

## INCIBE. INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 3 de noviembre 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.

### Segunda edición del MOOC para educadores “Educar en seguridad y privacidad digital”

El 7 de noviembre comenzará la segunda edición del curso *online* masivo y abierto (MOOC) “Educar en seguridad y privacidad digital”, con el fin de ofrecer las herramientas necesarias a docentes y educadores para trabajar el bienestar en el entorno digital de los/as menores, así como el uso de las aplicaciones y dispositivos que utiliza el alumnado y el equipo docente para el desarrollo de su trabajo.

La formación, lanzada en colaboración con la Agencia Española de Protección de Datos (AEPD) y el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), se desarrollará hasta el 14 de diciembre y tendrá una duración de 5 horas semanales.

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

### ¿Cómo ayudan los hackers a las empresas?

La ciberdelincuencia continúa diseñando nuevas fórmulas para poner a prueba las defensas de las empresas. Por ello, cada vez son más las organizaciones que toman conciencia de la importancia de la protección de datos, ofreciendo interesantes planes de carrera para iniciar y desarrollar carreras como la de *hacker* o profesional de la ciberseguridad.

Además, existe una oferta de recursos y programas formativos que facilitan la adquisición de habilidades y competencias para acceder al sector. De este modo, la seguridad de la información proporciona grandes oportunidades para la reorientación profesional de perfiles, estén o no relacionados con el ámbito tecnológico.

Más información: <https://www.incibe.es/ed2026/blog>

## Caso real del 017: cómo evitar ser víctima del fraude del “sí” y la suscripción a servicios premium

Una mujer de mediana edad se pone en contacto con el servicio Tu Ayuda en Ciberseguridad de INCIBE, a través del 017, tras haber atendido una llamada extraña. Según indica, había contestado la llamada diciendo “sí”, y acto seguido, sin haber mantenido conversación alguna, escuchó una locución dándole la enhorabuena por haber activado el servicio de Amazon Premium por un importe de 200€ mensuales. No obstante, la usuaria comenta que no había facilitado datos personales ni bancarios donde pudieran hacerle llegar los cargos de dicha suscripción. ¿Qué pautas le dio INCIBE?

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

## INCIBE publica una guía para empresas sobre ciberseguridad en la identidad digital y la reputación online

Con el auge de Internet como entorno comercial es fundamental para cualquier empresa tener presencia, comunicarse con los potenciales clientes y ofrecer sus productos o servicios a través de este medio. Por ello, debe saber gestionar la identidad corporativa *online*, con el fin de que el negocio adquiera y mantenga su buena reputación.

A la identidad digital corporativa contribuyen, además de las comunicaciones por correo electrónico y mensajería instantánea, la presencia en Internet mediante una página web o tienda *online* y las redes sociales. En el caso de la reputación *online*, es el prestigio que tiene una marca en el mundo digital. ¿Qué medidas pueden aplicar las organizaciones para proteger ambos aspectos?

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

## Detectada una campaña de phishing que trata de infectar con malware a través de supuestas facturas

Además, esta semana INCIBE ha identificado una nueva campaña de correos electrónicos fraudulentos que distribuyen *malware*. El *modus operandi* es un *phishing* que trata de suplantar la identidad de proveedores genéricos, falsificando el envío de supuestas facturas con el objetivo de que el receptor ejecute *malware*.

En caso de haber ejecutado los archivos a los que se remite en el correo fraudulento o que pueden estar adjuntos en el mismo, se recomienda aislar el equipo de la red lo antes posible. Este equipo debe aislarse y apagarse hasta que se ocupe un técnico, ya que, de lo contrario, el *malware* tendría mayor tiempo para hacer efecto.

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

# BOLETÍN INFORMATIVO



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



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