Comunidad de Madrid

INFORMACIÓN Y COMPROMISO EN PROTECCIÓN DE DATOS PERSONALES

De conformidad con lo previsto en el artículo 18 del Decreto 79/2020, de 16 de septiembre, del Consejo de Gobierno, por el que se regula la modalidad de prestación de servicios en régimen de teletrabajo en la Administración de la Comunidad de Madrid,

SE INFORMA al empleado público que:

En el desarrollo de sus funciones en régimen de teletrabajo, **deberá cumplir en todo momento con las obligaciones** previstas en el Reglamento (UE) 2016/679, de Protección de Datos Personales (en adelante, RGPD), en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDPGDD) y en el resto de **normativa vigente sobre protección de datos de carácter personal, tanto respecto de la información en papel como respecto de la información en formato electrónico**.

En concreto, el empleado público, en el desarrollo del teletrabajo:

Está sujeto al deber de confidencialidad al que se refiere el art. 5 de la LOPDPGDD y el art. 5.1.f) del RGPD. La obligación del deber de confidencialidad será complementaria de la del deber de secreto profesional recogido en el Estatuto Básico del Empleado Público (art. 53.12).

Debe velar por la integridad y confidencialidad de los datos personales utilizados. Para ello, debe tratarlos de manera que se garantice una seguridad adecuada, a fin de evitar el acceso no autorizado o ilícito y la pérdida, destrucción o daño accidental de los datos personales (artículo 5.1.f) del RGPD.

Respecto del uso de ordenadores en teletrabajo: Ha de conocer y aplicar la guía de la Agencia para la Administración Digital de la Comunidad de Madrid "*Recomendaciones de seguridad de la información para el trabajo en remoto*", (con pautas a seguir al utilizar ordenadores, para mantener segura la información de los ciudadanos y los servicios de la Comunidad), disponible a través de la intranet, en el portal CAU/Teletrabajo/Seguridad, además de otras guías relacionadas que elabore la Agencia para la Administración Digital de la Comunidad de Madrid. Asimismo, la conexión con los sistemas informáticos de la Administración autonómica deberá llevarse a cabo conforme a las recomendaciones de seguridad establecidas por Madrid Digital para garantizar la accesibilidad, agilidad, seguridad y confidencialidad de la comunicación y de los sistemas de información.

Respecto de la salida temporal de documentos de las unidades administrativas, (ya sea en papel o en formato digital), el empleado deberá elaborar una relación de las mismas lo más exhaustiva posible, para permitir llevar un control sobre la documentación. Dicha relación deberá ser aprobada por el responsable o quien se determine, cumplimentando

la solicitud prevista al efecto según las indicaciones dadas por la Subdirección General de Archivos y Gestión Documental que, en su caso, le faciliten en su Centro Directivo.

Se detallan, a continuación, las directrices a seguir en teletrabajo:

1. **Proteger el dispositivo utilizado en teletrabajo y el acceso al mismo**, cumpliendo las mismas medidas de seguridad que la Comunidad de Madrid impone para el trabajo presencial. En particular, el empleado público:

- Debe definir y utilizar contraseñas de acceso robustas y diferentes a las utilizadas para acceder a otros ámbitos de internet y debe garantizarse el secreto de las contraseñas.
- Debe evitar almacenar las claves de acceso a los sistemas en los navegadores del equipo (no habilitando las opciones de recordar claves), introduciendo la contraseña cada vez que se vaya a conectar a los sistemas.
- No debe descargar ni instalar aplicaciones o software que no hayan sido previamente autorizados por la organización.
- Debe evitar la conexión de los dispositivos a la red corporativa desde lugares públicos, así como la conexión a redes WIFI abiertas no seguras.
- Debe proteger los mecanismos de autenticación definidos (certificados, contraseñas, sistemas de doble factor,…) para validarse ante los sistemas de control de acceso remoto de la organización.
- Debe utilizar el ordenador corporativo exclusivamente para uso profesional.
- En el supuesto de que se permita o sea necesario utilizar dispositivos propios del empleado (no corporativos), debe:
  - evitar simultanear la actividad personal con la profesional y definir perfiles independientes para desarrollar cada tipo de tarea.
  - verificar que el software antivirus y el firewall están actualizados y que el equipo se encuentra protegido.
  - comunicar robos, pérdidas de información u otras incidencias de la misma manera que si se tratase de dispositivos de la Comunidad de Madrid.
- Debe desconfiar de los correos sospechosos o no conocidos, borrándolos y no descargando su información adjunta, ya sean ficheros con extensiones inusuales o enlaces con un patrón fuera de lo normal.
- Debe desactivar las conexiones WIFI, bluetooth y similares que no estén siendo utilizadas, si pueden ser gestionadas por el empleado.
- Debe desconectar la sesión de acceso remoto y apagar o bloquear el acceso al dispositivo, una vez concluida la jornada de trabajo en situación de movilidad.

Comunidad de Madrid

- Debe garantizar un uso y custodia con la debida diligencia de los dispositivos que facilite la Comunidad de Madrid, para evitar averías, daños, pérdidas o sustracciones y no utilizarlos para finalidades diferentes a las derivadas de la prestación de servicios que ha justificado su entrega. Igual diligencia se exige respecto de las herramientas ofimáticas y del acceso a las aplicaciones informáticas que se le faciliten.

2. **Garantizar la confidencialidad de la información que se está manejando**. El empleado público:

- Debe minimizar la salida de **documentación en papel** de la unidad administrativa, aplicando en su caso los protocolos previstos por la Subdirección General de Archivos y Gestión Documental, y extremar las precauciones para evitar accesos no autorizados por parte de terceros u otras brechas de seguridad en su custodia, evitando trasladar la documentación a sitio diferente de su oficina o lugar de teletrabajo, especialmente si se trata de documentos originales. Cuando se tenga que destruir documentación, debe hacerlo de manera segura, que impida futuros accesos por terceros no autorizados.
- Debe extremar las precauciones para evitar el acceso no autorizado a la información personal, propia y de terceros, manejada, no dejando a la vista ningún soporte de información en el lugar donde se desarrolle el teletrabajo, evitando exponer la pantalla a la mirada de terceros y bloqueando las sesiones de los dispositivos cuando estos estén desatendidos.
- Debe cifrar con contraseñas robustas los dispositivos externos de almacenamiento de información, si los utiliza.
- Debe evitar conversaciones laborales accesibles por parte de terceros ajenos utilizando, por ejemplo, auriculares o retirándose a un espacio en el que el empleado público no esté acompañado.
- Debe evitar el envío de correos electrónicos con información confidencial o con documentos que contengan datos personales. Si es imprescindible hacerlo, debe utilizar exclusivamente el correo corporativo y no debe poner datos personales en el asunto; la documentación no irá en el cuerpo del correo, sino en un documento adjunto y con acceso cifrado.
- No debe utilizar plataformas no autorizadas por la Comunidad de Madrid y/o gratuitas de transmisión de archivos informáticos por internet (por ejemplo, *"We Transfer"*, *"WhatsApp"*), para enviar información confidencial o que contenga datos personales, dentro o fuera de la organización.
- No debe usar convertidores gratuitos sobre documentos que contengan información confidencial o datos personales (convertidores de pdf a Word, etc.).

- Utilizar los prefijos de número oculto en caso de tener que realizar puntualmente alguna llamada de trabajo desde un teléfono no corporativo (#31# en el caso de teléfono móvil o el prefijo 067 desde un teléfono fijo). Para mayor seguridad, se debe confirmar esta información con el operador de telefonía que corresponda en cada caso y tener en cuenta que hay teléfonos que rechazan las llamadas "desconocidas".
- En las videoconferencias deben:
  - Evitar establecer comunicaciones con desconocidos o que no estén dentro de la lista de contactos.
  - Añadir únicamente a contactos conocidos y de confianza. Verificar la identidad de los nuevos contactos por los medios precisos, sobre todo cuando vamos a iniciar una videoconferencia por primera vez con ellos.
  - Utilizar perfiles de usuario con autenticación mediante contraseña segura, para evitar el acceso por usuarios no autorizados.
  - Deshabilitar las funciones de cámara y compartir escritorio por defecto. Habilitar solo cuando sea necesario.
  - Cubrir la cámara cuando el sistema no está en uso y configurarla para que, al comenzar una videoconferencia, presente una imagen neutra, que no muestre información comprometida en caso de establecer una conexión errónea.
  - Apagar o silenciar los micrófonos cuando el sistema no esté en uso.

3. Guardar la información en los espacios de red habilitados.

- Debe evitar almacenar la información generada durante la situación de movilidad de forma local en el dispositivo utilizado, usando al efecto los recursos de almacenamiento compartido o en la nube proporcionados por la organización.
- No debe bloquear o deshabilitar la política de copia de seguridad corporativa definida para cada dispositivo.
- Si se permite la utilización de **equipos personales**:
  - ➢ No debe utilizar bajo ningún concepto aplicaciones no autorizadas en la política de la entidad para almacenar o compartir información (servicios en nube de alojamiento de archivos, correos personales, mensajería rápida, etc.)
  - ➢ Debe cerrar siempre la sesión y eliminar la información residual que pueda quedar almacenada en el dispositivo, como archivos temporales del navegador o descargas de documentos.
  - ➢ No debe dejar guardada información de forma local en el dispositivo personal al objeto de evitar accesos no autorizados.

Comunidad de Madrid

4. **Si hay sospecha de que la información ha podido verse comprometida, comunicar con carácter inmediato la brecha de seguridad al responsable.**

- Debe comunicarlo con carácter inmediato a su responsable y/o al Jefe de Área de Madrid Digital de su consejería, que informarán al Delegado de Protección de Datos de la consejería y evaluarán conjuntamente el incidente, determinando si hay que comunicarlo a la Agencia Española de Protección de Datos (AEPD) en caso de que el mismo cumpla con los supuestos de notificación exigidos por la normativa vigente en materia de seguridad de la información y protección de datos personales.
- Si se suscita cualquier cuestión en el contexto de las situaciones de movilidad que pueda representar un riesgo para los datos personales contenidos en los dispositivos, recursos o herramientas corporativos (portátiles, teléfonos, tablets, carpetas compartidas, aplicativos, etc.) respecto de la protección de la información deben comunicarlo, a la mayor brevedad, a la Agencia para la Administración Digital de la Comunidad de Madrid mediante cualquiera de las siguientes vías:

  Teléfono: 91 580 04 04

  Correo electrónico: md_cau@madrid.org

  Web: https://gestiona3.madrid.org/portalcau

  Ejemplos de incidentes que afectan o pueden afectar a la seguridad y/o confidencialidad de la información:

  - Extravío, robo o sustracción de un dispositivo externo con información (datos personales, datos confidenciales,…).
  - Sospecha de existencia de virus o de funcionamiento anómalo del dispositivo.
  - Sospecha de algún acceso a la información no autorizada.
  - Cualquier otra incidencia que pueda afectar a la seguridad y/o a la confidencialidad de la información.

COMPROMISO EN PROTECCIÓN DE DATOS PERSONALES

Las directrices indicadas contribuyen a cumplir con el deber de confidencialidad y secreto profesional exigido para todo empleado público en el desempeño de sus funciones, tanto en la normativa de protección de datos citada al principio del documento como en el artículo 52 del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

Comunidad de Madrid

El incumplimiento de estos deberes puede suponer una infracción muy grave de conformidad con los apartados e) y f) del artículo 95.2 de la citada Ley, pudiendo conllevar una sanción de las previstas en el artículo 96.

Asimismo, si de dicho incumplimiento se derivase responsabilidad patrimonial por haberse causado un daño efectivo a un tercero, la Administración Pública, cuando hubiere indemnizado a los lesionados, exigirá del personal a su servicio la responsabilidad en que hubieran incurrido por dolo, culpa o negligencia graves (artículo 36 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público).

El empleado público abajo firmante se compromete a cumplir con las obligaciones indicadas anteriormente, de conformidad con lo previsto en el artículo 18 del Decreto 79/2020, de 16 de septiembre.

Firma:

Puesto de trabajo nº: