



- ✓ Usar contraseñas diferentes, complejas y cambiarlas con frecuencia.
- ✓ Activar el doble factor de autenticación cuando sea posible.
- ✓ Separar el ámbito personal y profesional.
- ✓ Configurar el bloqueo automático de los dispositivos cuando no se usen.
- ✓ Mantener actualizado el sistema operativo, antivirus y aplicaciones.
- ✓ Instalar aplicaciones solo si es desde fuentes oficiales.
- ✓ Revisar el candado del navegador antes de usar servicios confidenciales.
- ✓ Usar navegación privada cuando sea necesario.
- ✓ Si un correo o mensaje parece sospechoso:
 - Tener cuidado al usar los enlaces y los archivos adjuntos que contenga.
 - Si procede, reenviar a **abuse@juntadeandalucia.es**
- ✓ Usar VPN al acceder a servicios confidenciales desde redes wifi públicas.
- ✓ Tener copias de seguridad de la información más crítica.

sedian

Seguridad Digital
de Andalucía

BUENOS HÁBITOS EN CIBERSEGURIDAD



DOBLE FACTOR DE AUTENTICACIÓN

El doble factor de autenticación permite que un servicio en internet pida la confirmación de una operación por un medio distinto de la propia aplicación en sí: un código enviado por SMS o correo electrónico, requiriendo el uso de la huella digital, etc.

La doble autenticación, muy usada por aplicaciones bancarias, es cada vez más popular, pero requiere la activación expresa por parte de la persona usuaria.

La configuración de esta medida de seguridad depende mucho del servicio concreto a usar, pero se puede encontrar en su ayuda oficial, incluyendo en el buscador "doble factor de autenticación" junto con el nombre del servicio.



GESTORES DE CONTRASEÑAS

Un gestor de contraseñas puede funcionar como un programa independiente del equipo o como un complemento que se instala en el navegador y que funciona exclusivamente con servicios web.

Prácticamente todos los gestores de contraseñas sirven como almacenamiento seguro donde guardar las credenciales de acceso a nuestros servicios aunque los gestores más avanzados, y que suelen requerir licencias de uso, permiten la autenticación automática en los servicios o incluso el cambio automático de estas contraseñas.

En el blog de Andalucía es Digital puede encontrar información sobre diversos gestores de contraseñas:

<https://www.blog.andaluciaesdigital.es/gestores-decontrasenas-gratuitos/>



HERRAMIENTAS ESPECÍFICAS

La Junta de Andalucía dispone de aplicaciones que permiten independizarnos de herramientas externas ajenas a nuestra capacidad de gestión y que pueden plantear un riesgo en seguridad. Aunque podamos echar de menos algunas funcionalidades conviene sopesar la pérdida de control real sobre la información corporativa y de la ciudadanía andaluza.