FOR-COMN.20)
1.2	01/10/2006	Domingo Laguna	Se incluye como nota la necesidad de instalar los certificados raíz de GVA
1.3	25/08/2009	Oscar Rodríguez	Se incluye un apartado con FAQ's
1.4	26/04/2010	Domingo Laguna	Se elimina la posibilidad de Cert. Camerfirma y Linux/Windows 7 64 bits
1.5	20/10/2010	Domingo Laguna	Se incluyen cláusulas que debe cumplir el solicitante.
1.6	11/11/2010	Domingo Laguna	Inclusión cláusulas de Confidencialidad. Modificación de la URL para descarga el cliente de VPN. Posibilidad de envío de la solicitud por vía electrónica. Inclusión de email de contacto para la renovación/cancelación del acceso.
1.7	14/07/2011	Pau Roda	Inclusión de Errores Conocidos
1.8	15/01/2012	Óscar Rodríguez	DNI electrónico. Publicación VPN SSL. Gestión de caducidades. Certificados de entidad.
1.9	13/06/2013	Marc Salom	Inclusión de Errores Conocidos
1.10	19/02/2014	Marc Salom	Inclusión de Errores Conocidos
1.11	22/04/2014	Pau Roda	Conexión con sist. operativo Mac OS X
1.12	27/09/2017	Alberto Babiera	Introducción DNle. Actualización software.

1.2	13/09/2018	David Reyes	Actualización del tratamiento de la solicitud. Eliminada referencia a FOR-COMN.20
1.21	18/02/2020	Alberto Merino	Actualización URL descarga del cliente VPN.
1.22	16/06/2020	Ciro Alejandro Galvis	Actualización URL certificados.
1.23	26/01/2021	María del Mar Bonet	Actualización campos obligatorios.
1.3	27/01/2021	María del Mar Bonet	Actualización campos obligatorios. Se elimina el Anexo 2. Se actualizan las imágenes del apartado de <i>Generación del ticket en la aplicación SIGESTI.</i>
1.31	16/02/2021	María del Mar Bonet	Se actualiza enlace a Cisco AnyConnect Se añade referencia a documento relacionado
1.32	22/11/2022	Elena Ejarque González	Se actualiza nuevo certificado admitido FNMT Se actualiza nuevo menú selección certificado cliente
1.33	03/02/2023	Elena Ejarque González	Se actualizan los enlaces a descargas de ACCV Se actualizan tarjetas criptográficas Se actualiza legislación referente a protección de datos
1.34	30/03/2023	Elena Ejarque González	Se actualizan los enlaces a descargas del manual y el cliente de VPN
1.35	20/04/2023	María del Mar Bonet Ramos	Se actualiza la instalación de los certificados de la ACCV en macOS
1.36	02/05/2023	Elena Ejarque González	Se elimina punto 5.4 Configuración para Residencias

Ámbito

	Grupo o Individuos	Comentarios
Origen	CGRA	
Aplicación	CSUISP	
Visibilidad	CSUISP	

Estatus

Estatus	Fecha	Por	Descripción de Cambios Realizados
Borrador	01/01/2012	Óscar Rodríguez	
Propuesta	16/01/2012	Óscar Rodríguez	Publicación VPN SSL (apartado 5.2). Gestión de caducidades (apartado 4). DNI electrónico (apartado 3).
Revisión	21/11/2012	Mercedes Dobón	
Aceptado	05/12/2012	Mercedes Dobón	
Publicado	07/12/2012	GTCOM	
Revisión	13/10/2017	CGRA Seguridad	Introducción DNle. Actualización de software.
Aceptado	13/10/2017	CGRA Seguridad	
Publicado	13/10/2017	CGRA Seguridad	
Revisión	26/09/2018	David Reyes	Actualización del tratamiento de la solicitud. Eliminada referencia a FOR-COMN.020
Aceptado	18/02/2020	Alberto Merino	Actualización URL descarga del cliente VPN.
Publicado	18/02/2020	CGRA	
Revisión	16/06/2020	Ciro Galvis	
Aceptado	16/06/2020	CGRA	
Publicado	15/07/2020	CGRA	
Revisión	26/01/2021	María del Mar Bonet	Actualización campos obligatorios.
Aceptado	26/01/2021	CGRA	
Publicado	26/01/2021	CGRA	
Revisión	27/01/2021	María del Mar Bonet	Campos obligatorios y generación de ticket
Aceptado	27/01/2021	CGRA	
Publicado	27/01/2021	CGRA	
Revisión	16/02/2021	María del Mar Bonet	Actualizar enlace a Cisco AnyConnect, añadir referencia a documento relacionado
Revisión	22/11/2022	CGRA Seguridad	Introducción de nuevo certificado FNMT Se actualiza nuevo menú selección certificado cliente
Aceptado	22/11/2022	CGRA	
Publicado	22/11/2022	CGRA	

Estatus	Fecha	Por	Descripción de Cambios Realizados
Revisión	03/02/2023	CGRA Seguridad	Se actualizan los enlaces a descargas de ACCV Se actualizan tarjetas criptográficas Se actualiza legislación referente a protección de datos
Aceptado	03/02/2023	CGRA	
Publicado	03/02/2023	CGRA	
Revisión	30/03/2023	CGRA	Se actualizan los enlaces a descargas del manual y el cliente de VPN
Aceptado	30/03/2023	CGRA	
Publicado	30/03/2023	CGRA	
Revisión	20/04/2023	CGRA	Se actualiza la instalación de los certificados de la ACCV en macOS
Aceptado	20/04/2023	CGRA	
Publicado	20/04/2023	CGRA	
Revisión	02/05/2023	CGRA	Se elimina punto 5.4 Configuración para Residencias
Aceptado	02/05/2023	CGRA	
Publicado	02/05/2023	CGRA	

Documentos relacionados

Referencia	Título	Naturaleza de la relación
NOR-COMN.009	Requerimientos para la conexión VPN-site-to-site entre la Conselleria de Sanitat i Salut Pública y un organismo externo	
FOR-COMN.029	Formulario para dar de alta usuarios VPN	

Índice de contenido

1	PROPÓSITO Y DESCRIPCIÓN.....	6
2	ÁMBITO Y APLICACIÓN	7
3	REQUISITOS PREVIOS	8
3.1	Obtener un certificado digital personal.	8
3.2	Instalar el software Cisco Anyconnect.	9
3.2.1	Instalación de los certificados raíz.....	9
3.2.2	Instalación de los certificados personales	11
3.3	Apertura de puertos en la red Local de la empresa.	14
4	TRATAMIENTO DE LA SOLICITUD	15
5	CONFIGURACIÓN DEL ACCESO	18
5.1	Modo VPN SSL.....	18
5.2	Instalación de los certificados de la ACCV sobre macOS	21
5.3	Configuración VPN macOS	24
6	SOPORTE PARA LA CONEXIÓN A EMPRESAS EXTERNAS.....	28
6.1	Alcance del Soporte.....	28
6.2	Pasos que seguir cuando haya problemas.....	28
6.3	Fallos más frecuentes.....	29
6.3.1	El Cisco AnyConnect no encuentra mi certificado de usuario.....	29
6.3.2	Certificados raíz no importados.....	30
6.3.3	Error 412.....	30
6.3.4	Error 427.....	31
6.3.5	Error de negociación de certificado	31
6.3.6	Error de conexión.....	32
6.3.7	Error de conexión con Cisco AnyConnect:	33
6.3.8	Error de conexión con nuevas tarjetas de la ACCV (clave de 2048 bits)	34
6.3.9	Error de conexión con aplicaciones tras establecer la VPN.....	34
	ANEXO I: CLÁUSULAS ASOCIADAS AL USO DEL SERVICIO VPN	35

1 Propósito y Descripción

El propósito de este documento es definir un manual a seguir por parte de las empresas/usuarios que necesiten acceder a equipos de la Conselleria desde fuera de la Red Arterias mediante un cliente VPN.

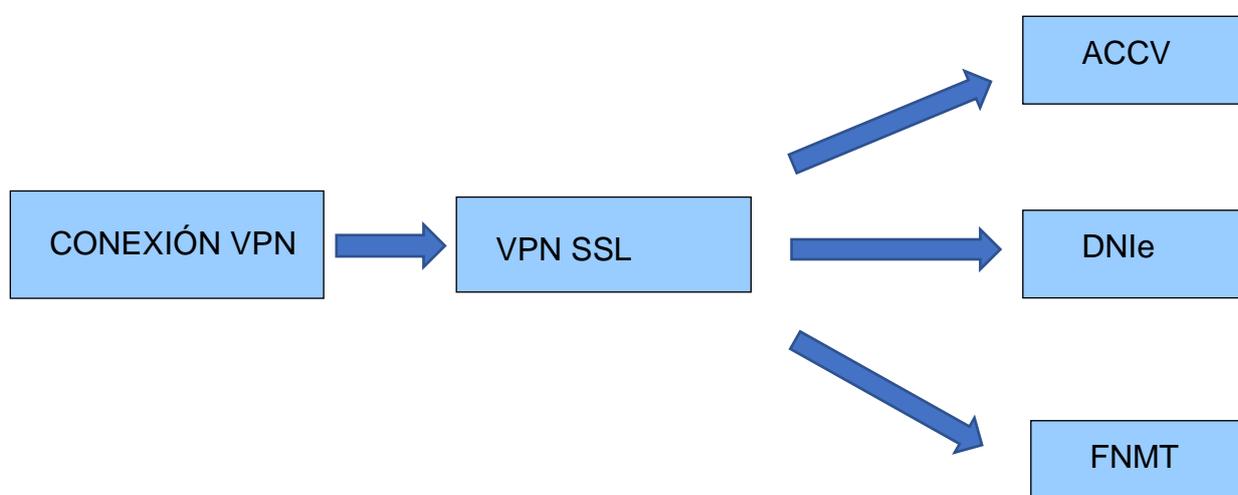
2 Ámbito y Aplicación

El ámbito de este documento corresponde al CGRA y al personal solicitante de una conexión VPN con la Conselleria de Sanitat Universal i Salut Pública.

3 Requisitos previos

La conexión VPN a la Conselleria de Sanitat Universal i Salut Pública (CSUiSP) se realiza mediante:

- **VPN SSL.** En este caso puede utilizarse un certificado de la ACCV, FNMT o el certificado digital incluido en el DNI electrónico español.



3.1 Obtener un certificado digital personal.

El primer requisito es obtener un certificado digital personal. Dicho certificado puede ser emitido por la Autoridad de Certificación de la Generalitat Valenciana (ACCV), por la Fábrica Nacional de Moneda y Timbre (FNMT) o también puede ser utilizado el certificado digital incluido en el DNI electrónico con un lector de tarjeta apropiado.

3.2 Instalar el software Cisco Anyconnect.

- Instalar el software cliente de Cisco. Este puede ser obtenido en la siguiente dirección:

<https://www.san.gva.es/web/conselleria-de-sanidad-universal-y-salud-publica/client-vpn>

3.2.1 Instalación de los certificados raíz.

En la web <https://www.accv.es/servicios/ciudadanos-y-autonomos/descarga-de-certificados-jerarquia/>

pueden descargarse los certificados raíz de la ACCV necesarios para la conexión VPN:



Estos son los certificados vigentes de
nuestra jerarquía



De ellos dependen los certificados finales que emitimos. Sólo necesitarás descargarlos si tu aplicación, servidor o sistema no confía en ellos por defecto. Lo cual es lo habitual para los principales entornos de Escritorio.

ACCVRAIZ1 | CA RAÍZ (VIGENTE HASTA 31/12/2030)

Emisor: ACCVRAIZ1
Hash: 9A:6E:CO:12:E1:A7:DA:9D:BE:34:19:4D:47:8A:D7:C0:DB:18:22:FB:07:1D:F1:29:81:49:6E:D1:04:38:41:13
Clave: RSA 4096 bits - SHA256
CRL: [Lista de certificados revocados.](#)

ACCVCA-120 | CA SUBORDINADA PARA PERSONAS FÍSICAS (VIGENTE HASTA 31/12/2026)

Emisor: ACCVRAIZ1
Hash: 2D:E6:20:F2:D1:20:0A:A9:0B:16:C3:CC:F6:70:FD:7E:D1:43:79:AB:06:FA:8B:03:1C:FE:F8:DA:05:1E:A5:A2
Clave: RSA 4096 bits - SHA256
CRL: [Lista de certificados revocados.](#)

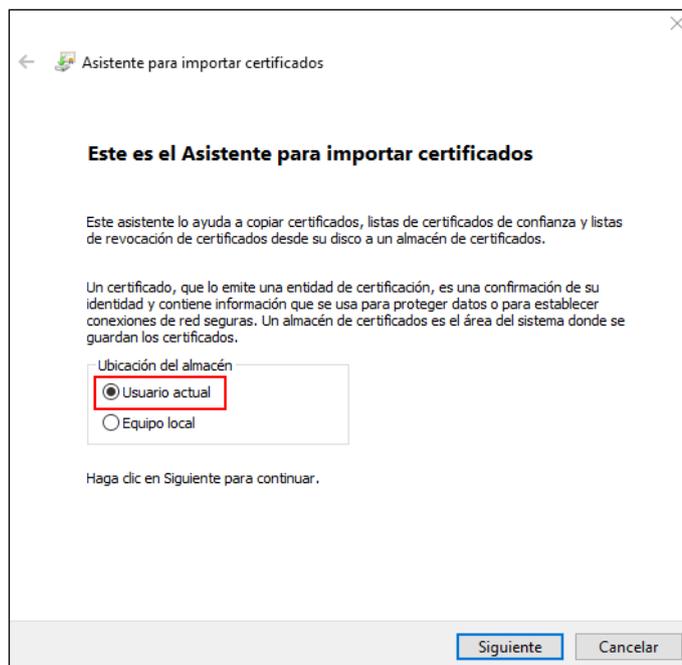
ACCVCA-110 | CA SUBORDINADA PARA ENTIDADES (VIGENTE HASTA 31/12/2026)

Emisor: ACCVRAIZ1
Hash: E9:32:7A:34:7C:BE:1C:B9:4C:DC:9A:A5:4C:B3:1B:6E:43:D6:89:68:D1:7D:09:CE:32:6A:09:1B:FC:2F:0B:11
Clave: RSA 4096 bits - SHA256
CRL: [Lista de certificados revocados.](#)

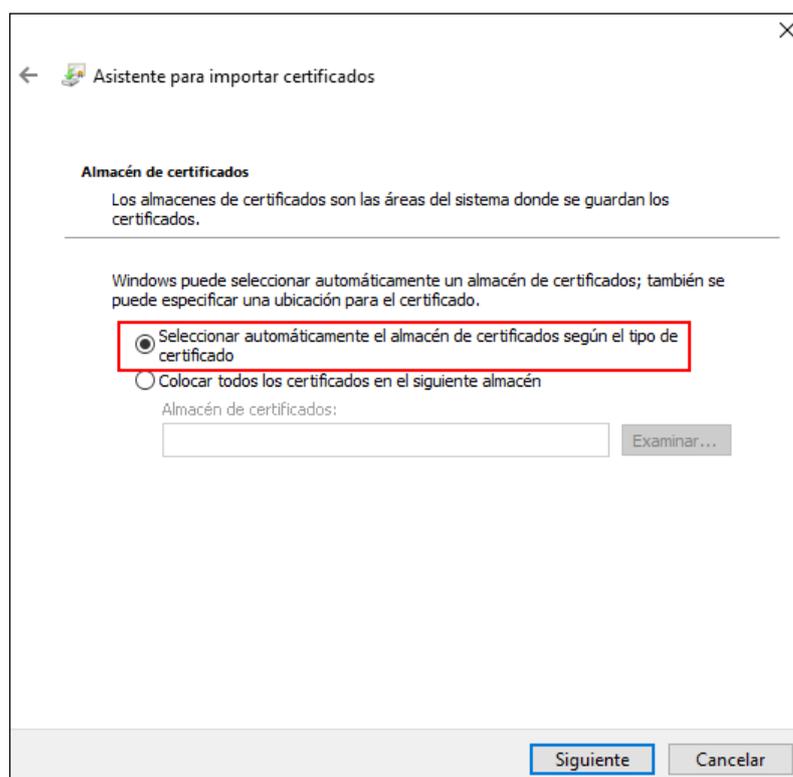
Para instalar cada uno de los certificados anteriores seguimos el mismo procedimiento. Lo ejecutamos y seleccionamos “Instalar certificado...”



Seleccionamos Usuario actual en la ubicación del almacén.



Por último, marcamos que se seleccione automáticamente el almacén de certificados y finalizamos la instalación.



Debemos repetir este proceso para todos los certificados listados en el inicio de este apartado.

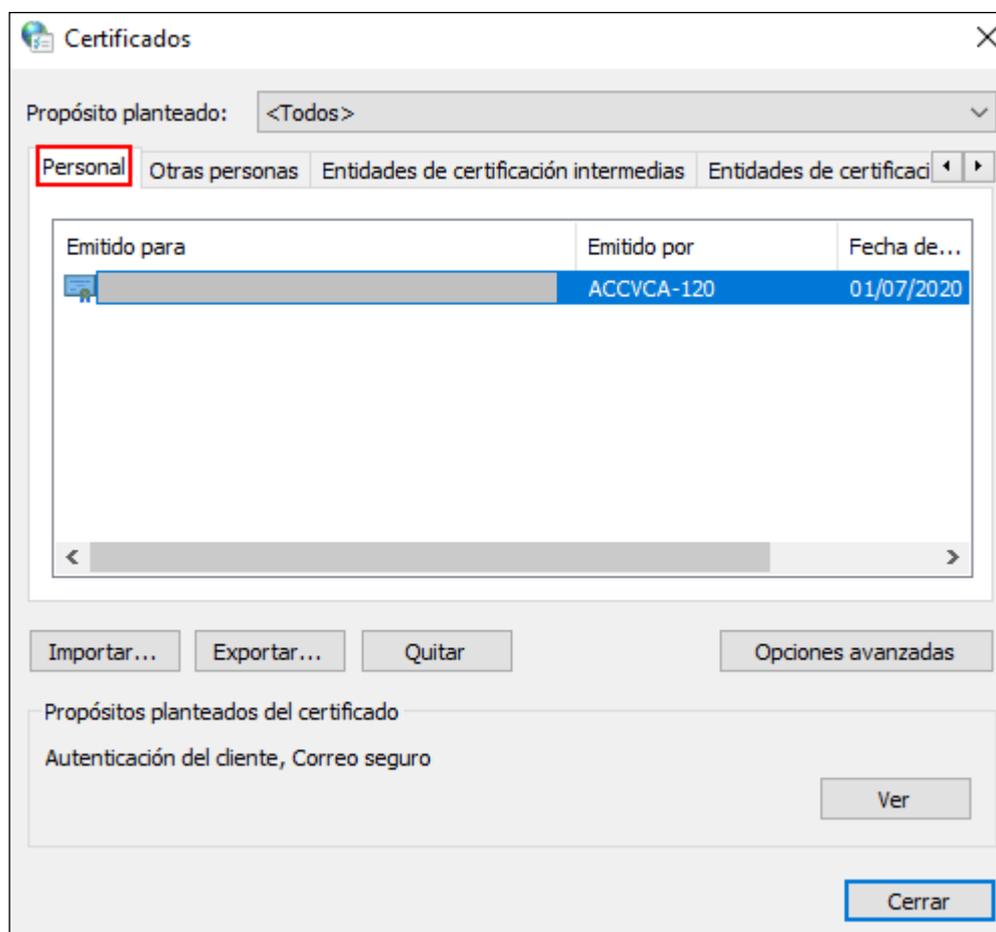
3.2.2 Instalación de los certificados personales

Los certificados personales a utilizar pueden ser los de la ACCV, FNMT o el DNle.

Certificado Personal de la ACCV y FNMT

Al igual que los certificados raíz, también debemos instalar el certificado personal. Hacemos doble click sobre nuestro certificado personal, lo instalamos con nuestra contraseña y aparecerá en la pestaña de Personal del almacén de certificados.

Podemos comprobarlo una vez instalado desde Panel de Control → Opciones de Internet → Contenido → Certificados.



Si se utiliza la tarjeta criptográfica, es necesario conectar el certificado digital de la tarjeta criptográfica a través del lector de tarjetas al equipo desde el que se realizará la conexión VPN.

Para ello se necesitará el software CardOS API, G&D o Bit4id (consultar compatibilidades con las versiones de Windows).

Puede consultar las siguientes páginas de la ACCV si necesita más información:

<https://www.accv.es/descargables/>

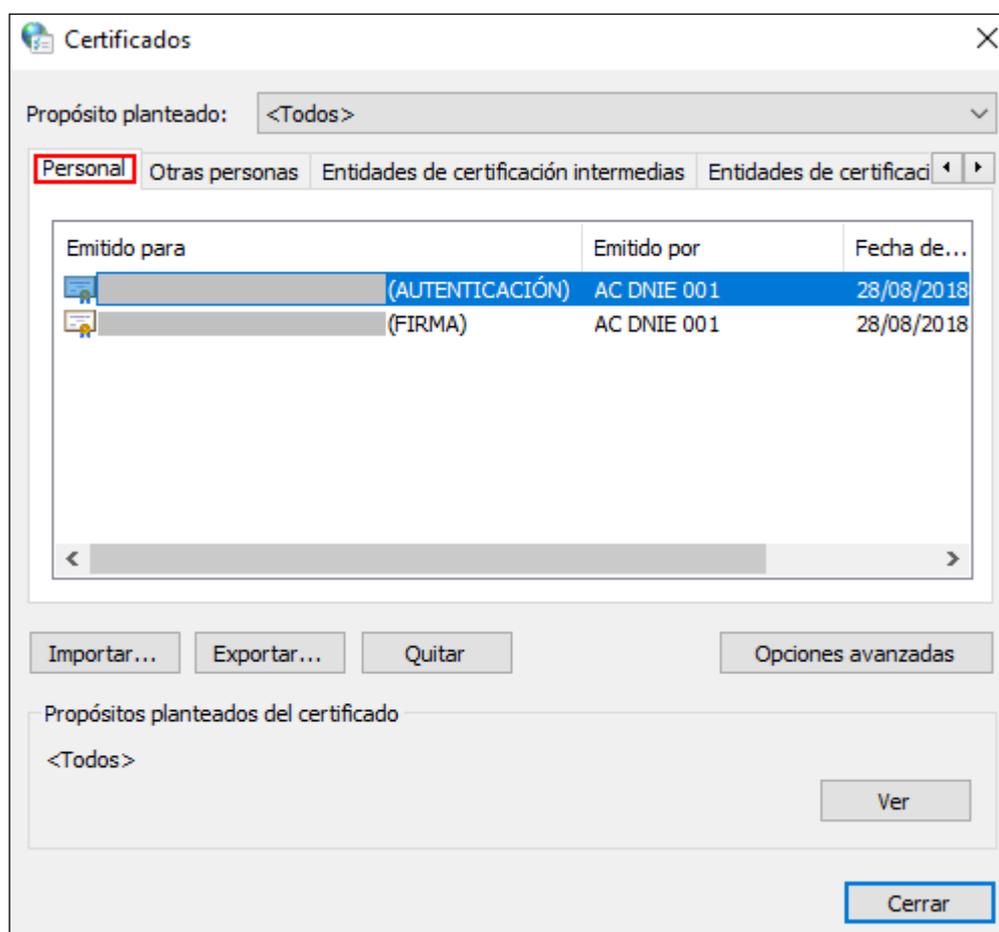
<https://www.accv.es/manuales-y-guias>

De los dos certificados que aparecerán se debe elegir el certificado de FIRMA (a priori desde la herramienta no es posible distinguirlos).

Certificados DNIE

Para usar los certificados personales del DNIE primero debemos comprobar que nuestro lector de tarjetas es compatible con el DNIE e instalar sus controladores.

Una vez hecho esto podemos introducir nuestro DNIE con los certificados activados (apartado 3.1.2) y se cargarán automáticamente en la pestaña Personal del almacén de certificados. Para comprobarlo de nuevo podemos ir a Panel de Control→Opciones de Internet→Contenido→Certificados.



3.3 Apertura de puertos en la red Local de la empresa.

La red local de la empresa debe tener abiertos de salida los siguientes puertos y protocolos.

- UDP 500 (ISAKMP/IKE)
- UDP 4500 (NAT-T) o en su defecto los Protocolos ESP (IP 50) y AH (IP 51).

4 Tratamiento de la solicitud

Para habilitar el acceso VPN es necesario que el responsable del proyecto, contrato, convenio, etc, genere una solicitud en el Sistema de gestión de Servicios TI (SIGESTI) de la Conselleria de Sanitat Universal i Salut Pública.

Al realizar la solicitud de acceso, el usuario final se compromete al cumplimiento de las cláusulas de confidencialidad y uso de la conexión que vienen descritas en este documento.

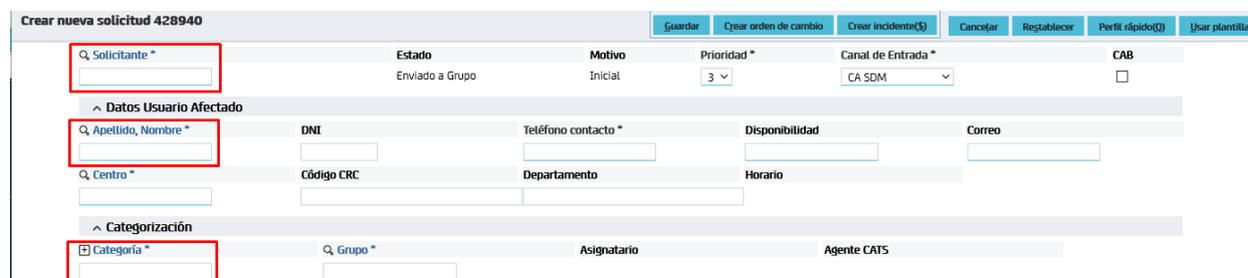
Una vez recibida y validada la solicitud, se procederá a la creación del usuario VPN con su correspondiente contraseña, que le será notificada a la persona que realizó la solicitud inicialmente.

Consideraciones para tener en cuenta:

- La solicitud debe especificar el nombre y apellidos de la persona que solicita el acceso y la empresa u organismo al que pertenece.
- La solicitud debe especificar el DNI del usuario final, ya que éste será el identificador de acceso único a la VPN, así como un correo electrónico válido y un teléfono de contacto.
- La solicitud debe especificar el Proyecto o Servicio para el cual se requiere el acceso VPN.
- Por defecto se asigna un año como fecha de caducidad para la VPN del usuario final asociada a un proyecto global.
- La solicitud debe especificar la aplicación o funcionalidad de los accesos requeridos.

Generación del ticket en la aplicación SIGESTI:

- Todos los campos señalados a continuación son requeridos para la tramitación de la solicitud.



Crear nueva solicitud 428940

Guardar Crear orden de cambio Crear incidente(3) Cancelar Restablecer Perfil rápido(0) Usar plantilla

Q Solicitante *	Estado	Motivo	Prioridad *	Canal de Entrada *	CAB
<input type="text"/>	Enviado a Grupo	Inicial	3	CA SDM	<input type="checkbox"/>

^ Datos Usuario Afectado

Q Apellido, Nombre *	DNI	Teléfono contacto *	Disponibilidad	Correo
<input type="text"/>				
Q Centro *	Código CRC	Departamento	Horario	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	

^ Categorización

<input checked="" type="checkbox"/> Categoría *	Q Grupo *	Asignatario	Agente CATS
<input type="text"/>	<input type="text"/>		

- Se debe generar el ticket de solicitud bajo la siguiente categoría:

Solicitud→Redes y Telecomunicaciones→Accesos externos→VPN-L2L

Selección de área de solicitud

Área de solicitud

▼ Solicitud

> Aplicacion

Aplicación.Alegaciones Categoría para que las empresas realicen alegaciones relacionadas con tickets que impactan en la facturación

> **Business Intelligence** Solicitudes relacionadas con sistemas de BI

> **Calidad** Petición relacionada con aspectos relativos a la calidad de los proyectos/servicios.

> **CMDB e Inventario**

> **Documentacion**

> **Integraciones** Peticiones relacionadas con las integraciones entre aplicaciones.

Llamada erronea Llamadas recibidas por equivocación.

> **Mantenimiento del centro de informatica** Peticiones relacionadas con el mantenimiento del centro de informática

> **Monitorizacion**

> **Notificacion**

> **Puesto de trabajo** Peticiones relacionadas con el puesto de trabajo

▼ Redes y Telecomunicaciones

▼ Accesos externos

Línea dedicada Peticiones relacionadas con la línea dedicada

VPN-L2L Peticiones relacionadas con la VPN o L2L

Análisis o monitorización de tráfico red Solicitud de análisis o monitorización del tráfico de la red

Auditoría de seguridad en red Solicitud de auditoría de seguridad en red

Conectividad entre/a sistemas de información Peticiones de conectividad entre/a sistemas de información

> Datos

Direccionamiento IP Petición de direccionamiento de IP

GPRS/Tablets Peticiones relacionadas con el servicio de movilidad (GPRS, tablets, SIM)

Informes Trafico / Extensiones de voz Solicitud de informes de tráfico o de extensiones de voz (proveedor de servicios WAN/Voz)

Servicios de red (DNS, Proxys) Solicitudes relacionadas con servicios de red (DNS, proxys).

Videoconferencia Peticiones relacionadas con el servicio de videoconferencia

> Voz

> Seguridad

Servicio no soportado Solicitudes relacionadas con servicios no soportados en el catálogo de servicios de CATS

...

- En el campo "Resumen" debe figurar el nombre del usuario o de la empresa/organismo para la que se solicita el acceso.

^ Información detallada

Resumen * **Ortografía**

Ejemplo: Solicitud alta VPN – [Nombre/DNI] / [Empresa/Organismo]

- En la descripción del ticket se debe incluir la siguiente información **obligatoriamente**:

Se solicita la generación de un acceso VPN a la red de la Conselleria de Sanitat Universal i Salut Pública.

Los datos relacionados para dicho acceso son los siguientes:

Nombre y apellidos del usuario final*:

DNI del usuario final*:

Empresa/Organismo del usuario final*:

Teléfono del usuario final*:

Correo electrónico del usuario final*:

Proyecto/Servicio*:

Listado de accesos requeridos:

- Aplicación o funcionalidad*:
- Dirección IP:
- Puertos:

* Campos obligatorios

5 Configuración del Acceso

5.1 Modo VPN SSL

PASOS:

- 1.- Conectar al PC el lector con la tarjeta criptográfica (certificado de la ACCV, DNI electrónico o FNMT).
- 2.- Introducir en un navegador web: ["https://vpn.san.gva.es"](https://vpn.san.gva.es) (Ver **NOTA**).
- 3.- Seleccionar el certificado en la ventana emergente que aparece (se pedirá el PIN del certificado).
- 4.- Introducir Usuario y Password asignado a la conexión VPN (estas credenciales son para acceder a la red de Conselleria y serán facilitadas por el CGRA llamando al 961961555).
- 5.- Aparecerá una ventana de CiscoAnyConnect que pedirá descargar e instalar un cliente ligero de Cisco para la conexión VPN.
- 6.- Una vez finalizada la instalación, la conexión pasa a estado "connected" y con una dirección IP de Sanidad asignada.

NOTA:

SI EL PC DESDE EL QUE SE VA A REALIZAR LA CONEXIÓN VPN SSL TIENE SISTEMA OPERATIVO WINDOWS, SE PUEDE DESCARGAR DIRECTAMENTE LA APLICACIÓN "Cisco Anyconnect" DESDE LA WEB <https://www.san.gva.es/web/conselleria-de-sanidad-universal-y-salud-publica/client-vpn> Y EJECUTARLA ESPECIFICANDO COMO SERVIDOR REMOTO "vpn.san.gva.es" (se solicitará a continuación el PIN del certificado, así como el usuario/password asociado a la conexión).

Estás en: Conselleria de Sanidad Universal y Salud Pública / Cliente VPN

CLIENTE VPN PARA CONEXIÓN A LA RED DE LA CONSELLERIA DE SANITAT

Para instalar el cliente VPN en tu equipo:

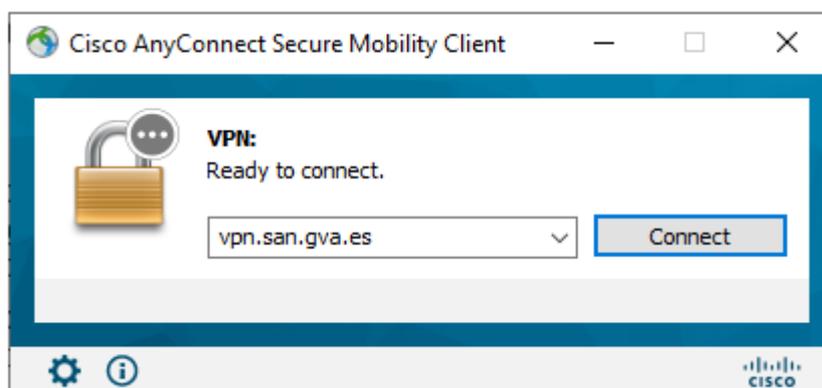
▶ Manual de acceso a Conselleria de Sanitat Universal i Salut Pública mediante cliente VPN

1. Si tienes una versión anterior instalada, desinstala primero
2. Descàrrega la versió Cisco Anyconnect 4.10.06 del sistema operatiu corresponent

▶ Windows 8, 10 i 11

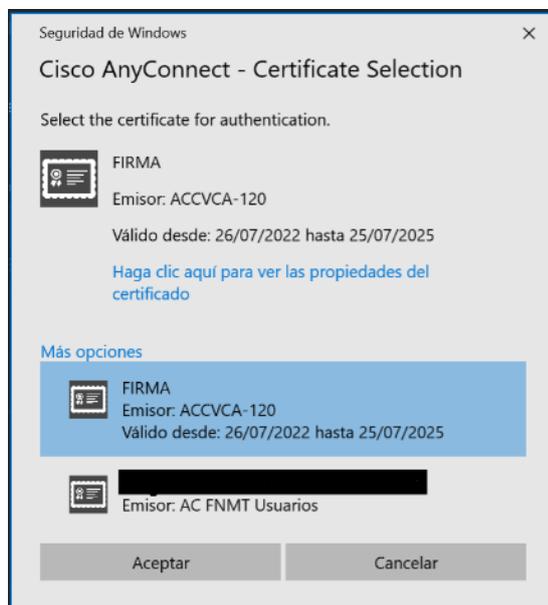
▶ Linux x64

▶ Mac

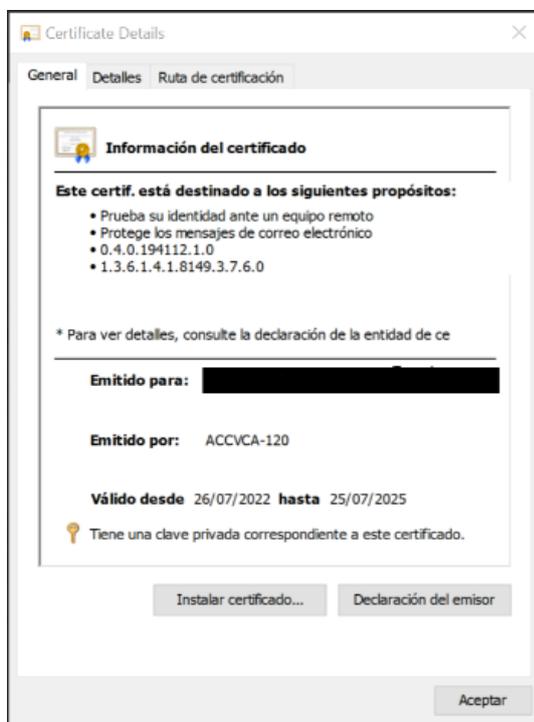


Cuando la aplicación nos pida el certificado personal, deberemos seccionar el certificado asociado al usuario que va a acceder a la VPN.

Este certificado personal **deberá estar instalado en la cuenta de usuario del equipo.**



Podemos hacer clic en las propiedades del certificado para asegurarnos de que hemos elegido nuestro certificado.



5.2 Instalación de los certificados de la ACCV sobre macOS

A continuación, se describen los pasos a realizar para instalar los certificados digitales de la cadena de certificación de la Agencia de Tecnología y Certificación Electrónica, ACCV, en el navegador Safari sobre los sistemas operativos macOS.

La instalación de la cadena de certificación en el navegador es imprescindible para el correcto funcionamiento de sus certificados.

Los pasos que seguir son los siguientes:

- Abra el navegador Safari, acceda a la página <https://www.accv.es/vl/servicios/empresas/descarga-de-certificados-jerarquia/> y pulse sobre el icono “**Descargar Jerarquía**”



- Haga clic sobre los enlaces “**ACCVRAIZ1**”, “**ACCVA-120**” y “**ACCVA-110**” y descargarlos.

[ACCVRAIZ1 | CA RAÍZ \(VIGENTE HASTA 31/12/2030\)](#) ⌵

Emisor: ACCVRAIZ1
Hash: 9A:6E:C0:12:E1:A7:DA:9D:BE:34:19:4D:47:8A:D7:C0:DB:18:22:FB:07:1D:F1:29:81:49:6E:D1:04:38:41:13
Clave: RSA 4096 bits - SHA256
CRL: [Lista de certificados revocados.](#)

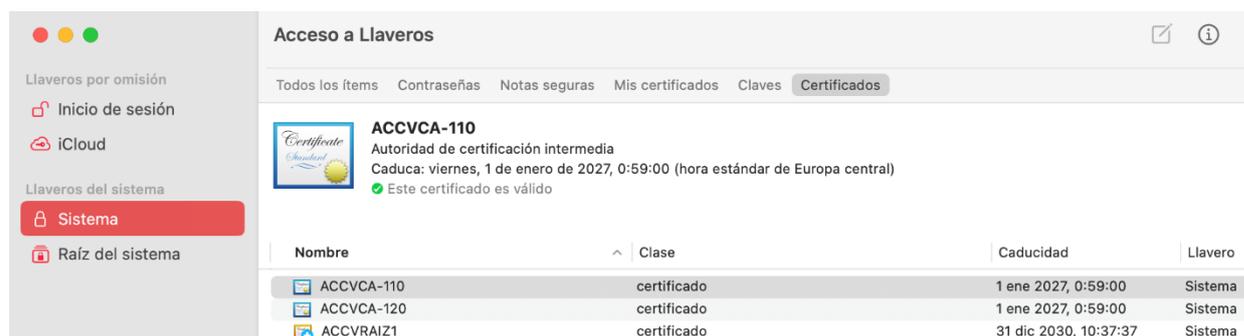
[ACCVA-120 | CA SUBORDINADA PARA PERSONAS FÍSICAS \(VIGENTE HASTA 31/12/2026\)](#) ⌵

Emisor: ACCVRAIZ1
Hash: 2D:E6:20:F2:D1:20:0A:A9:0B:16:C3:CC:F6:70:FD:7E:D1:43:79:AB:06:FA:8B:03:1C:FE:F8:DA:05:1E:A5:A2
Clave: RSA 4096 bits - SHA256
CRL: [Lista de certificados revocados.](#)

[ACCVA-110 | CA SUBORDINADA PARA ENTIDADES \(VIGENTE HASTA 31/12/2026\)](#) ⌵

Emisor: ACCVRAIZ1
Hash: E9:32:7A:34:7C:BE:1C:B9:4C:DC:9A:A5:4C:B3:1B:6E:43:D6:89:68:D1:7D:09:CE:32:6A:09:1B:FC:2F:0B:11
Clave: RSA 4096 bits - SHA256
CRL: [Lista de certificados revocados.](#)

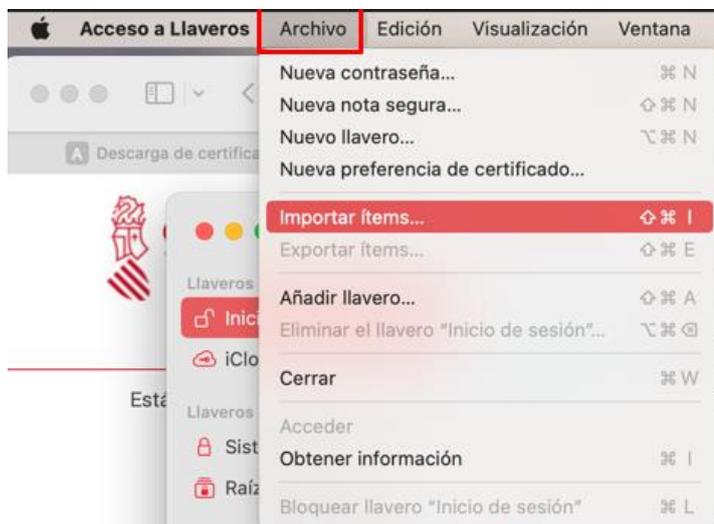
- c) Ir a la carpeta de Descargas y hacer doble click sobre el certificado **ACCVRAIZ1.crt** para instalarlo y registrarlo en su Sistema.
- d) Repetir esta operación para **ACCVCA-120.crt** y **ACCVCA-110.crt**
- e) Comprobar que habéis registrado correctamente los tres certificados anteriores, abra la aplicación “Acceso a llaveros” y seleccionar “Sistema” → “Certificados”.



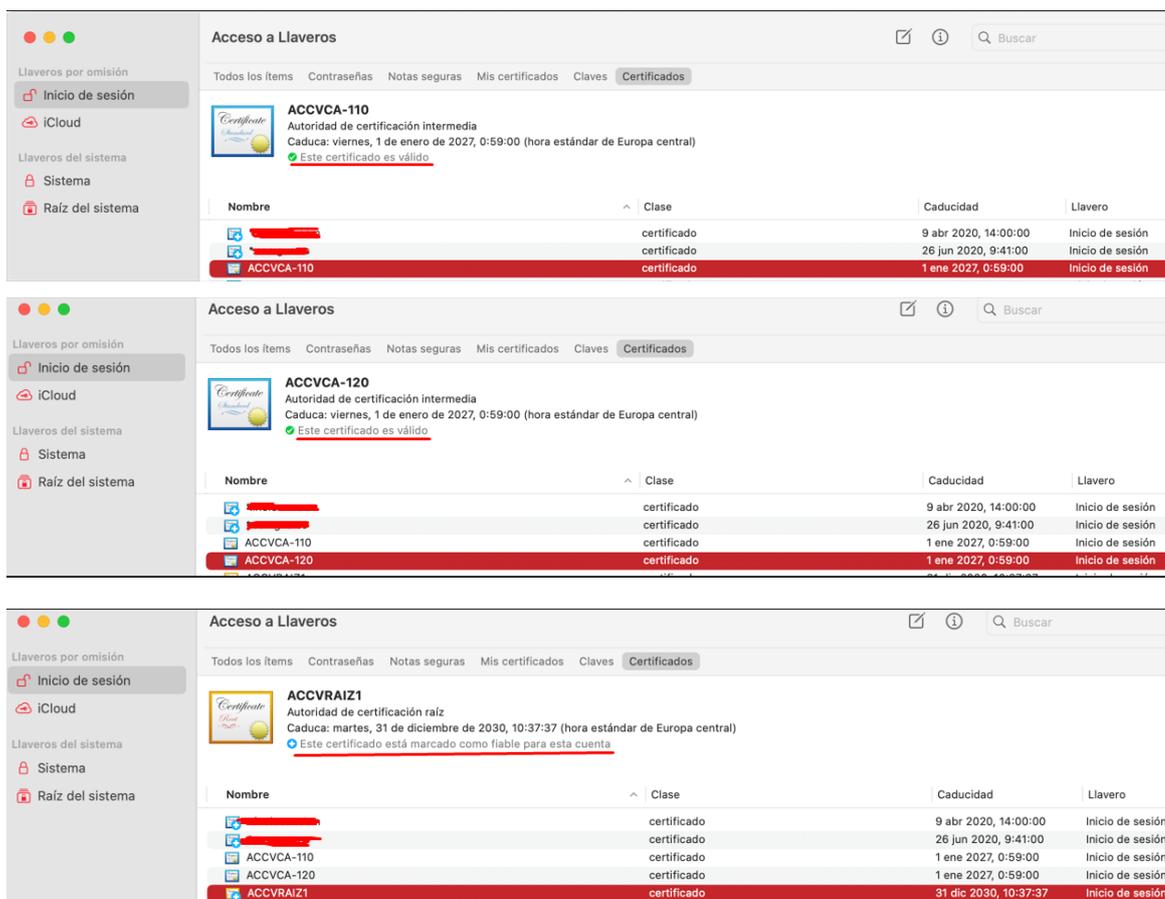
- f) Hacer click derecho sobre el certificado “ACCVRAIZ1” i seleccionar “Obtener información”. En la ventana del certificado despliegue “Confiar” y seleccione “Confiar siempre” en la opción “Al utilizar este certificado”



- g) Instalar los tres certificados en ‘Inicio de sesión’ mediante el menú de “Acceso a llaveros” en “Archivo→Importar items”.



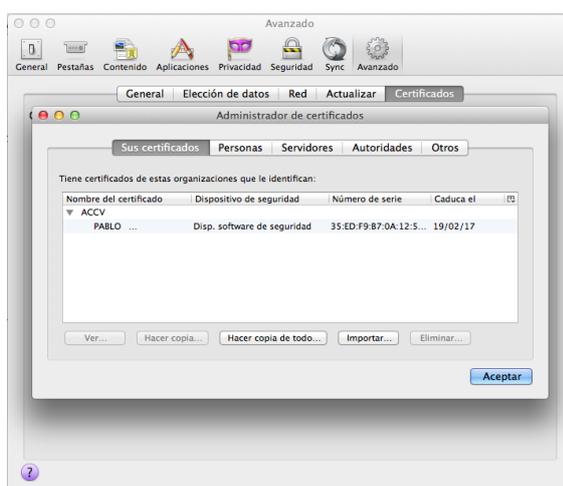
h) Repita el proceso f) para ACCVRAIZ1 y compruebe que ha registrado correctamente los tres certificados.



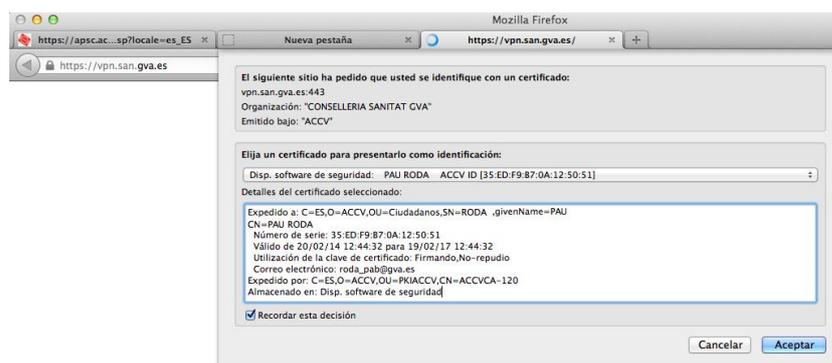
5.3 Configuración VPN macOS

Ahora vamos a describir los pasos a realizar para realizar la conexión VPN. El primer paso es comprobar que el certificado está correctamente instalado.

Es posible que se pida una contraseña maestra que deberemos configurar en el submenú **Seguridad**, que se nos pedirá tras arrancar el navegador o acceder a una web segura o con petición de **Login**.



El siguiente paso es acceder a la web <https://vpn.san.gva.es> donde automáticamente el navegador pedirá el acceso a través de nuestro certificado tal y como muestra la siguiente imagen:

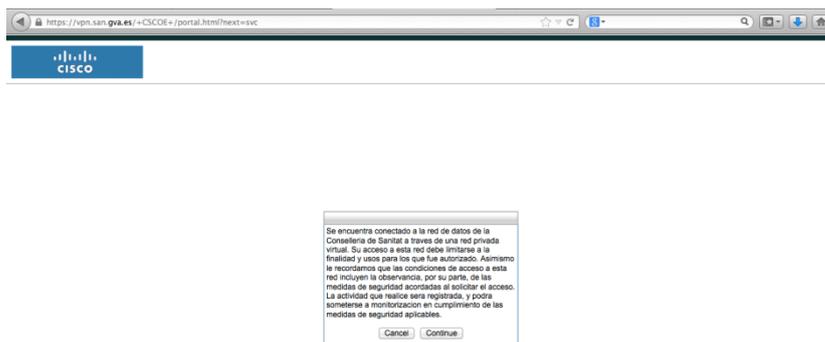


Tras el primer paso (**Autenticación de Usuario**) se nos pedirá la **Identificación**, donde se insertará el usuario y password facilitado por CGRA.

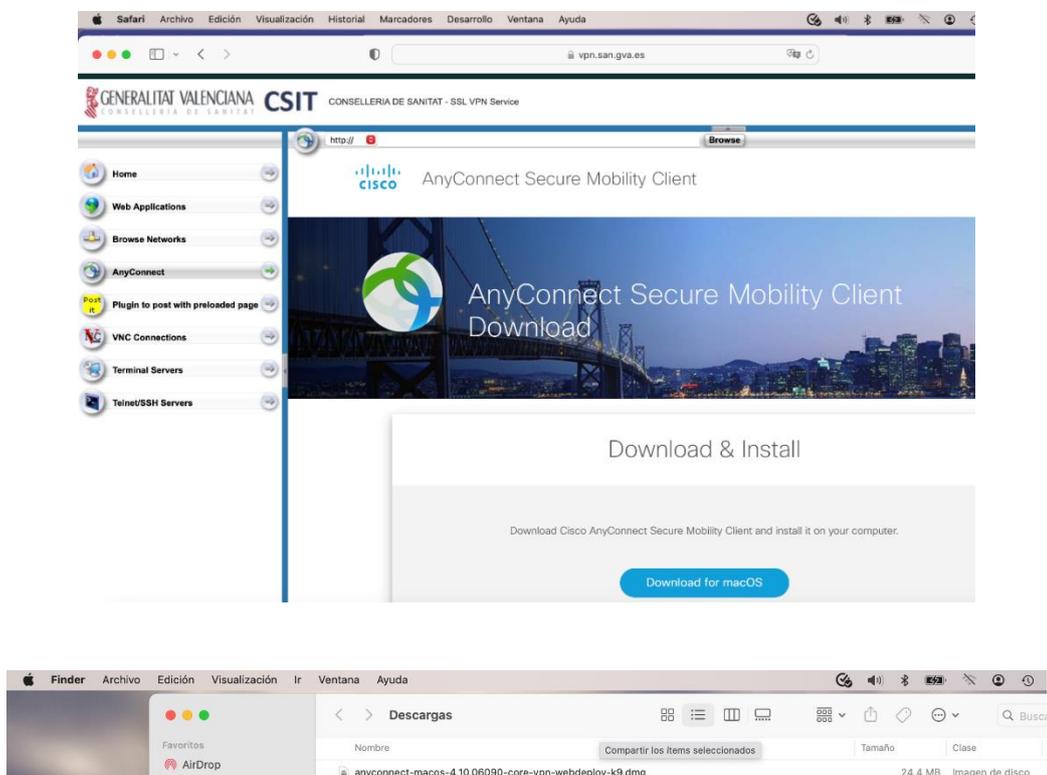
En algunas ocasiones no se produce la autenticación en primera instancia y aparece directamente la identificación, causando fallo directamente con el usuario/password facilitado. En estos casos se debe revisar que los certificados y la contraseña maestra

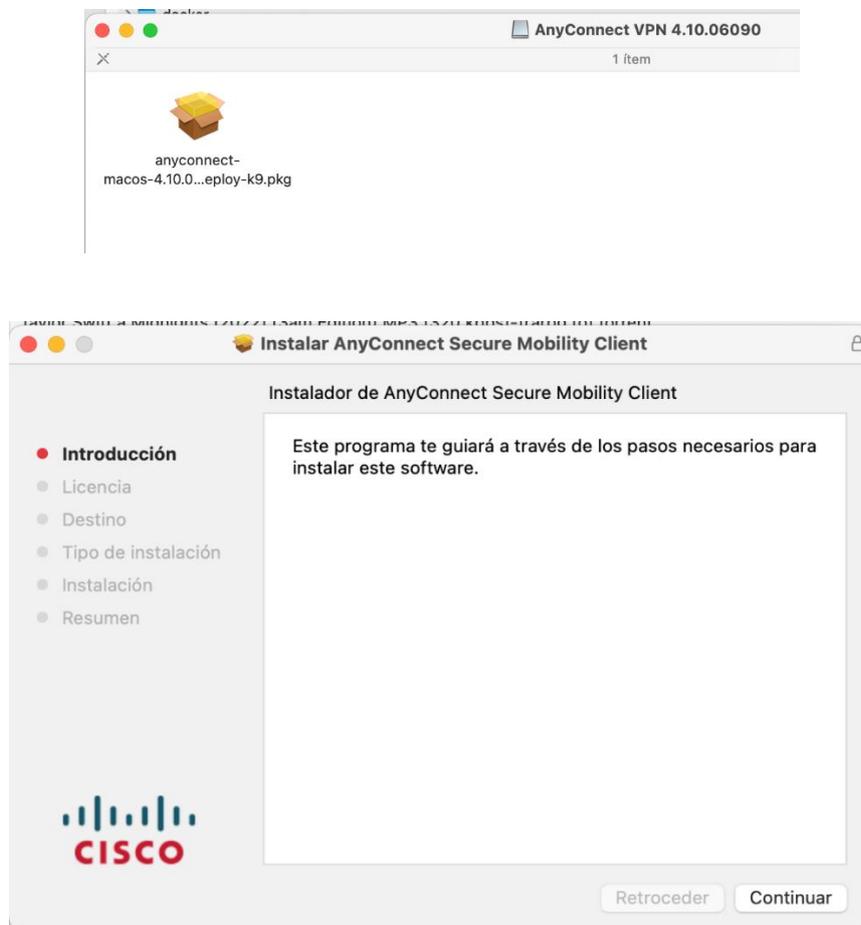
estén correctamente configurados.

Una vez validado el acceso aparecerá una pantalla como la siguiente mostrando un mensaje de bienvenida a la *Red Arterias*.

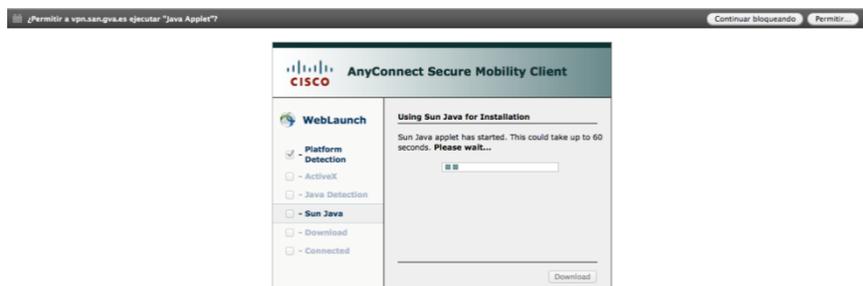


Acto seguido la web redirige al applet que detectará el sistema operativo y facilitará la descarga del instalador del cliente ligero de Cisco para que se realice la conexión.





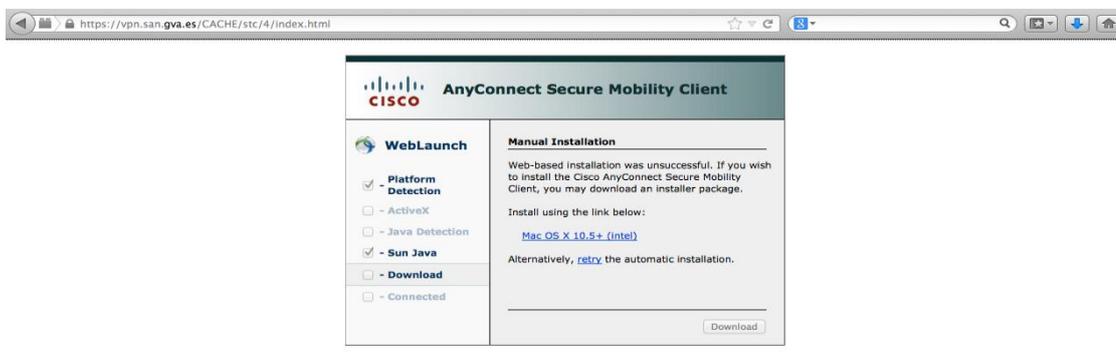
En caso de que la seguridad del navegador esté activada aparecerá el mensaje **¿Permitir a vpn.san.gva.es ejecutar “Java Applet”?** Se deberá permitir el acceso para la autodetección.



Es posible que se vuelva a pedir confirmación de acceso durante la ejecución del applet, tal y como se muestra:



Cuando se detecta el sistema operativo se lanza directamente el enlace al instalador recomendado:



Y al acceder al enlace nos descargamos el instalador, que posteriormente ejecutaremos e iniciaremos:



6 Soporte para la conexión a empresas externas.

6.1 Alcance del Soporte.

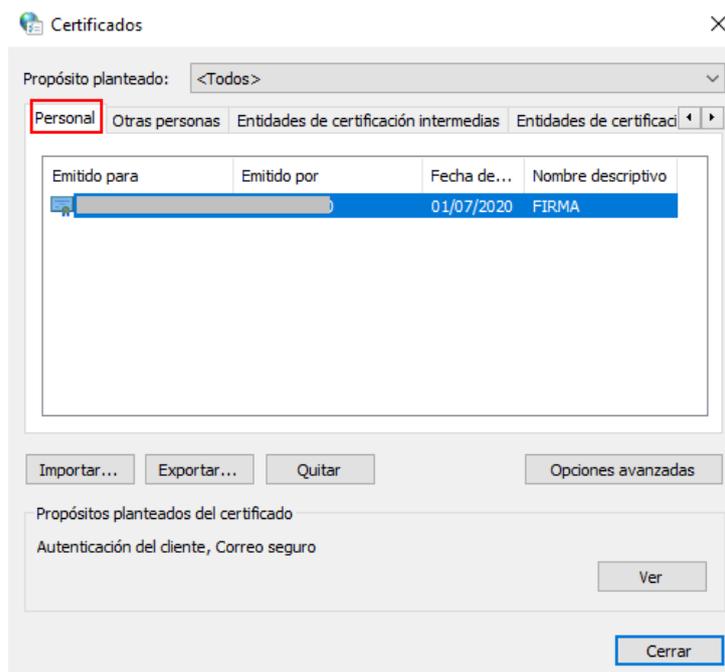
- El soporte que el CGRA ofrece a las empresas para la conexión mediante cliente de VPN se centra en los problemas que surjan con el concentrador de VPN ubicado en la red Arterias.
- Si el concentrador de VPN está funcionando normalmente, los problemas que aparezcan con la conexión del cliente deben ser resueltos por el departamento de informática interna o redes de la propia empresa. No obstante, el CGRA prestará la ayuda oportuna para que el personal de la empresa pueda averiguar donde reside su problema.
- En caso de tener que contactar con el CGRA para descartar problemas con el concentrador, o cualquier otra duda, preferiblemente lo hará el personal de la empresa de soporte a Informática y no el usuario final.

6.2 Pasos que seguir cuando haya problemas.

- Revisión de los requerimientos previos descritos en el apartado 2 de este documento.
- Revisión de los fallos más frecuentes del apartado 6.3 de este documento.
- Contacto con el soporte interno de tu propia empresa para que revisen que se cumplan todos los requisitos previos.
- Puesta en contacto del soporte de Informática interna de la empresa con el CGRA en el 902 20 20 03. Siendo conscientes que el soporte proporcionado por el CGRA es el definido el punto 6.1 (Alcance del soporte).

6.3 Fallos más frecuentes.

6.3.1 El Cisco AnyConnect no encuentra mi certificado de usuario.



Este error puede deberse a 2 causas:

- Funcionamiento incorrecto del lector de tarjetas o un problema en el certificado. Puede ser necesario reinstalar los drivers del lector (realizando pruebas en varios PCs) o consultar con la ACCV si hay algún problema con el certificado en caso de que el error persista. Consultar con el soporte local de Informática en la empresa para descartar posibles limitaciones o configuraciones incorrectas de los PCs.
- Puede comprobarse si el certificado funciona correctamente utilizándolo para identificarse en la web de la Agencia Tributaria (<http://www.aeat.es>). En caso de que funcione OK, entonces el problema debe estar en el *Cisco VPN Client*, el cual deberá actualizarse de versión siguiendo las indicaciones del apartado 2 en este mismo documento.
- El certificado personal debe aparecer en la pestaña Personal tal y como se indica en la imagen. (Panel de Control → Opciones de Internet → Contenido → Certificados).

6.3.2 Certificados raíz no importados.

Los certificados raíz de la ACCV son necesarios para validar certificados de usuario por lo que deben instalarse siguiendo las indicaciones del apartado 3.2.1 en este mismo documento.

6.3.3 Error 412

Este error puede deberse a 3 causas:

- Problema local del *Cisco Anyconnect* debido al cacheo interno de conexiones anteriores. Puede solucionarse cerrando el cliente y volviéndolo a abrir. En otras ocasiones puede ser necesario reiniciar el servicio de Windows “Cisco Systems, Inc. VPN Service” o incluso reiniciar el PC.
- Problema en la conexión a Internet. Cuando en el log del *Cisco Anyconnect* se aprecian muchas retransmisiones de paquetes y posteriormente la eliminación de los SAs del túnel VPN, la causa puede ser debida a microcortes en la conexión a Internet utilizada. Es necesario realizar pruebas de conexión a través de una conexión a Internet distinta para discernir si este es el problema.

TAMBIÉN ES NECESARIO QUE EL SOPORTE LOCAL DE INFORMÁTICA VERIFIQUE QUE LOS FIREWALLS DE LA EMPRESA TIENE ABIERTOS LOS PUERTOS QUE UTILIZA LA VPN:

UDP 500 (ISAKMP/IKE)

UDP 4500 (NAT-T)

Protocolo de encapsulación ESP (IP 50)

Protocolo de autenticación AH (IP 51)

- Problema en el Concentrador VPN de Sanidad. Es una incidencia muy extraña y afectaría a todas las conexiones VPN por lo que en caso de realizar alguna actuación sobre este equipo se avisaría adecuadamente con antelación suficiente.

6.3.4 Error 427



Este error puede deberse a 2 causas:

- Fallo al negociar las políticas (típicamente la IP asignada) a través del túnel VPN. Consultar al CGRA.
- Tiempo excedido para especificar el password individual. Escribir el password con mayor rapidez nada más sale la pantalla.

En caso de que al escribir el password vuelva a salir otra vez la misma pantalla solicitándolo, eso indica que se introducido incorrectamente. Consultar al CGRA para confirmar la contraseña asignada.

6.3.5 Error de negociación de certificado

En el caso de que aparezcan las siguientes líneas:

```
CERT/0x63600035
Done with the hash signing with signature length of 0.
CERT/0xE3600005
Failed to RSA sign the hash for IKE phase 1 negotiation using my certificate.
IKE/0xE300009B
Failed to generate signature: Signature generation failed (SigUtil:97)
IKE/0xE300009B
Failed to build Signature payload (MsgHandlerMM:489)
IKE/0xE300009B
Failed to build MM msg5 (NavigatorMM:312)
IKE/0xE30000A7
Unexpected SW error occurred while processing Identity Protection (Main Mode)
negotiator:(Navigator:2263)
```

El error viene dado por lo siguiente:

“The VPN client using certificate authentication with a 4096 bit ID certificate fails to connect. The following error messages may be seen in the VPN client log”

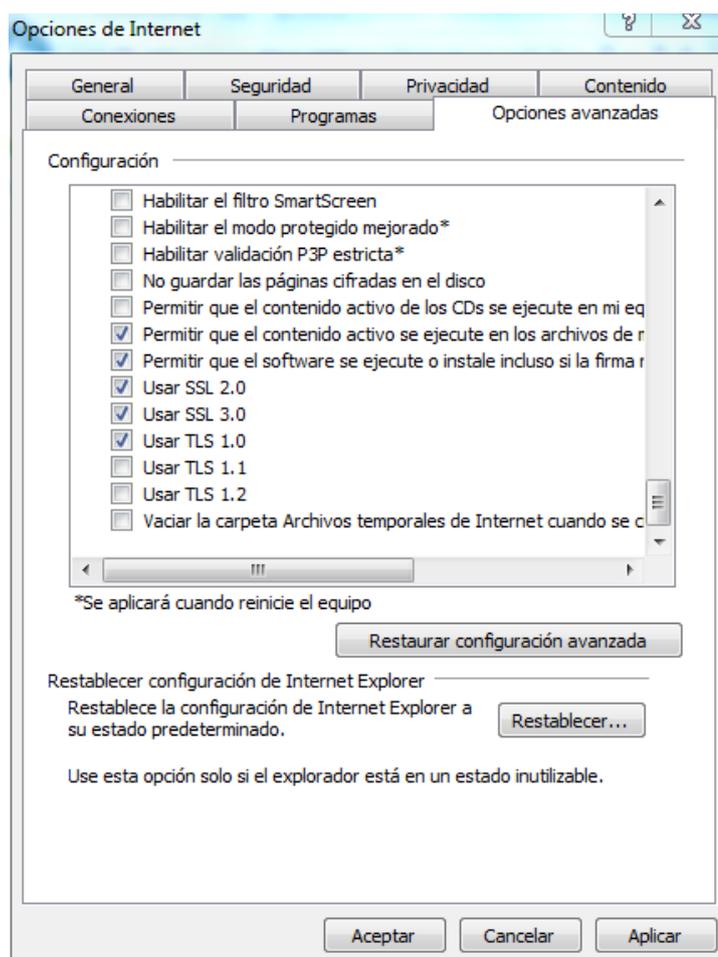
Y aparecerán los siguientes mensajes:

Failed to RSA sign the hash for IKE phase 1 negotiation using my certificate.
Failed to generate signature: Signature generation failed (SigUtil:97)
Failed to build Signature payload (MsgHandlerMM:489)
Failed to build MM msg5 (NavigatorMM:312)
Unexpected SW error occurred while processing Identity Protection (Main Mode)
negotiator:(Navigator:2263)

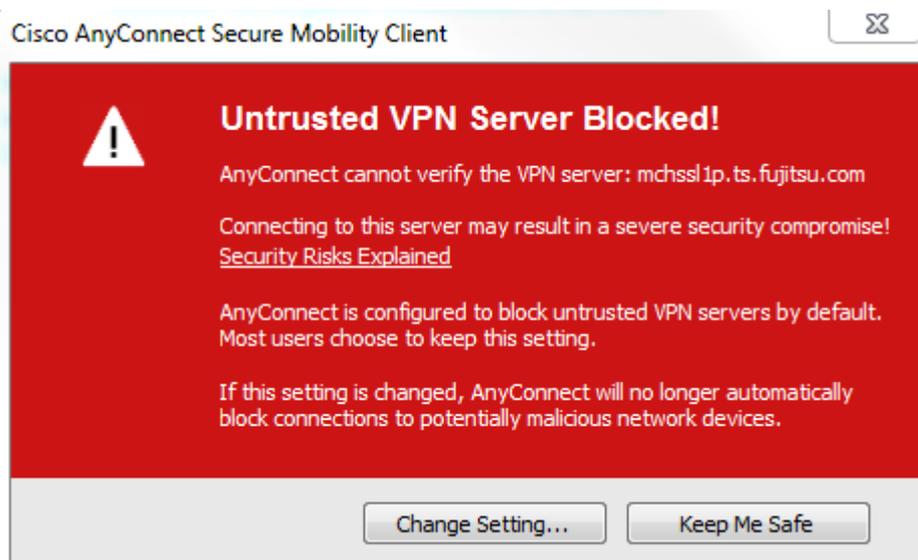
Por lo tanto, se debe revisar el certificado con que se conecta el cliente de VPN.

6.3.6 Error de conexión

Si aparece el mensaje de “Connection attempt failed. Please try again”, se soluciona activando en el Internet Explorer, Opciones de Internet, Opciones avanzadas, los siguientes puntos indicados en el gráfico:



6.3.7 Error de conexión con Cisco AnyConnect:

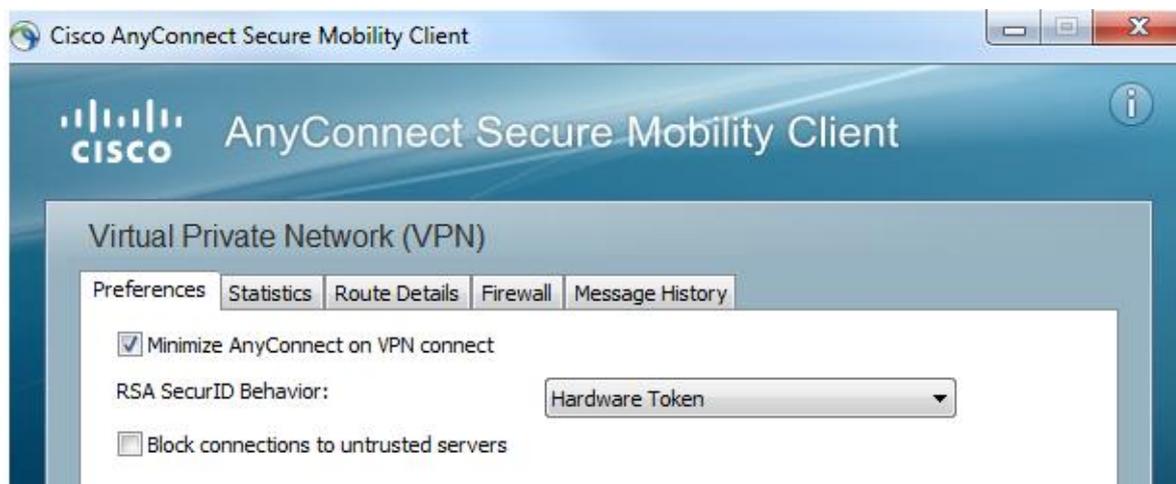


Este problema se soluciona instalando el certificado de la Autoridad de Certificación para personas físicas y otros usos de la ACCV, **ACCVCA-120**.

Se puede descargar desde la web de la ACCV:

<https://www.accv.es/servicios/descargar-jerarquia-accv/>

Si el problema persiste tras instalar el certificado, se puede solucionar a través de la opción "Change Settings", desmarcando la opción "Block connections to untrusted servers".



6.3.8 Error de conexión con nuevas tarjetas de la ACCV (clave de 2048 bits)

En caso de que la conexión VPN falle utilizando las nuevas tarjetas emitidas por la ACCV con funcionalidad SHA-2 y claves de 2048 bits, se necesitará hacer lo siguiente:

- Instalar la última versión de controlador de la tarjeta Siemens desde: http://www.accv.es/fileadmin/Archivos/software/ACCV_instal_Tarjeta.exe

6.3.9 Error de conexión con aplicaciones tras establecer la VPN

En algunos casos cuando la empresa remota utiliza un servidor proxy en su red, puede suceder que el acceso a servidores o aplicaciones de la Conselleria no funcione correctamente. Esto es debido a que la resolución DNS de esa aplicación la realiza el proxy de la empresa en lugar de hacerla el fichero host del PC remoto.

Para solucionar ese problema, la empresa deberá configurar excepciones en el proxy o en el navegador web de los usuarios que conecten de forma que, para determinadas URLs, no se conecte con el proxy de la empresa sino de forma directa para así realizar correctamente la resolución DNS.

ANEXO I: Cláusulas asociadas al uso del servicio VPN

Mediante la firma de la solicitud de acceso, el solicitante queda obligado al cumplimiento de las siguientes cláusulas, que regulan el acceso al servicio de conexión VPN ofrecido por la Conselleria de Sanidad a empleados y proveedores.

Primera- Finalidad

Realizar un uso correcto del servicio de conexión VPN, así como de los recursos informáticos a los que se acceda.

Segunda- Uso de los recursos informáticos.

1. Para utilizar los recursos informáticos ofrecidos por la Conselleria de Sanidad, el solicitante ha de obtener previamente la autorización correspondiente.
2. El solicitante será el responsable directo de todas las actividades realizadas bajo su nombre.
3. Bajo ningún concepto el solicitante atentará contra la integridad, funcionamiento o disponibilidad de los recursos informáticos propiedad de la Conselleria de Sanidad.
4. Se considera un atentado contra la integridad de los recursos informáticos de la Conselleria de Sanidad por parte del usuario, la falta de medidas contra software malicioso y la instalación de software no autorizado, así como el acceso a los recursos informáticos fuera del plazo de duración de la solicitud.

Tercera- Seguridad de la información.

1. El solicitante se compromete a cumplir todas las normas relativas a acceso a datos¹, con especial mención a las siguientes:
 - a. Obligación de mantener el deber de secreto de sus propias claves de acceso. Nunca debe facilitar a nadie sus credenciales.
 - b. Obligación de notificar cualquier situación en la que el secreto de su contraseña se haya visto comprometido.
 - c. Obligación de comunicar las incidencias de seguridad de las que tenga conocimiento.
 - d. Obligación de cerrar la conexión cuando abandone el puesto de trabajo.
 - e. Obligación de limitar el uso de la información al desempeño de sus funciones.
 - f. Obligación de informar sobre cambios en el desempeño de sus funciones por si pudiera suponer cambios en sus perfiles de acceso.
 - g. Obligación de mantener secreto sobre la información a las que tiene acceso, en especial sobre los datos de carácter personal y de salud, incluso tras haber finalizado su relación profesional con la Conselleria de Sanidad.
 - h. Prohibición de extraer información, sin autorización expresa, a soportes externos tales como disquetes, memorias, discos, portátiles o cualquier otro soporte.

¹ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE, 6 de diciembre de 2018). Real Decreto-ley 14/2019, de 31 de octubre. Ley Orgánica 7/2021 de 26 de mayo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

- i. Obligación de velar por la seguridad de las copias o extracciones de datos para cuyo manejo se encuentre autorizado y, en su caso, de alertar sobre su posible deterioro u obsolescencia.
 - j. Obligación de vigilar la impresión y el flujo de documentos generados durante el desempeño de sus funciones, con el fin de prevenir su sustracción o la pérdida de confidencialidad de la información que contengan.
 - k. Obligación de leer y cumplir las normas de seguridad y buena conducta que, en relación con el tratamiento de datos, establezca la Conselleria de Sanidad.
2. En el caso de usuarios que accedan en nombre de una empresa:
- a. El solicitante se responsabilizará de que sus empleados conozcan y se sometan a las condiciones establecidas en los párrafos anteriores.
 - b. El solicitante mantendrá y proporcionará a la Conselleria de Sanidad una relación permanentemente actualizada de los usuarios con acceso autorizado al servicio VPN.
 - c. El solicitante deberá mantener un registro de accesos al servicio VPN, que almacene el nombre de usuario conectado, fecha y hora de conexión, fecha y hora de desconexión, y recurso al que accede, independientemente de las medidas que la Conselleria de Sanidad tiene adoptadas en este aspecto.
 - d. La Conselleria de Sanidad se reserva el derecho a comprobar el cumplimiento, por parte del solicitante, de las todas las medidas expuestas anteriormente.