

INSTRUCCIONES BÁSICAS PARA EL TRATAMIENTO DE DATOS PERSONALES - TELETRABAJO

En atención a que todas las personas que colaboran con nuestra institución están prestando tareas desde sus domicilios, queremos aprovechar esta carta para reforzar el conocimiento de la política de seguridad adoptada por COLEGIO SAN AGUSTIN (Madrid) para el tratamiento respetuoso de los datos personales de los que somos responsables.

Se indican a continuación las medidas de seguridad a tener en cuenta durante el **teletrabajo**, en cumplimiento de la normativa vigente en materia de protección de datos:

a) El personal deberá **custodiar los datos personales** que traten en el ejercicio de sus funciones, impidiendo que terceros no autorizados accedan a dicha información, adoptando medidas como: Política de mesas limpias, cerrar con llave los cajones, armarios y archivos, bloquear la pantalla del ordenador cuando no estén presentes, mantener en secreto las contraseñas de acceso a los datos personales, entre otras.

b) El acceso a todos los dispositivos utilizados para el tratamiento de datos personales debe estar restringido mediante el uso de **contraseñas robustas**.

Siempre que sea posible se creará dentro del propio dispositivo utilizado **dos usuarios**, uno para el ámbito personal y otro para los asuntos laborales, desde el que se podrá tener acceso a la información del centro.

c) Se debe limitar el uso de dispositivos USB. En caso de que sea estrictamente necesario su utilización para poder dar debido cumplimiento a las funciones propias del personal, el acceso a dichos dispositivos deberá estar **protegido con contraseña**.

d) Durante los traslados de soportes con datos personales, se **deberán custodiar** eficazmente dichos **soportes** impidiendo el acceso de terceros a la información.

e) El personal **no podrá utilizar programas o aplicaciones que no hayan sido autorizadas** por el centro. Para el cumplimiento de la función educativa, solo se podrán utilizar las herramientas puestas a disposición por el centro educativo.

f) Como norma general en los correos electrónicos que se envíen a varias personas, se deberán **poner las direcciones de correo en Copia Oculta (CCO)**. Asimismo, se deberá prestar **especial atención en los destinatarios de los correos electrónicos**, evitando que la información contenida en los correos sea puesta en conocimiento de personas no autorizadas.

g) Los papeles que contengan datos personales deberán **eliminarse** cuando dejen de ser necesarios para la finalidad para la que se recogieron, y nunca deberán tirarse a la basura sin su previa destrucción.

h) El personal deberá **almacenar toda la información tratada en el directorio de red o programa correspondiente** indicado por la Dirección, lo que permitirá que a esta información se le apliquen las medidas de seguridad existentes y que se someta a los procedimientos de copias de seguridad aplicados por la organización

i) No descargar **aplicaciones de dudosa procedencia**. Se trata de evitar que un virus en el dispositivo o hackeo del sistema puedan suponer una fuga de información.

j) **Evitar la conexión a redes públicas.**

k) El personal **comunicará de forma inmediata cualquier incidencia** relacionada con el tratamiento de datos personales. La comunicación se podrá realizar a la siguiente dirección: csam@csamadrid.org

COLEGIO SAN AGUSTIN (Madrid)