2. Seguridad y privacidad en Internet



Decálogo: 10 pasos hacia la ciberseguridad de Aragonesa de Servicios Telemáticos

Actualmente usamos diariamente las nuevas tecnologías tanto en casa como en el trabajo y, en este escenario, desde la **perspectiva de la seguridad de la información, hemos de tener mayor cuidado** pues, como empleados públicos que gestionamos información en primera persona somos el primer perímetro de seguridad de los datos que manejamos.

> De ahí, que sea clave nuestra implicación en la **gestión segura de la información**, desde la adopción de pautas de comportamiento seguro con las tecnologías hasta la integración de medidas de mejora de la seguridad de la información con la que trabajamos.

A continuación, te presentamos **el Decálogo** que nos recomienda seguir el medio técnico del Gobierno de Aragón, Aragonesa de Servicios Telemáticos:

Copyright 2026

- **Puesto de trabajo.** Mantén la mesa “limpia” de papeles que contengan información sensible. Bloquea la sesión de tu equipo cuando abandones tu puesto. Es sencillo, pulsa a la vez [Tecla Windows + tecla L], tu equipo bloqueará la sesión automáticamente.

- **Dispositivos.** Es mejor que no modifiques la configuración de tus dispositivos si no estás plenamente seguro de lo que quieres modificar. Es arriesgado conectar dispositivos USB no confiables y no está permitido instalar aplicaciones no autorizadas. En tus dispositivos móviles establece una clave de acceso y activa la opción de bloqueo automático.

- **Uso de Equipos No Corporativos.** No manejes información corporativa en equipos de acceso público y, si accedes al correo del Gobierno de Aragón desde tu equipo personal, no descargues ficheros al equipo.

- **Gestión de Credenciales.** No compartas tus credenciales de acceso (usuario y contraseña). Tus credenciales deben ser únicas e intransferibles. No utilices tus credenciales de acceso corporativas en aplicaciones de uso personal porque pueden verse expuestas. No apuntes tus credenciales en lugares visibles.

- **Correo Electrónico.** Fíjate en el emisor del correo y elimina todo correo sospechoso que recibas. Evita los correos en cadena, es decir el reenvío de correos que van dirigidos a un gran número de personas.

- **Navegación.** Evita acceder a páginas webs no confiables y no pinches en enlaces (links) sospechosos. Es preferible escribir la dirección directamente en la barra del navegador y fijarse de que realmente accedes a donde quieres acceder.

- **Viaja Seguro.** Procura no transportar información sensible en dispositivos extraíbles. Si lo haces, cifra la información. No manejes información sensible en redes WIFI no confiables.

- **Protección de la información.** Realiza copias de seguridad de aquella información sensible que sólo esté alojada en tus dispositivos. Más vale un ‘por si acaso’ que un ‘no pensé’.

Copyright 2026

- **Fugas de Información.** No facilites información sensible si no estás seguro de quién es el receptor de la misma. Destruye la información sensible en formato papel (y si es con una destructora del papel, mejor). En todo caso, no la tires a la papelera.

- **Tú eres la Clave.** Si detectas cualquier actividad sospechosa o un funcionamiento anómalo de tu equipo, avisa al 4100.

Revision #7
Created 2023-04-18 13:27:02 CEST by Meritxell Pradel
Updated 2023-10-06 14:12:29 CEST by Silvia Coscolin Sanchez

Copyright 2026