Recomendaciones para teletrabajo seguro

1) Teletrabajo seguro

Estos días complicados, los expertos en sanidad nos están informando de que una de las medidas más eficaces para frenar las epidemias provocadas por virus es la responsabilidad particular de cada persona y determinado comportamiento social. De la misma forma, nuestra manera de utilizar la tecnología puede prevenir problemas de seguridad y contribuir a que los sistemas de la UPCT sean más seguros y resistentes a ataques informáticos.

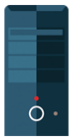
En estos días en que el teletrabajo se ha generalizado en todos los ámbitos de la actividad universitaria, os queremos indicar unas recomendaciones que serán de gran ayuda para todos.

Más allá de ser recomendables, algunas de estas medidas deben cumplirse necesariamente. En la red de la UPCT y en los equipos conectados a la misma se aplican las medidas de seguridad que se determinan para todas las Administraciones Públicas españolas en el Esquema Nacional de Seguridad: cortafuegos en la cabecera de red; filtrado de tráfico malicioso; antivirus corporativo; política de actualización de sistemas operativos; división en subredes con distintos niveles de seguridad; copias de seguridad; medidas para protección de la información; control de accesos; etc. Al habilitar el acceso remoto desde un equipo o red doméstica, muchas de estas medidas no podrían aplicarse por lo que, si alguien entrara en vuestro equipo de casa mientras estéis conectados en remoto a la UPCT, se saltaría gran parte de las defensas que tenemos configuradas en nuestros sistemas.

Por esto, sólo se permite el acceso remoto a vuestros equipos de trabajo a través de la VPN (sobre el uso de la VPN). Pero esto solo no es suficiente, debemos reforzarlo con las siguientes buenas prácticas.

2) Sobre la seguridad del equipo desde el que se accede

Para hacer frente a situaciones como la que vivimos actualmente, se va a recomendar a todo el personal de la universidad que trabajen desde sus domicilios, utilizando equipos de uso particular si fuera necesario. Estos equipos no dispondrán de las medidas de seguridad y de las opciones de configuración que se implantan en los equipos de trabajo del personal de la UPCT; pero para garantizar unas mínimas condiciones de seguridad de acceso a los recursos e información de la Universidad, es muy importante tener en cuenta en las siguientes medidas:

 Sistema operativo con soporte y parches de seguridad actualizados	Mínimo
 Tener instalado y actualizado un AntiVirus	Mínimo
 Únicamente se podrá administrar el sistema desde un usuario administrador	Mínimo
 Si el equipo es de uso compartido, utilizar una Cuenta diferenciada para realizar el teletrabajo	Mínimo
 El equipo se bloqueará al cabo de un tiempo prudencial de inactividad	Mínimo
 Cortafuegos personal habilitado	Avanzado

3) Sobre la seguridad en la red doméstica

Normalmente en nuestro domicilio dispondremos de una red inalámbrica (wifi) que dará acceso a Internet a nuestros dispositivos. Esta red wifi está controlada por un equipo denominado “router”, que es el que hace de frontera entre nuestra red doméstica y el proveedor de acceso a Internet. La seguridad de nuestra wifi doméstica es un elemento clave para la protección de nuestra conexión. Aquí damos algunas recomendaciones para hacer nuestra wifi doméstica más segura (los detalles deberán consultarse en el manual específico que nos proporcione nuestro proveedor):

	Activar la conexión segura (WPA2) que garantiza un nivel de cifrado de la información suficientemente fuerte y dar sólo la contraseña de acceso a personas de confianza	Básico
	Usar un identificador de red (SSID) que no revele ninguna información personal	Básico
	Utilizar contraseñas fuertes tanto para configurar el acceso a la red como para la administración del router	Recomendado
	Apagar el router cuando no se va a usar (por ejemplo, por la noche).	Recomendado
	Cambiar la contraseña por defecto del usuario administrador del router	Recomendado
	Tener el router debidamente actualizado (firmware y software)	Recomendado
	Deshabilitar servicios innecesarios que pudieran estar habilitados en el router; p.ej. gestión remota	Avanzado

Establecer en el router filtrado por la dirección MAC (media access control) de los equipos a los se les permita el acceso	Avanzado

4) Sobre el tratamiento seguro de la información

Durante el tiempo que estemos teletrabajando será necesario acceder a información confidencial o a datos de carácter personal y hacer un tratamiento de los mismos. Es necesario, por tanto, tener en cuenta algunas consideraciones y recomendaciones:

- En la mayoría de los casos, el acceso a las aplicaciones de gestión y a la información que tratan será siempre desde el puesto de trabajo en la red de la universidad, al que se accede vía conexión remota (VPN). Más información en https://online.upct.es/themes/online/assets/documents/que_tengo_que_hacer_para_conectarme_desde_casa_al_ordenador_del_trabajo_v3.pdf
- Si se está trabajando con documentos internos, aparte de ser fundamental cumplir con los requisitos básicos enumerados en el punto 2, se debe considerar lo siguiente:
  - Si la confidencialidad de la información a tratar es alta o se trata de datos personales dentro de una categoría especial, el tratamiento se debe realizar desde el puesto de trabajo en la red de la universidad, al que se accede vía conexión remota (VPN).
  - En otros casos, puede ser más ágil descargarlo y trabajar en el equipo local. En este caso, **SIEMPRE se debe volver a subir la versión actualizada a la carpeta en red de nuestra unidad y borrar de forma segura en el equipo doméstico la copia del fichero correspondiente.**
  - Se usarán herramientas para borrado seguro (por ejemplo FileShredder https://www.fileshredder.org/).

  - Usar herramientas para el almacenamiento cifrado de la información confidencial (Bitlocker de Microsoft, aunque es más recomendable VeraCrypt https://www.veracrypt.fr/en/Home.html).
  - También es posible crear un espacio de almacenamiento en UPCTCloud y compartirlo temporalmente con compañeros del trabajo que necesiten acceder al mismo. Se debe eliminar el documento una vez subido a la carpeta de la Unidad/Departamento.
  - En caso de duda, consultar al superior jerárquico.

- Para el envío de correos a otros compañeros utilizar siempre la plataforma de correo de la Universidad. Si se requiere un mayor nivel de confidencialidad de la información que se va a enviar por correo, se puede cifrar el correo mediante PGP (https://www.openpgp.org/software/) o S/MIME (https://support.office.com/es-es/article/Cifrar-mensajes-mediante-S-MIME-en-Outlook-Web-App-2E57E4BD-4CC2-4531-9A39-426E7C873E26)
- En general, para la comunicación y colaboración con otros compañeros de la universidad se deben utilizar las herramientas disponibles en UPCTCloud (Teams, OneDrive, Forms, etc.)

5) Generales

- Cuidado con los bulos: contrastad las noticias que recibáis y no contribuyáis a su difusión.
- Estad especialmente atentos a los mensajes falsos y phishing, sobre todo con temáticas relacionadas con el COVID-19.
- No os conectéis NUNCA desde redes wifi abiertas a los sistemas de la Universidad o a sitios donde manejéis información privada o confidencial.
- Os insistimos que debéis utilizar contraseñas fuertes en vuestro entorno doméstico, de la misma forma que si estuvierais en vuestro puesto de trabajo de la universidad; posibilidad de usar gestores de contraseñas (https://keepass.info/ , https://www.lastpass.com/es).

- Impedid y/o controlad el acceso al equipo desde que el realizáis el teletrabajo a otros miembros de la familia, especialmente a los niños; pueden, de forma accidental, borrar o modificar información e, incluso, infectar el equipo.
- En general, seguid siempre los consejos de seguridad de organismos como INCIBE (https://www.incibe.es y https://www.osi.es/es) y CCN-CERT (https://www.ccn-cert.cni.es)