

## INCIBE. INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 4 de agosto de 2023.- El Instituto Nacional de Ciberseguridad (INCIBE) es un organismo dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, consolidado como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos y empresas. Además, es un instrumento para la transformación social y oportunidad para la innovación, fomentando la I+D+i y el talento.

INCIBE centra sus esfuerzos en la prestación de servicios públicos de prevención, concienciación, detección y respuesta ante incidentes de seguridad, adaptándose a cada público específico (menores, ciudadanía y empresas), así como al desarrollo de tecnología y herramientas que permiten identificar, catalogar y analizar dichos incidentes.

### Caso real del 017: menor con dificultad en el desarrollo realiza sexting y es víctima de sextorsión

Una madre preocupada por una menor con dificultad en su desarrollo madurativo se pone en contacto con el servicio Tu Ayuda en Ciberseguridad tras enterarse de que su hija estaba publicando contenido comprometido.

En ese momento, se descubrió que las personas con las que estaba compartiendo las imágenes le estaban presionando con difundirlas, en caso de que no les enviara más. Ante esta situación, los padres decidieron acudir a las Fuerzas y Cuerpos de Seguridad del Estado para solicitar orientación y denunciar los hechos, así como buscar a través del 017 recomendaciones de profesionales del sector de la ciberseguridad.

Más información: <https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales>

### INCIBE detecta una campaña de sextorsión amenazando con publicar vídeos íntimos

Esta semana INCIBE ha detectado una campaña de correos electrónicos fraudulentos que busca extorsionar a las víctimas exigiéndoles un pago en criptomonedas Bitcoin para evitar que compartan unas supuestas grabaciones íntimas con los contactos de la víctima. Conocido como sextorsión, este engaño puede afectar a cualquier persona, ya que el ciberdelincuente no posee realmente ninguna grabación de la persona, sino que se trata de una forma de preocupar al usuario y provocar que actúe rápido y sin pensar.

En caso de recibir el correo electrónico mencionado, se recomienda eliminarlo directamente y bajo ningún concepto pagar al extorsionador, ni tratar de ponerse en contacto con él contestando al correo.

Más información: <https://www.incibe.es/ciudadania/avisos>

Esta información puede ser usada en parte o en su integridad citando la fuente.

## ¿Cómo reducir el impacto financiero de los incidentes de ciberseguridad?

La aceleración digital deja un futuro abierto a cambios, nuevas formas de negocio y, por supuesto, a nuevas amenazas. Es lógico pensar que, al igual que está cambiando la manera en la que se trabaja, debería ocurrir lo mismo con la forma en la que se protege la información de la empresa.

Es por ello que es importante tener en cuenta nuevas estrategias para aumentar la resiliencia de las pymes y que, a su vez, sean efectivas y de fácil implementación. Una de ellas es la malla de ciberseguridad, un enfoque conceptual moderno de la arquitectura de seguridad que permite a la empresa desplegar e integrar la seguridad en los activos, ya sea en las instalaciones, en los centros de datos o en la nube.

Más información: <https://www.incibe.es/empresas/blog>

## INCIBE identifica una campaña de suplantación a Netflix

INCIBE ha detectado una campaña de *phishing* que afecta a Netflix, cuyo objetivo es obtener información de la tarjeta de crédito y datos personales, a través del enlace que acompaña al mensaje del email.

En caso de ser víctima de este engaño, se recomienda acudir a la entidad bancaria y ponerle al tanto de la situación para tomar las medidas necesarias, ponerse en contacto con las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y realizar *egosurfing* para comprobar si se han expuesto los datos personales o bancarios.

Más información: <https://www.incibe.es/ciudadania/avisos>

## INCIBE detecta una campaña de *phishing* que suplanta a iCloud

INCIBE también ha detectado una serie de correos electrónicos fraudulentos que buscan suplantar la identidad de iCloud a través de la técnica conocida como *phishing*, en los que se notifica al destinatario que ha excedido su capacidad de almacenamiento en el servicio de la nube iCloud y se incluye un enlace que supuestamente ofrece 50 GB de almacenamiento adicional como parte de un programa de fidelización.

En caso de recibir el correo y siempre y cuando no se haya proporcionado ninguna información, se aconseja marcarlo como 'correo no deseado' y eliminarlo de la bandeja de entrada. Sin embargo, si se han ingresado los datos de la tarjeta de crédito o información personal en el formulario, se recomienda ponerse en contacto con la entidad bancaria inmediatamente.

Más información: <https://www.incibe.es/ciudadania/avisos>

Esta información puede ser usada en parte o en su integridad citando la fuente.

## TU AYUDA EN CIBERSEGURIDAD



Teléfono  
017



WhatsApp  
900 116 117



Telegram  
@INCIBE017



Formulario  
web



Atención  
presencial



Más información: <https://www.incibe.es/>



Esta información puede ser usada en parte o en su integridad citando la fuente.