COMPROBACIONES DE SEGURIDAD PARA LOS EQUIPOS QUE SE CONECTAN A TRAVÉS DE LA VPN CORPORATIVA

Para aumentar la seguridad de la red corporativa de la Generalitat, además de las comprobaciones que se puedan realizar durante el proceso de alta de conexiones VPN corporativas, se han implantado una serie de comprobaciones básicas de seguridad que se ejecutan cada vez que los usuarios inician el proceso de conexión a la citada VPN y que impiden la conexión si los equipos utilizados no cumplen ciertos requisitos.

Este manual, dirigido a las personas usuarias de la conexión VPN corporativa, especifica dichos requisitos mínimos e indica cómo actuar en caso de que, a pesar de cumplirlos, se encuentren problemas en el proceso de conexión.

Contenido

1 Equipos con sistema operativo Windows

Los equipos con sistema operativo Windows deben cumplir los siguientes requisitos para que se pueda completar la conexión con la red corporativa:

1.1 Versión del sistema operativo

La versión del sistema operativo debe contar con soporte por parte de Microsoft. Las versiones soportadas se irán actualizando a medida que Microsoft cambie su política de soporte de productos. En el momento de publicar el presente documento las versiones soportadas son las siguientes:

- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Como referencia general y actualizada, se puede usar la siguiente página web e introducir la versión del sistema operativo cuya fecha de soporte se quiera comprobar: https://docs.microsoft.com/es-es/lifecycle/products/

1.2 Antivirus instalado

El equipo debe contar con un antivirus instalado, activo y con soporte por parte del fabricante. Además, en los antivirus soportados se comprueba que la última actualización por parte del fabricante fue hace menos de 5 días. En el Apartado 5 tiene el listado completo de antivirus y versiones para los que se realiza dicha comprobación.

2 Equipos con sistema operativo Mac OS

Los equipos con sistema operativo Mac OS deben cumplir los siguientes requisitos para que se pueda completar la conexión con la red corporativa.

2.1 Versión del sistema operativo

La versión del sistema operativo debe contar con soporte por parte de Apple. Las versiones soportadas se irán actualizando a medida que Apple cambie su política de soporte de productos. En el momento de publicar el presente documento las versiones soportadas son las siguientes:

- macOS Big Sur 11
- macOS Monterrey 12
- macOS Ventura 13
- macOS Sonoma 14

Apple no publica una directiva concreta de soporte de sus productos pero, como referencia general, su política de soporte suele ser dos versiones por detrás de la última soportada. La siguiente referencia no oficial puede ayudar a determinar las versiones soportadas en cada momento: https://computing.cs.cmu.edu/desktop/os-lifecycle

2.2 Antivirus instalado

El equipo debe contar con un antivirus instalado, activo y con soporte por parte del fabricante. Además, en los antivirus soportados se comprueba que la última actualización por parte del fabricante fue hace menos de 5 días. Para comprobar el listado completo de antivirus y versiones que soportan la comprobación de firmas, se puede consultar el apartado 5 de este mismo documento.

2.3 System Integrity Protection activo

El sistema operativo Mac OS tiene una funcionalidad llamada 'System Integrity Protection' que realiza comprobaciones activas de los ficheros y servicios del sistema para comprobar si han sido alterados, además corrige automáticamente los problemas que pudieran existir. Si esta funcionalidad está desactivada, no se permitirá la conexión con la red corporativa. A continuación, puede encontrar más información sobre esta funcionalidad y cómo activarla:

https://developer.apple.com/documentation/security/disabling_and_enabling_system_integrity_protection

3 Consideraciones generales

Las comprobaciones de seguridad que realiza el software para la conexión mediante VPN podrían no funcionar adecuadamente si se utilizan versiones antiguas de la aplicación. Cuando existan problemas de conexión, se debe descargar la última versión del software disponible en el siguiente enlace: https://softwarevpn.gva.es/.

La conexión al enlace anterior requiere tener instalado en el equipo el mismo certificado digital que se necesita también para conectar a la VPN de Generalitat, por lo que se puede utilizar para comprobar que el certificado digital del usuario no causará problemas al utilizar la aplicación VPN.

Si se tienen problemas en la conexión al enlace anterior, es posible que el certificado no sea válido. En ese caso, se puede comprobar su validez en el enlace http://valide.redsara.es/valide/inicio.html. Si aparece algún problema al realizar la validación de certificado del enlace anterior, por favor consulte con el organismo emisor de su certificado.

Los proveedores de certificados digitales admitidos tanto en el enlace de descarga de la aplicación VPN como en el propio acceso a la conexión VPN corporativa de la Generalitat son:

- ACCV
- Autoridad Certificación de la Abogacía
- Autoridad de Certificación de los Registradores
- Camerfirma
- FNMT

- DNIe
- Security Data
- Banco Central del Ecuador
- idCAT

4 Resolución de problemas

La DGTIC no proporcionará soporte a los usuarios pertenecientes a empresas adjudicatarias de contratos con la Generalitat. Si un usuario o usuaria tiene cualquier incidencia en el proceso o si sigue sin poder conectarse a la red corporativa tras aplicar estos cambios, deberá ponerse en contacto con su departamento TI.

Si un usuario o usuaria de la DGTIC tiene cualquier incidencia en el proceso o si sigue sin poder conectarse a la red corporativa tras aplicar estos cambios, tiene a su disposición el teléfono único del Centro de Atención al Usuario TIC, CAU-TIC (963 985300), y el Portal de Servicios de la DGTIC (gvatic.gva.es) para solicitar asistencia.

5 Listado de fabricantes de herramientas antivirus autorizados

- Apple Inc.
- AVAST Software a.s.
- Avast Software s.r.o.
- AVG Technologies CZ, s.r.o.
- Avira GmbH
- Bitdefender
- Carbon Black, Inc.
- Check Point Software Technologies
- Cisco Systems, Inc.
- ClamWin Pty Ltd
- CrowdStrike, Inc.
- Cybereason
- Cylance Inc.
- ESET
- F-Secure Corporation
- FireEye, Inc.
- Fortinet Inc.
- Ivanti, Inc.
- Kaspersky
- Kaspersky Lab
- Malwarebytes Corporation
- McAfee, Inc.
- Microsoft Corporation
- Palo Alto Networks, Inc.
- Panda Security, S.L.
- ReaQta BV
- SentinelOne
- Sophos
- Sophos Limited
- Sourcefire, Inc
- Stormshield
- Symantec Corporation
- Trend Micro
- Trend Micro, Inc.
- WatchGuard Technologies Inc