

TITULARES

Compras seguras en Navidad

Durante la temporada navideña, debemos extremar las precauciones en nuestra actividad online. Este periodo es aprovechado por los ciberdelincuentes para llevar a cabo acciones fraudulentas mediante diversas técnicas.

[Pág. 2](#)**Sharenting, cuando los padres ponen en riesgo la imagen de sus hijos**

Aunque el término pueda resultar desconocido, es una práctica habitual entre padres, madres e incluso abuelos. El término sharenting une los conceptos de compartir y paternidad.

[Pág. 3](#)**Navidades Ciberseguras**

Compartimos una serie de recomendaciones para que podáis disfrutar de manera segura y fiable, evitando los principales riesgos y bulos que giran en torno a estas fechas tan señaladas.

[Pág. 4](#)

Feliz
Navidad

Concienciación

EI POST-IT

Uso de la
información

LA PELÍCULA**CONTRAPORTADA**

El phishing corporativo se dispara en 2025



Estafas con PayPal usan emails reales para colarte compras falsas



Firma electrónica: cuán segura es y principales usos



Predicciones de ciberseguridad para 2026



Comprueba si tu cuenta de correo está comprometida, <https://haveibeenpwned.com/>. Si es así, **cambia la contraseña**.

TITULARES

Compras seguras en Navidad

Si no lo has hecho ya, seguro que muy pronto comenzarás a realizar tus compras de regalos para estas fechas tan entrañables. Como ya viene siendo habitual, cada vez es más común recurrir a la compra online para ahorrar tiempo y evitar aglomeraciones en los ya abarrotados centros comerciales de tu ciudad.

Durante la temporada navideña, debemos extremar las precauciones en nuestra actividad online. Este periodo es aprovechado por los ciberdelincuentes para propagar noticias falsas y fraudes basados en las cosas que hacemos o necesitamos en esta época del año, utilizando técnicas de ingeniería social.

A continuación te compartimos algunos consejos prácticos y sencillos para que tus compras online sean seguras y libres de riesgos.



Navidad CyberSegura: 4 pasos para compras online

#CiberseguridadAND

1. PREPARACIÓN

Prepara dispositivos y cuentas

-  Actualiza software del ordenador o móvil
-  Activa la verificación en dos pasos (2FA)
-  Nunca uses WiFi pública al comprar

2. EXPLORACIÓN

Pre-venta: Vendor Due Diligence (VDD)

-  Verifica https:// y candado en navegador
-  Consulta reseñas de la tienda online
-  Desconfía de ofertas demasiado buenas
-  Cuidado con ingeniería social y phishing

3. COMPRA

¡Asegura la transacción!

-  Usa sistemas de pago que mitiguen el riesgo (PayPal, tarjetas virtuales/monedero)
-  Establece límites de gasto en la aplicación del banco

4. RESPUESTA

¡Responde a Incidentes (IRP)!

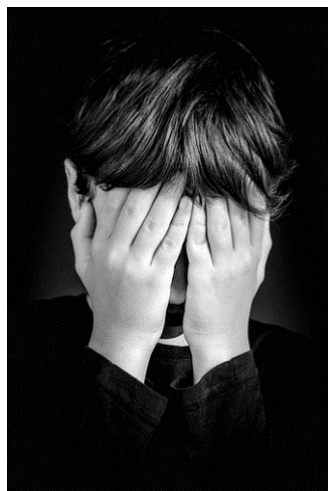
-  Guarda documentación (haz capturas de pantalla)
-  Llama al 017 de INCIBE (es gratis)
-  Denuncia ante Policía/Guardia Civil

**CENTRO
CIBERSEGURIDAD
ANDALUCÍA****OFICINA DE
FORMACIÓN Y
CONCIENCIACIÓN****Junta de Andalucía****Agencia Digital
de Andalucía**

Sharenting, cuando los padres ponen en riesgo la imagen de sus hijos

Los tiempos han cambiado, y lo que antes era un lujo excepcional y complejo, hoy es una acción cotidiana, accesible y rápida. Hacemos fotografías a diario, más si en el hogar hay menores de edad. Después, resulta difícil resistirse a compartirlas.

Pero es un contenido sensible por el mero hecho de afectar a la imagen de un menor, y pasa a formar parte de una **cadena de difusión** de información: nosotros la enviamos, un par de familiares la comparten con terceras personas, y estas a su vez con otras tantas. Puede llegar a manos de alguien desconocido, que sin conocer a tu hijo/a, decida publicarlo en la Red o simplemente guardarlo en su móvil.



Reflexiona sobre la necesidad de compartir

La rápida evolución de la tecnología y su entrada en los hogares es la causa de que nos hayamos visto desbordados por la multitud de opciones disponibles a la hora de compartir datos personales, imágenes y vídeos. Internet y sus aplicaciones nos lo ponen cada vez más fácil, y tenemos que entender que, a menudo, existen intereses detrás para que hagamos pública cada vez más información.

¿Nos extraña que los menores puedan llegar a sentirse abrumados al descubrir, con los años, que cientos de contenidos propios están al alcance de cualquiera en Internet? Además, hay que ser conscientes de que es una situación que no puede deshacerse por completo: algunas imágenes y vídeos pueden ser imposibles de eliminar o recuperar después de ser compartidas.

¿La solución pasa por blindar la imagen de los menores?

La normativa actual especifica que siempre [debe prevalecer el bienestar del menor](#), y que este puede decidir sobre su propia imagen a partir de los 14 años, según la Ley de Protección de datos de carácter personal. Esta también puntualiza que cuando otros menores aparecen en la imagen, siempre debemos tener el permiso de sus responsables legales para poder compartirla.

¿Y si alguna de las fotos publicadas no le gusta a nuestro hijo/a?

Lo más recomendable es respetar siempre su punto de vista y no publicarla o bien eliminarla, si ya lo hemos hecho. Además, recordemos que a partir de los 14 años pueden decidir. Como padres debemos tener claro que su bienestar, también en Internet, es lo primero.

Disfrutar de la tecnología y las opciones que nos ofrece para guardar nuestros recuerdos familiares no es incompatible con la seguridad y el bienestar de nuestros hijos/as. La moderación y el sentido común son la clave.

Navidades Ciberseguras

NAVIDADES CIBERSEGURAS

- ❄️ Aprovecha las vacaciones para cambiar tus **contraseñas**, que sean robustas.
- ❄️ Cuidado con los **juguets** con conexión a Internet, recuerda que siempre debe haber un adulto supervisando su uso.
- ❄️ Si juegas a la **lotería**, asegúrate de comprarla en los portales web de distribución oficiales y no en otros no autorizados.
- ❄️ **Protege** tus usuarios y contraseñas, cuidado con correos sobre permisos o peticiones sospechosas.
- ❄️ Estas Navidades cuida tu **imagen** y la de tu familia y amigos, no compartas en Internet contenido comprometido ya que se quedará para siempre.

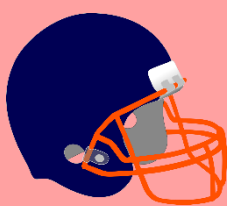
Si te cae algún regalo **tecnológico**, configúralo de forma segura. Que otra persona no pueda controlarlo por ti.



EL POST-IT

Uso de la
información

[Código de conducta](#) en el uso de las tecnologías de la información y la comunicación para profesionales públicos de la administración de la Junta de Andalucía.



Debemos proteger la información a la que tienes acceso y prevenir y evitar cualquier operación que pueda producir una alteración indebida, inutilización, destrucción, robo, revelación o uso no autorizado de la misma.

El acceso a la información, no confiere derecho alguno en cuanto a posesión, titularidad, derecho de copia, de cesión o divulgación de la misma, o cualquier otro derecho.



Protegeremos la información en formato papel, tomando las precauciones necesarias para evitar que esta información pueda ser conocida por personal no autorizado. En particular, no se abandonarán documentos en impresoras, escáneres o faxes. Guardaremos la documentación en lugar seguro evitando que quede sobre las mesas de trabajo al final de la jornada y se seguirán las reglas para su custodia y destrucción.

Debemos cumplir las normas de seguridad y protección de la propiedad intelectual al introducir documentos o archivos en equipos, servidores, redes y sistemas.



Cuando participes en proyectos de análisis de grandes datos o creación de modelos predictivos, es obligatorio seguir las normas y códigos éticos correspondientes.



LA PELÍCULA



Los Santos Inocentes

Hay algunas personas que, por inocencia o descuido, tienen ciertos comportamientos digitales que pueden poner en peligro la seguridad de la información, así como la de los medios electrónicos que utilizan (o incluso comparten) en su desempeño profesional. Para no ser un "santo inocente", te recomendamos las siguientes prácticas.



Contraseñas



Certificados



Internet



Información

01. Contraseñas

No facilites tus contraseñas a otras personas.
Nunca escribas contraseñas en un post-it que dejas cerca del equipo.
Crea contraseñas que combinen mayúsculas/minúsculas, números y caracteres especiales.

02. Certificados

No le dejes tu certificado digital a otras personas para que lo usen en tu nombre.

03. Internet

Evita navegar por sitios web de dudosa reputación.
Reporta correos electrónicos que parezcan sospechosos.

04. Información

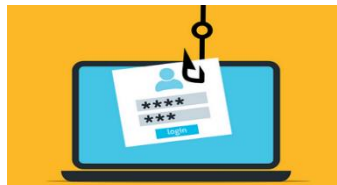
No dejes la sesión abierta cuando te ausentes de tu puesto de trabajo.
Desconfía de llamadas telefónicas donde te pidan datos personales.
Mantente alerta ante avisos por fuga de datos/información en herramientas o servicios.

CONTRAPORTADA

El phishing corporativo se dispara en 2025

Los ataques de phishing se han multiplicado por cuatro en 2025, siendo capaces de engañar incluso a usuarios concienciados y sorteando defensas tradicionales. Superan ya a las amenazas de malware, y ponen en jaque la identidad digital de organizaciones públicas y privadas.

[Más aquí.](#)



Estafas con PayPal usan emails reales para colarte compras falsas

Una estafa abusa del sistema de suscripciones de PayPal para enviar correos reales con falsas compras, burlando filtros de seguridad y alarmando a miles de usuarios. [Más información.](#)



Firma electrónica: cuán segura es y principales usos

La firma electrónica se ha convertido en una herramienta fundamental para garantizar la identidad de los usuarios y la validez de ciertos documentos. Aunque la tecnología es bastante segura, existen amenazas indirectas que es muy importante conocer. [Te dejamos más info aquí.](#)



Predicciones de ciberseguridad para 2026

Con cada final de año llegan los adelantos de lo que se espera para el siguiente. Y en materia de ciberseguridad también ocurre, porque este ámbito cambia a una velocidad enorme. En este artículo se recogen algunas de las predicciones que los expertos están haciendo para 2026. [Conócelas aquí.](#)



¿Has observado un comportamiento digital sospechoso? ¿Estás recibiendo intentos de phishing?
¿Has sufrido un incidente de seguridad? ¡Notifícalo de inmediato por correo o teléfono!

incidentes.soc@juntadeandalucia.es / 955 060 974 (Corporativo 360974)