# Condiciones de seguridad para la prestación de servicios en régimen de teletrabajo por parte de personal de la Conselleria mediante dispositivos privados con motivo de la crisis del COVID-19

Las tecnologías de la información y las comunicaciones (TIC) son elementos críticos para la actividad de los centros sanitarios, así como para la coordinación de todo el sistema público de salud. Los profesionales que se ocupan de esas tecnologías son otro elemento crítico. Su conocimiento sobre las infraestructuras y servicios TIC de cada centro les hace difícilmente reemplazables.

En las circunstancias excepcionales en que nos encontramos es preciso evitar la exposición de todo el personal, incluidos los profesionales de las TIC, a riesgos innecesarios que pudieran comprometer su salud y la operatividad de los centros sanitarios. Esta situación obliga a considerar medidas extraordinarias, como permitir a determinadas personas el acceso desde sus domicilios a determinados sistemas de información de la Conselleria para realizar funciones análogas a las que realizan desde sus puestos de trabajo habituales (teletrabajo). Es más, ante la posibilidad de que los equipos corporativos disponibles no fueran suficientes para atender toda la demanda, se plantea la cuestión de si se podría permitir dicho acceso desde equipos personales (=domésticos), y en tal caso bajo qué condiciones.[1]

El uso de equipos domésticos para el acceso a infraestructuras, sistemas o información bajo la responsabilidad de la Conselleria entraña riesgos para todos los agentes implicados. En términos generales esos riesgos son inasumibles.

No obstante lo anterior, a continuación se indican algunas medidas extraordinarias que, si se aplican diligentemente, permiten reducir el riesgo a un nivel aceptable dadas las circunstancias.

1. La utilización de equipos personales para el acceso a los sistemas y servicios internos de la Conselleria es una solución excepcional que sólo debe permitirse en casos debidamente justificados. La firma de la autorización que figura en el Anexo 2 supone

1 Se sobreentiende que las funcionalidades requeridas no se limitan al acceso a los servicios publicados a través de Internet, como la consulta de la cuenta de correo electrónico corporativo, la asistencia a las actividades formativas de la EVES o del IVAP, las consultas a la historia de salud electrónica o de la bolsa de trabajo. Para todas estas actividades basta con disponer de un equipo básico y de las credenciales correspondientes, no siendo necesario ni un equipo corporativo, ni tener conexión a la rede de datos interna.

la aceptación de las condiciones descritas en este documento y, en la parte que corresponda, de las que figuran en la licencia de uso del producto[2].

2. El acceso a los sistemas y servicios internos de la Conselleria desde fuera de la red de datos corporativa debe realizarse siempre mediante VPN. Esto es válido tanto si los equipos son corporativos como domésticos. Cuanto sigue presupone que el usuario está habilitado y dispone de las credenciales necesarias, y que su equipo tiene instalado el cliente VPN.

3. Los usuarios que utilicen equipos domésticos deberán instalar previamente el producto Cytomic Endpoint Agent siguiendo el procedimiento descrito en el Anexo. La instalación de este software es obligatoria, independientemente de los productos de seguridad instalados en el equipo. Entre las características del producto y servicios asociados cabe destacar las siguientes[3]:
    a) El agente no interfiere con otros programas, incluidos productos de seguridad, y es muy parco en el consumo de recursos. Esencialmente se limita a comprobar la reputación de cada proceso justo antes de que se ejecute. Cuando el proceso no es fiable puede bloquearlo.
    b) El agente instalado en cada equipo actúa bajo la supervisión de una consola central que tiene visibilidad sobre toda la red de datos de la Conselleria. Desde esta consola se va construyendo una base de datos con los procesos fiables propios de nuestra organización (los de O-C, SIA, GAIA, etc.) Por este motivo el despliegue del producto debe hacerse de manera controlada, con un breve periodo inicial para que la consola aprenda a identificar nuestros procesos fiables antes de lanzar un despliegue masivo.
    c) El agente instalado no analiza las unidades de almacenamiento del equipo en busca de software malicioso. Llegado el caso, impide la ejecución del software malicioso, pero no lo elimina del equipo. Para eso es necesario otro software y hacerlo es responsabilidad del propietario del equipo doméstico, aunque en determinados casos podríamos intervenir y eliminarlo de manera remota.
    d) El agente recoge cierta información técnica de las máquinas en las que se instala, como el nombre del equipo, la dirección IP de la red local doméstica (ojo, no la IP pública), nombres de algunas carpetas y archivos… pero en ningún caso el historial de navegación, ni las carpetas o los archivos en sí. En algún caso esos nombres podrían resultar identificativos, por ejemplo si el nombre del equipo fuera “El_portátil_de_Fulanito_Fulánez”, o si se abriera un documento infectado llamado “Diario_de Fulanito_Fulánez.doc”.
    e) El agente forma parte de la familia de productos Panda EDR (Endpoint Detection and Response), que figura como producto cualificado en la edición de febrero de 2020 del Catálogo de Productos de Seguridad TIC que publica el CCN. En esta categoría se incluyen aquellos productos que cumplen los requisitos de seguridad exigidos para el manejo de información sensible. El Catálogo reconoce la capacidad de este producto para ser utilizado en sistemas de categoría alta según la clasificación del ENS.[4]
    f) La Conselleria sólo usará la información que proporciona este producto sobre los equipos en los que esté instalado para realizar el debido control de accesos

---

2 https://manage.cytomicmodel.com/Resources/Views/Eula/ad_es-ES_cytomic.html

3 Una guía completa está disponible en: https://info.cytomicmodel.com/resources/guides/EPDR/v09/es/EPDR-guia-ES.pdf

4 CCN-STIC-105 Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación Centro Criptológico Nacional 2 Edición Febrero de 2020: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html

a sus sistemas, para investigar posibles incidencias que afectaran a los activos bajo su responsabilidad y para gestionar las licencias del producto. En ningún caso se accederá a otra información que la imprescindible para esas tareas sin comunicación y consentimiento previos del usuario del equipo.

g) En caso de incidente o duda relacionados con el uso de este software, los usuarios deben ponerse en contacto con CATS (tf. 989500).
h) La Conselleria dispone de cierto número de licencias temporales de este producto para hacer frente a la crisis desatada por el COVID-19. El futuro de esas licencias dependerá de cómo vaya evolucionando la situación.

4. La desactivación o la desinstalación del agente deben realizarse desde la consola central. En el caso de que un usuario quisiera desactivar o eliminar el agente de su equipo, deberá comunicarlo previamente a CATS.
5. Aparte de los ataques de software malicioso, la principal amenaza para los activos bajo responsabilidad de la Conselleria son las fugas de información. Tratándose de equipos no controlados directamente por la Conselleria, y dado que estamos en una situación de emergencia, poco se puede hacer más que apelar a la responsabilidad del usuario. Así, el usuario del equipo debe comprometerse no descargar de los sistemas de la Conselleria información que no sea estrictamente imprescindible para el desempeño de sus funciones en estas circunstancias excepcionales. También debe comprometerse a eliminarla del equipo una vez haya dejado de ser necesaria, a no guardar copias en otros dispositivos ni en ningún espacio de almacenamiento en la nube (Drive, OneDrive, iCloud, Dropbox, etc.), a no transferirla a terceros por ningún medio (Whatsapp, Messenger…) y a no ejecutar en el equipo programas de compartición de ficheros (P2P) mientras tenga instalado el software para el acceso por VPN a la red de datos de la Conselleria.

En la situación actual, la seguridad de las infraestructuras y sistemas de la Conselleria y de la información puesta bajo su responsabilidad dependen más que nunca de que el personal haga un uso responsable de los instrumentos y medios a su disposición, aunque fueran de su propiedad, para realizar actuaciones en nombre de la Conselleria. Ante cualquier duda sobre esta cuestión, puede dirigirse a CATS o al servicio técnico de asistencia del centro, desde donde trasladarán la pregunta al órgano competente si fuera necesario.

Además de insistir en la llamada a la responsabilidad, conviene recordar que los sistemas críticos o los que manejan información sensible, como son los datos sanitarios, tienen activada la trazabilidad de las actuaciones. La Conselleria tiene el deber de revisar estos registros e investigar los posibles incidentes. Las negligencias e incumplimientos podrán tener consecuencias disciplinarias, incluso cuando no llegasen a ocasionar un incidente.

# ANEXO 1. Instalación del agente Cytomic Endpoint Agent

Los siguientes enlaces le permitirán descargar el instalador en su equipo. Una vez descargado tendrá que ejecutarlo (doble click) para proceder a su instalación. A partir de ese momento el programa estará activo y arrancará automáticamente cada vez que encienda el equipo. Para elegir el instalador adecuado dispone de varias opciones:

Si tiene usuario y cuenta del dominio CS (los que usa para identificarse cuando enciende un equipo de la Conselleria)

1. En equipos con Windows:
   https://transit.san.gva.es/owncloud/index.php/s/Ta0HIAV8V2wsLTh
2. En equipos con MacOS:
   https://transit.san.gva.es/owncloud/index.php/s/9XB2EnGMpGya82f
3. En equipos con Linux:
   https://transit.san.gva.es/owncloud/index.php/s/UdVYCqR0zxcueeY

En caso contrario, o si hubiera tenido alguna dificultadecon el anterior:

1. En equipos con Windows:
   https://manage.cytomicmodel.com/api/v1/accounts/8dcd781b-068e-4c3f-b6b0-9246dc69e613/sites/a3c25366-c340-41d4-9805-4e8d8075fc63/installers?installerType=2&platform=1&managedConfigurationId=106815ce-6fb6-4efa-9b09-e2cb309f7444&customGroupId=5a00c15a-2dd8-42cb-9abe-89e812cb8b05&integrationGroupType=0
2. En equipos con MacOS:
   https://manage.cytomicmodel.com/api/v1/accounts/8dcd781b-068e-4c3f-b6b0-9246dc69e613/sites/a3c25366-c340-41d4-9805-4e8d8075fc63/installers?installerType=2&platform=3&managedConfigurationId=106815ce-6fb6-4efa-9b09-e2cb309f7444&customGroupId=9fe2917e-346b-4a14-a827-eca2446cf5d5&integrationGroupType=0
3. En equipos con Linux:
   https://manage.cytomicmodel.com/api/v1/accounts/8dcd781b-068e-4c3f-b6b0-9246dc69e613/sites/a3c25366-c340-41d4-9805-4e8d8075fc63/installers?installerType=2&platform=2&managedConfigurationId=106815ce-6fb6-4efa-9b09-e2cb309f7444&customGroupId=9fe2917e-346b-4a14-a827-eca2446cf5d5&integrationGroupType=0

# ANEXO 2. Autorización para el uso de dispositivos personales

D/Dª …….
Con DNI ……..
Que desempeña funciones de….
En el centro...

Dadas las especiales circunstancias creadas por la crisis del COVID-19
Solicita poder acceder con medios propios desde su domicilio a (indicar los sistemas o aplicaciones que corresponda):……..
Con objeto de (indicar el motivo)...

Para lo que declara haber leído, aceptar y comprometerse a cumplir las condiciones establecidas en este documento "Condiciones para el uso de equipos domésticos durante la situación de emergencia generada por COVID-19" y, en la parte que corresponda, de las que figuran en las licencias de uso de los productos instalados[5]. Entre tales condiciones destacan las siguientes:

1. Hacer un uso responsable de los medios y privilegios que derivan de la aceptación de esta solicitud.
2. Crear cuentas de usuario separadas que impidan el acceso a la información o sistemas de la Conselleria por parte de otros posibles usuarios del equipo.
3. Descargar de los sistemas de la Conselleria sólo la información estrictamente imprescindible para el desempeño de sus funciones en estas circunstancias excepcionales.
4. Eliminar dicha información del equipo una vez haya dejado de ser necesaria.
5. No guardar copias de la información en otros dispositivos, ni en ningún espacio de almacenamiento en la nube (Drive, OneDrive, iCloud, Dropbox, etc.), ni a transferirla a terceros por ningún medio (Whatsapp, Messenger…)
6. No ejecutar en el equipo programas de compartición de ficheros (P2P) mientras tenga instalado el software para el acceso por VPN a la red de datos de la Conselleria.
7. Permitir la instalación del software necesario para hacer efectivo el acceso a la red de datos y a los sistemas de la Conselleria, y a no desactivarlos o desinstalarlos por su cuenta, sino siguiendo los procedimientos establecidos para ello.
8. Comunicar cualquier incidente que pudiera comprometer la seguridad de la información o de los sistemas bajo responsabilidad de la Conselleria.

| | |
|---|---|
| El/la solicitante,<br>D/Dª | VºBº de su responsable<br>D/Dª |

La persona responsable del órgano donde trabaja la solicitante (indicar órgano y puesto) declara que ésta desempeña funciones relevantes para la prestación de servicios públicos esenciales y que dichas funciones no puede llevarlas a cabo en las circunstancias actuales desde su puesto de trabajo habitual con las suficientes garantías para su seguridad personal y la continuidad de los servicios, así como que el órgano no dispone en este momento de medios técnicos suficientes (ordenador portátil) para facilitar el acceso remoto a la persona solicitante.

5 https://manage.cytomicmodel.com/Resources/Views/Eula/ad_es-ES_cytomic.html

# ANEXO 3. Información relativa al tratamiento de datos personales cuya finalidad es la aplicación de controles de seguridad durante la prestación de servicios en régimen de teletrabajo por parte del personal de la Conselleria con medios privados y con motivo de la crisis del COVID-19

De conformidad con la normativa de protección de datos, se informa al personal de la Conselleria que desempeñe servicios en régimen de teletrabajo utilizando medios propios con motivo de la situación creada por COVID-19, de que los datos de contacto que facilite, así como los relativos a sus equipos personales que recaben las herramientas de uso obligatorio para la prestación de servicios en régimen de teletrabajo serán objeto de tratamiento de conformidad con las siguientes condiciones:

a) Tiene la condición de responsable del tratamiento la Consellería de Sanidad Universal y Salud Pública (C/ Micer Mascó, 31, 33, 46010 Valencia, Valencia).

b) La finalidad para el tratamiento de datos personales es garantizar la seguridad de los sistemas de información de la Consellería de conformidad con lo dispuesto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Las bases de legitimación general son las siguientes:

- Art. 6.1 c) RGPD: Obligación legal de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Art. 6.1 e) RGPD: Interés público para la gestión de la seguridad de la información de la Consellería y mantenimiento de servicios públicos esenciales.

c) Los datos personales no serán comunicados a terceros.

d) Los datos se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos y de conformidad con normativa de archivos y documentación.

e) La persona interesada puede ejercer sus derechos de acceso, rectificación, supresión, la limitación de su tratamiento, oposición, portabilidad y no ser sometido a una decisión basada exclusivamente en el tratamiento de los datos personales a mediante escrito dirigido a la Consellería de Sanidad Universal y Salud Pública.

f) La persona interesada tiene derecho a contactar o reclamar ante el Delegado de Protección de Datos mediante el envío de un correo electrónico a la dirección dpd@gva.es.

g) Así mismo, en el caso de que entienda vulnerado su derecho a la protección de datos, la persona interesada tiene derecho a reclamar ante la Agencia Española de Protección de Datos (www.aepd.es).