Castilla-La Mancha

Seguridad de la información y Protección de Datos

protecciondatos@jccm.es

Como empleados públicos estamos obligados a proteger los datos de carácter personal que tratamos en el ejercicio de nuestras funciones.
También accedemos a los sistemas de información de nuestros organismos: utilizamos ordenadores, dispositivos móviles, nos conectamos a la red…

Es necesario cumplir con ciertas prácticas que ayuden a no comprometer la seguridad de la información y velar por la protección de datos de carácter personal.

Datos de carácter personal

- No comuniques datos personales a otras administraciones, entidades o particulares sin autorización del Responsable del tratamiento o superior jerárquico.
- Cumple con tu deber de secreto en relación con los datos que manejas, incluso después de terminar la relación laboral con esta Administración.

Puesto de trabajo

- No cambies sin autorización la configuración estándar de los sistemas.
- Cuando te ausentes, bloquea tu equipo. 
- Utiliza recursos de red para almacenar información.
- Recoge la documentación cuando finalice tu jornada laboral.

Almacenar información

- Asegúrate de que se hacen copias de seguridad de tu información.
- Ten cuidado al almacenar o distribuir información en dispositivos portables.
- Si necesitas de almacenamiento alternativos, comunícalo a la organización.
- Usa cifrado para almacenar información sensible.

Navegación por Internet

- Verifica los sitios seguros y sé cauto con los que no lo son. https://
- Ten cuidado al abrir ficheros descargados de Internet.
- Si te identificas, cierra tu sesión cuando acabes.
- Las contraseñas no deben almacenarse en el navegador.
- Limpia el historial y la caché del navegador.
- Ten cuidado con la información confidencial.

Correo electrónico

- Sé consciente de donde utilizas tu dirección de correo profesional.
- No respondas a mensajes ni abras o descargues archivos adjuntos de remitentes desconocidos o que no te inspiren confianza.
- No sigas las cadenas de correos y ten cuidado al reenviar correos.
- Evita enviar información sensible, confidencial y protegida a través del correo electrónico.

Contraseñas

- Deben ser secretas, no las compartas.
- Utiliza contraseñas robustas (mínimo 8 caracteres, mezcla de números, mayúsculas, minúsculas y signos especiales).
- Si crees que se ha comprometido tu contraseña, cámbiala inmediatamente.

Dispositivos de usuario

Teléfonos móviles, tabletas, memorias USB, tarjetas de memoria (SD)…

- Distingue entre dispositivos personales y profesionales, evita conectar tus dispositivos personales en los ordenadores corporativos.
- No conectes dispositivos desconocidos.
- Custodia tus dispositivos portables.
- Ten cuidado con las conexiones inalámbricas, especialmente si son públicas.
- Cuando te deshagas de tus dispositivos, asegúrate de que no tengan información.
- Comunica cuanto antes cualquier robo o extravío.

COMUNICA cualquier incidencia que pueda comprometer la seguridad de la información o la protección de datos según los procedimientos establecidos por tu organismo.

En caso de duda sobre la protección de datos de carácter personal consulta a la Delegada de Protección de Datos, **protecciondatos@jccm.es**.