COMPROVACIONS DE SEGURETAT PER ALS EQUIPS QUE ES CONNECTEN A TRAVÉS DE LA VPN CORPORATIVA

Per a augmentar la seguretat de la xarxa corporativa de la Generalitat, a més de les comprovacions que es puguen realitzar durant el procés d'alta de connexions VPN corporatives, s'han implantat una sèrie de comprovacions bàsiques de seguretat que s'executen cada vegada que els usuaris inicien el procés de connexió a la citada VPN i que impedeixen la connexió si els equips utilitzats no compleixen uns certs requisits.

Aquest manual, dirigit a les persones usuàries de la connexió VPN corporativa, especifica aquests requisits mínims i indica com actuar en cas que, malgrat complir-los, es troben problemes en el procés de connexió.

Contingut

1 Equips amb sistema operatiu Windows

Els equips amb sistema operatiu Windows han de complir els següents requisits perquè es puga completar la connexió amb la xarxa corporativa:

1.1 Versió del sistema operatiu

La versió del sistema operatiu ha de comptar amb suport per part de Microsoft. Les versions suportades s'aniran actualitzant a mesura que Microsoft canvie la seua política de suport de productes. En el moment de publicar el present documente les versions suportades són les següents:

- Windows 10
- Windows 11
- Windows Server 2012 (fins al 10 d'octubre de 2023)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Com a referència general i actualitzada, es pot usar la següent pàgina web i introduir la versió del sistema operatiu la data de suport del qual es vulga comprovar: https://docs.microsoft.com/es-es/lifecycle/products/

1.2 Antivirus instal·lat

L'equip ha de comptar amb un antivirus instal·lat, actiu i amb suport per part del fabricant. A més, en els antivirus suportats es comprova que l'última actualització per part del fabricant va ser fa menys de cinc dies. L'apartat 5 té el llistat complet d'antivirus i versions per als quals es realitza aquesta comprovació.

2 Equips amb sistema operatiu Mac OS

Els equips amb sistema operatiu Mac OS han de complir els següents requisits perquè es puga completar la connexió amb la xarxa corporativa.

2.1 Versió del sistema operatiu

La versió del sistema operatiu ha de comptar amb suport per part d'Apple. Les versions suportades s'aniran actualitzant a mesura que Apple canvie la seua política de suport de productes. En el moment de publicar el present document, les versions suportades són les següents:

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

Apple no publica una directiva concreta de suport dels seus productes però, com a referència general, la seua política de suport sol ser dues versions per darrere de l'última suportada. La següent referència no oficial pot ajudar a determinar les versions suportades a cada moment: https://computing.cs.cmu.edu/desktop/os-lifecycle

2.2 Antivirus instal·lat

L'equip ha de comptar amb un antivirus instal·lat, actiu i amb suport per part del fabricant. A més, en els antivirus suportats es comprova que l'última actualització per part del fabricant va ser fa menys de cinc dies. Per a comprovar el llistat complet d'antivirus i versions que suporten la comprovació de signatures, es pot consultar l'apartat 5 d'aquest mateix document.

2.3 System Integrity Protection actiu

El sistema operatiu Mac OS té una funcionalitat anomenada 'System Integrity Protection' que realitza comprovacions actives dels fitxers i serveis del sistema per a comprovar si han sigut alterats, a més corregeix automàticament els problemes que puguen existir. Si aquesta funcionalitat està desactivada, no es permetrà la connexió amb la xarxa corporativa. A continuació, pot trobar més informació sobre aquesta funcionalitat i com activar-la:

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

3 Consideracions generals

Les comprovacions de seguretat que realitza el programari per a la connexió mitjançant VPN podrien no funcionar adequadament si s'utilitzen versions antigues de l'aplicació. Quan existisquen problemes de connexió, s'ha de descarregar l'última versió del programari disponible en el següent enllaç: https://softwarevpn.gva.es/.

La connexió a l'enllaç anterior requereix tindre instal·lat en l'equip el mateix certificat digital que es necessita també per a connectar a la VPN de Generalitat, per la qual cosa es pot utilitzar per a comprovar que el certificat digital de l'usuari no causarà problemes en utilitzar l'aplicació VPN.

Si es tenen problemes en la connexió a l'enllaç anterior, és possible que el certificat no siga vàlid. En aqueix cas, es pot comprovar la seua validesa en l'enllaç http://valide.redsara.es/valide/inicio.html. Si apareix algun problema en realitzar la validació de certificat de l'enllaç anterior, per favor consulte amb l'organisme emissor del seu certificat.

Els proveïdors de certificats digitals admesos tant en l'enllaç de descàrrega de l'aplicació VPN com en l'accés a la connexió VPN corporativa de la Generalitat són:

- ACCV
- Autoritat Certificació de l'Advocacia
- Autoritat de Certificació dels Registradors
- Camerfirma
- FNMT
- DNIe

- Security Data
- Banc Central de l'Equador
- idCAT

4 Resolució de problemes

La DGTIC no proporcionarà suport als usuaris pertanyents a empreses adjudicatàries de contractes amb la Generalitat. Si un usuari o usuària té qualsevol incidència en el procés o si segueix sense poder connectar-se a la xarxa corporativa després d'aplicar aquests canvis, haurà de posar-se en contacte amb el seu departament TI.

Si un usuari o usuària té qualsevol incidència en el procés o si segueix sense poder connectar-se a la xarxa corporativa després d'aplicar aquests canvis, té a la seua disposició el telèfon únic del Centre d'Atenció a l'Usuari TIC, CAU-TIC (963 985300), i el Portal de Serveis de la DGTIC (gvatic.gva.es) per a sol·licitar assistència.

5 Llistat de fabricants d'eines antivirus autoritzats

- 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