Anexo I - Dominio de Comunicaciones

Norma de seguridad para la conexión de dispositivos a las redes de comunicaciones.

1. Principios generales.

La conexión de un equipo de usuario a una toma de la red de datos, o bien una reubicación que implique el cambio de conexión de una toma de red a otra diferente, deberá ser solicitada al personal TIC correspondiente, quien se encargará de realizar o de que se realicen los trabajos oportunos.

El Área de Comunicaciones y Seguridad de la Secretaría General Adjunta de Informática (SGAI) en el ámbito de la Organización Central (ORGC), o el personal TIC encargado de las comunicaciones y de la seguridad en los Institutos Centros y Unidades (ICU), serán quienes determinen la conveniencia de efectuar dicha conexión, tras un análisis de seguridad previo efectuado para verificar que se cumplen los mínimos adecuados de protección, las condiciones que permitan realizar dicha conexión, y se determinen las redes virtuales (VLAN) a las que podrá tener acceso en función del perfil y necesidades del usuario. Igualmente será el personal de dichas unidades quien deberá efectuar, si procede y con carácter previo, las distintas labores de parcheo, configuración y habilitación de puertos en los distintos equipos que componen la electrónica de red del edificio.

En el ámbito de la ORGC no podrán conectarse, sin previo aviso, equipos de usuario a tomas de red. Igualmente, tampoco se podrá conectar a la red de comunicaciones corporativa un dispositivo distinto de los admitidos, habilitados y configurados por los servicios TIC responsables, salvo autorización previa y expresa del Área de Comunicaciones y Seguridad de la SGAI y previo análisis de seguridad efectuado al equipo para verificar que no contiene elementos software potencialmente dañinos para la red corporativa, ni para otros recursos del CSIC. Todo ello sin perjuicio de lo indicado más adelante respecto al uso y conexión de dispositivos ajenos a la titularidad o propiedad del CSIC, y muy especialmente en lo referente al "Bring Your Own Device" o "BYOD", práctica cada vez más extendida que hace referencia al empleo por parte del usuario de un equipo propio para utilizarlo en el trabajo y conectarlo a la red corporativa.

En los equipos de usuario no podrán instalarse o conectarse dispositivos de comunicaciones que permitan una conexión a redes externas, distintos de los que habilitan la conexión, cableada o inalámbrica, a la red corporativa del CSIC y a través de la cual se realiza la conexión a Internet con las adecuadas medidas de seguridad. En caso de requerirse tal acceso deberá solicitarse tal autorización al Área de Comunicaciones y Seguridad de la SGAI en el caso de la ORGC, o al responsable TIC correspondiente en el caso de ICU, indicando las causas que justifican dicha necesidad, debiendo contar con la autorización previa y expresa para ello.

Lo anterior implica que no podrá utilizarse un dispositivo móvil (teléfono móvil, tablet o dispositivo equivalente) conectado a Internet a través de redes de operadores móviles, configurado en modo *"hotspot"* (punto de acceso inalámbrico, o incluso cableado) para dar cobertura de internet al entorno y al cual pueda tratar de conectarse el equipo de usuario para disponer de conexión a Internet sin pasar por los recursos corporativos del CSIC que controlan y aseguran dicha conexión.

2. Conexión de dispositivos ajenos a la titularidad o propiedad del CSIC.

Resulta cada vez más frecuente la utilización de dispositivos personales, o al menos ajenos al CSIC, como equipos habituales de trabajo (PCs de sobremesa u ordenadores portátiles), que lógicamente requieren ser conectados a la red corporativa, ya sea a través de una toma de red o mediante una conexión a la red inalámbrica que pueda haber disponible.

Esta práctica, comúnmente conocida como "BYOD", debe por tanto ser regulada convenientemente.

En el ámbito de la ORGC, dado que por lo general se requiere habilitar en la electrónica de red la toma de datos a la que vaya a conectarse el equipo por medios cableados, deberá solicitarse autorización para la conexión de un "equipo BYOD". De la misma manera que con los equipos propios del CSIC, se deberá efectuar al equipo un análisis de seguridad previo a su conexión final a la red en las condiciones habituales, en paralelo a las tareas de configuración requeridas en la electrónica de red para posibilitar tal conexión.

Por su parte, los "equipos BYOD" en los ICU deberán ser conectados a una VLAN diferenciada con acceso exclusivamente a los recursos que en cada caso se determinen como adecuados, tomando como criterio principal la seguridad global de la red y de todos los demás elementos conectados a ésta.

En el supuesto de conexiones por medios inalámbricos de ordenadores portátiles, tabletas, smartphones o cualquier otro dispositivo, no se requiere, por lo general, la intervención de una unidad TIC para configurar en los dispositivos la conexión a la red corporativa, recayendo esta acción en el propio usuario, se elimina el requisito de efectuar un control y análisis previo del equipo, salvo situaciones que exijan lo contrario.

En el marco de sus actividades habituales de control del estado y de la seguridad de la red, el Área de Comunicaciones y Seguridad podrá monitorizar (sin acceso al contenido) los flujos de datos internos de la red, así como las conexiones efectuadas con el exterior para detectar posibles comportamientos anómalos y, en su caso, identificar los equipos que pudieran haberlos ocasionado. En el supuesto de identificar que alguno de dichos equipos se corresponde con un dispositivo "BYOD", se darán las instrucciones y pautas a seguir para evitar tal comportamiento, debiendo su usuario o propietario adoptar las medidas que se señalen. Si la situación persiste sin ser solventada, se podrá restringir el acceso del equipo a los recursos de la red corporativa.

3. Acceso remoto a la red corporativa.

No se podrá efectuar la conexión desde equipos ajenos a la red corporativa a equipos internos, salvo mediante mecanismos de Red Privada Virtual (VPN) convenientemente implantados por los servicios TIC de cada ICU, o por el Área de Comunicaciones y Seguridad de la SGAI, según el caso.

Para poder disponer de dichos accesos mediante VPN se presentará una solicitud motivada al Área de Comunicaciones y Seguridad de la SGAI, o al responsable TIC del ICU, que incluirá además de la correspondiente autorización de la persona responsable del solicitante, una justificación razonada de la necesidad e indicación de los recursos de la red interna corporativa a los que se precisa acceder desde el equipo externo y la duración estimada de la necesidad.

Cuando se efectúen las configuraciones que habiliten dicha conexión, se dará permiso de acceso exclusivamente a los recursos solicitados y adecuadamente justificados.

4. Utilización de dispositivos móviles.

En el ámbito de la presente normativa, se entenderá por dispositivo móvil cualquier elemento electrónico no fijo con capacidad de registrar, almacenar y/o transmitir datos, voz, video o imágenes, como los teléfonos móviles (smartphones, fundamentalmente) y las tabletas y, en determinadas circunstancias, los ordenadores portátiles, aunque por lo general estos últimos serán considerados como equipos de trabajo del usuario.

Por norma general, aunque no en exclusiva, los teléfonos móviles y las tabletas operan bajo los sistemas operativos Android (Google), iOS (Apple) y Windows Phone (Microsoft). Estos, en las diferentes versiones que vayan pudiendo ser liberadas en el futuro y siempre que mantengan, como en la actualidad, una cuota representativa en el mercado de dispositivos móviles, serán los sistemas operativos sobre los que se podrá asegurar un nivel mínimo de compatibilidad para el uso e instalación en ellos de determinadas aplicaciones y acceso a ciertos recursos corporativos.

No estará garantizada la compatibilidad de dispositivos que funcionen bajo otro tipo de plataformas, pudiendo con causa justificada llegar el caso de no permitir su utilización en la conexión a la red corporativa.

En el supuesto de que el personal del CSIC utilice móviles propios y, por tanto, externos al CSIC para acceder a las redes y recursos de la institución, deberán seguir asimismo la normativa de seguridad y las instrucciones que el personal TIC de su unidad facilite para efectuar dicha conexión. Dichas instrucciones podrán diferir en función de las características y condiciones específicas de cada terminal (modelo, versión del sistema operativo empleado, tipo de acceso o conexión que se solicita, etc.).

5. Conectividad y acceso a información.

Los dispositivos móviles suelen incorporar por sí mismos capacidad de conexión a redes externas (entre ellas internet), bien mediante conexiones propias a las redes de datos de los operadores móviles o bien mediante conexiones a redes o puntos de acceso Wifi, las cuales a su vez proporcionan la conexión con las redes externas.

Como se ha señalado previamente, la capacidad de conectividad deberá estar limitada a la conexión del propio dispositivo hacia redes externas (internet, u otras ajenas a la red privada corporativa del CSIC). **Cuando el dispositivo esté conectado a la red corporativa no podrá utilizarse en modo *hotspot*, de forma que actúe como punto de acceso a Internet al cual puedan conectarse otros dispositivos. No podrá aprovecharse la conexión a través del dispositivo móvil en modo *hotspot* para conectar equipos corporativos (PCs, portátiles, etc.) que habitualmente han de estar conectados por cable de red o bien mediante conexión a través de la red Wifi corporativa (SSID: *eduroam*).** Estas medidas tratan de evitar que los equipos accedan a Internet y otras redes sin los dos métodos indicados, y consiguientemente sin el paso por los distintos dispositivos y mecanismos de seguridad que forman parte de la infraestructura corporativa de comunicaciones y seguridad.

En caso de necesidad, se podrá almacenar en el dispositivo móvil corporativo aquella información de carácter personal estrictamente indispensable para el desarrollo de las funciones profesionales, procediendo a su borrado cuando ya no sea necesario su tratamiento.

En el caso de uso y conexión de un dispositivo móvil personal a la red corporativa no podrá descargarse, copiarse o almacenarse en el mismo información sensible o confidencial del CSIC a la que se haya tenido acceso desde el dispositivo, para evitar una posible salida incontrolada de dicha información una vez que el dispositivo se encuentre fuera de la red corporativa y de los controles y equipamiento de seguridad proporcionados por la misma.