Criterios específicos de seguridad TIC y protección de datos personales en el teletrabajo

La persona teletrabajadora debe garantizar la confidencialidad y la seguridad de los datos y de la información que utilice y a los que pueda acceder, y evitar por todos los medios posibles su alteración, pérdida, tratamiento, acceso no autorizado o uso inadecuado.

La persona teletrabajadora debe cumplir con la política de seguridad de la información de la UPC y el Manual UPC de protección de datos.

En cuanto a **seguridad informática y teletrabajo**, hay que seguir las indicaciones establecidas, que se pueden encontrar en este enlace: https://serveistic.upc.edu/ca/eines-teletreball/documentacio/guia-teletreball#section-0.

En cuanto a **protección de datos personales y teletrabajo**, hay que ajustarse a las siguientes indicaciones adicionales a las establecidas en el Manual UPC de protección de datos:

- El tratamiento de datos personales debe realizarse mediante los sistemas y servicios que la Universidad pone a disposición de las personas teletrabajadoras: https://serveistic.upc.edu/ca/treballa-en-remot/profesorado. Los datos personales no deben tratarse en servicios en la nube con los que la UPC no tenga un contrato establecido, puesto que se pierde la trazabilidad de dichos datos, no existen garantías de cómo se tratarán y se ponen en peligro.

- No se pueden compartir documentos con datos de carácter personal con las herramientas de teletrabajo (p. ej., Drive de G Suite) con usuarios de fuera del dominio upc.edu sin una autorización expresa.

- No se deben utilizar direcciones de correo electrónico que no sean de la UPC para enviar datos personales.

- En caso de utilizar direcciones de correo electrónico genéricas de la UPC, para enviar datos personales, es necesario que el correo electrónico indique la identidad de la persona que lo envía.

- Todas las personas teletrabajadoras son responsables de su sitio de teletrabajo y, por lo tanto, deben adoptar las medidas necesarias para impedir el acceso de personas no autorizadas a la información confidencial. La persona teletrabajadora debe mantener por un tiempo indefinido la máxima reserva sobre dicha información y no podrá divulgar ni utilizar datos, documentos, metodologías, claves, análisis, programas, estudios u otras informaciones pertenecientes a la UPC, tanto en soporte papel como electrónico, ni directamente ni mediante terceras personas o entidades. No se debe permitir el

acceso a los datos personales o a información confidencial a personas no autorizadas, por lo que hay que evitar que se encuentren al alcance de otras personas.

- La persona teletrabajadora dispone de una contraseña personal e intransferible para acceder a los archivos que contengan datos de carácter personal. Dicha contraseña tiene carácter confidencial, por lo que:

    - No está permitido revelarla a nadie sin la autorización expresa del jefe o jefa.
    - Se recomienda memorizarla y no anotarla en ninguna parte.
    - En el caso de que sea conocida por personas no autorizadas, habrá que cambiarla.
    - En el caso de que la persona no recuerde la contraseña, deberá ponerse en contacto con los servicios informáticos de la Universidad. (Es importante no almacenar las contraseñas en el navegador).

- El usuario debe utilizar los datos personales a los que tenga acceso única y exclusivamente para los fines previstos correspondientes al puesto de trabajo y no mezclarlos con datos o archivos privados.

- Hay que eliminar la información temporal de las carpetas de descargas y la papelera de reciclaje u otras carpetas similares que pueda haber en directorios del ordenador (p. ex., en Mis documentos) en el caso de que excepcionalmente se haya descargado documentación en local.

- Hay que cerrar las conexiones a los servidores y sitios web o intranets con la opción Desconectar o Cerrar sesión.

- Cuando la persona se ausente de su puesto de teletrabajo, deberá impedir el acceso de otras personas no autorizadas a documentos en pantalla y en papel que contengan datos de carácter personal. En cuanto a los equipos informáticos, puede impedirse su visualización mediante protectores de pantalla. En cuanto a la documentación en papel, debe almacenarse en un lugar seguro mientras no se utilice.

- No se debe destruir fuera de la Universidad la información en papel con datos personales o confidenciales. Es muy importante que no se tire en contenedores de reciclaje y que no se reutilice como papel reciclado en casa. La documentación con datos personales y confidenciales debe destruirse de acuerdo con las indicaciones del Archivo UPC.

El personal notificará cualquier incidente de seguridad informática o de protección de datos personales al servicio de atención al usuario ATIC -- atic@upc.edu -- y seguirá sus instrucciones, entre las que se podrían contemplar el bloqueo o desconexión de la red del dispositivo.

Versión 24 de marzo de 2021