Por una Administración segura y eficiente

La **implantación de las nuevas tecnologías en los trámites y gestiones de la Junta de Andalucía** es ya una realidad. La ciudadanía, las empresas y otras administraciones pueden realizar *online* más del 85% de los procedimientos censados, lo que supone **importantes beneficios y ventajas** para nuestra sociedad, aunque **aparecen también nuevos riesgos** y amenazas que debemos tener en cuenta.

¿Sabías que **AndalucíaCERT, el centro experto para la gestión de la seguridad digital de la Junta de Andalucía**, detecta cada día hasta un millón y medio de comportamientos sospechos en los sistemas de la Administración andaluza?

¿Qué debemos proteger?

- La **INFORMACIÓN** con la que trabajamos, que afecta directamente a los derechos y deberes de los ciudadanos y ciudadanas.
- Los **EQUIPOS** que la soportan, que deben incorporar medidas de seguridad informática para evitar posibles ataques.
- Las **PERSONAS** que la utilizan, que deben mantener la seguridad digital como un hábito en su día a día.

Un compromiso de todos

La seguridad digital debe ser un **compromiso de toda la organización**, desde la **dirección**, que debe impulsar y dinamizar la política de seguridad, a los **técnicos** responsables de implantar los procedimientos y normas de desarrollo y por último, de los **usuarios** finales que deben aplicar buenas prácticas en seguridad digital.

Precisamente las personas son el eslabón más débil de la cadena de la seguridad de la información. Por eso decimos que:

"el mejor sistema de seguridad eres Tú"

Más info en:
www.juntadeandalucia.es/AndaluciaCERT

JUNTA DE ANDALUCIA

seguridad+ Y CONFIANZA DIGITAL

seguridad+ Y CONFIANZA DIGITAL

Seguridad digital

Consejos prácticos y recomendaciones

JUNTA DE ANDALUCIA

El mejor sistema de seguridad eres tú

Claves para tu seguridad digital

- **Utiliza contraseñas seguras**, que incluyan números, letras y símbolos.
- **No abras correos** ni ficheros adjuntos **si desconfías o desconoces al remitente**. Elimínalos directamente.
- Procura que el **navegador esté siempre actualizado**. Mejora tu seguridad y la de los demás.
- **Utiliza software legal**, que ofrece mayor garantía.
- **Apaga el equipo diariamente** para facilitar que se realicen las actualizaciones de seguridad.
- **Realiza copias de seguridad de tus ficheros** con frecuencia. Así evitarás la pérdida de datos.
- **Mantente informado** sobre las alertas de seguridad.
- **La seguridad debe ser un hábito** y nunca debes bajar la guardia.

Preserva tus datos

- **Tus contraseñas son solamente tuyas**. No las compartas.
- **No utilices tus datos personales** (nombre, apellidos, aniversarios...) para configurar tu contraseña.
- **La firma digital** (o el DNI electrónico) es personal, **debes usarla solo tú y protegerla con contraseñas seguras**.
- Evita ser víctima de fraudes de tipo **phishing**, esos correos electrónicos o páginas web que imitan los de una empresa o institución para solicitar datos confidenciales.
- **Utiliza siempre contraseñas en tus dispositivos móviles** y configúralos para que se bloqueen cuando no los utilices.

Utiliza internet con seguridad

- **Navega** solo por **páginas web seguras y de confianza.**
- **Bloquea siempre tus sesiones** al ausentarte de tu puesto de trabajo.
- **Utiliza una contraseña diferente** para cada una de tus cuentas.
- **Ignora los correos en cadena**, que facilitan que luego recibas correos no deseados (**spam**).
- **En sitios públicos no te dejes nunca las sesiones abiertas**, otros podrían saber lo que has hecho en ese equipo.
- **Si navegas en un ordenador prestado, no dejes rastro de tu actividad.**
- **Los sistemas de mensajería privados son** fácilmente **visibles** para los demás. Piensa qué medio utilizas para tus comunicaciones.
- **Extrema la precaución** si vas a realizar **compras *online*, operaciones bancarias** o vas a facilitar información confidencial. Las páginas deben empezar por **https://** en lugar de http://, e incluyen un candado junto a la dirección.

Protege tu privacidad y tu imagen

- **Configura tus perfiles en redes sociales** de manera adecuada.
- **Piénsatelo bien antes de publicar un contenido.**
- Ten paciencia y **no respondas a provocaciones e insultos.**
- En las redes sociales y en tus comunicaciones en internet **no debes revelar datos personales ni de tu vida privada.**