Tecnología para crecer

Quiénes somos

CONÓCENOS

ASAC ofrece **soluciones integrales para el proceso de transformación digital de las empresas**, de forma cien por cien flexible, cercana y segura

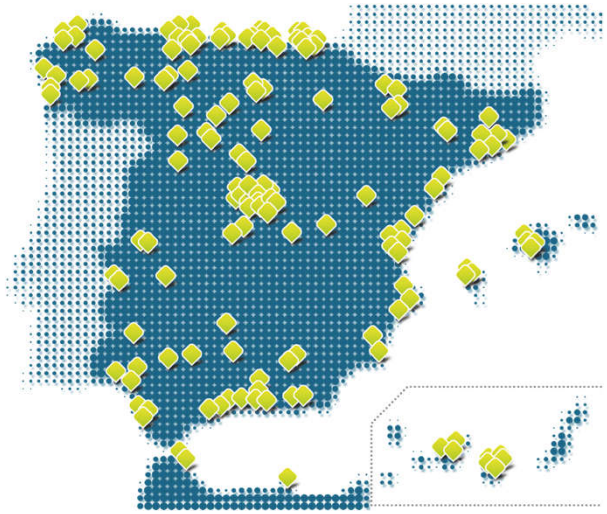
flexibilidad

cercanía

seguridad

En cifras

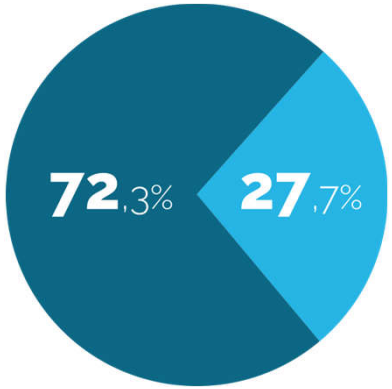
CONÓCENOS



presencia en todas las CCAA

cliente administración pública

cliente empresa privada



+2,1 M€
inversión tecnológica en 2024

+160
Trabajadores
El 50% protege nuestros sistemas

39
edad media
de la plantilla

2.680
horas anuales de formación

↑640
clientes

Instalaciones

CONÓCENOS

Edificio ASAC _ Pq Tecnológico de Asturias _ 33428 **Llanera**
Camino de la Térmica 27 _ Primera planta _ 29004 **Málaga**

Instalaciones

CONÓCENOS

- **Dos centros de proceso de datos propios** ubicados en España, interconectados por un anillo de fibra óptica propio, más acuerdos de presencia en data centers de Madrid y Barcelona.
- **Innovación en la prestación de servicios Cloud en alta disponibilidad geográfica.**
- **Certificaciones TIER III y ENS categoría Alta.**
- **Principales certificaciones ISO** del sector TIC.
- **Elevado nivel de certificación en infraestructuras.**

Certificaciones

Calidad y Seguridad certificada

UNE-EN ISO 9001:2000
Sistema de gestión de calidad

UNE-EN ISO 14001:2004
Sistema de gestión ambiental

UNE ISO 50001:2018
Sistema de gestión energética

ISO 20000-1
Sistema de gestión de los servicios de TI

ISO 22301
Sistema de gestión de continuidad de negocio

UNE-ISO/IEC 27001:2007
Sistemas de gestión de seguridad de la información

ISO/IEC 27017:2015
Certificado de seguridad en la nube

ISO/IEC 27018:2014
Certificado de privacidad en la nube

ISO/IEC 33000 · ISO/IEC 12207
Calidad en el ciclo de vida de Desarrollo de Software
Nivel de madurez 3

Nuestros partners

Conocimientos y experiencia

Protege tu empresa

Consejos prácticos para una ciberseguridad efectiva

asac_

Tecnología para crecer

¿ Qué es un ciberataque ?

Lunes por la mañana. La empresa no tiene internet. Al revisar las cámaras, ves que alguien desconectó el router durante la madrugada.

Recibes un correo con un archivo titulado “Nóminas febrero”. Lo abres y todo parece normal, pero unas horas después, el equipo va lento y algunos archivos ya no se abren.

Un empleado de marketing sube sin querer un Excel con datos de clientes a la web pública. Se da cuenta tres días después.

Pero es una oportunidad futura

¿ Qué es un ciberataque ?

Un **ciberataque** es una acción intencionada que se realiza a través de medios digitales para **acceder**, **dañar**, **robar**, **alterar** o **bloquear información**, **sistemas** o **infraestructuras tecnológicas** sin autorización.

Igual que el mundo físico, pero en vez de utilizar una ventana para entrar, **se explota una vulnerabilidad digital.**

¿ Qué es una vulnerabilidad ?

Debilidad o **fallo** en un **sistema**, **red**, **aplicación** o **comportamiento humano** que puede ser aprovechado por un atacante para comprometer la **confidencialidad**, **integridad** o **disponibilidad** de la información o los recursos digitales.

- **Software desactualizado**
- **Error de configuración**
- **Falta de cifrado**
- **Acceso mal gestionado**

Nivel Técnico

- **Ausencia de políticas**
- **Falta de procedimientos**
- **Falta de controles**

Nivel Corporativo

- **Falta de formación**
- **Contraseñas débiles**
- **Descuido**
- **Negligencia**

Nivel Humano

Mi empresa no es un objetivo

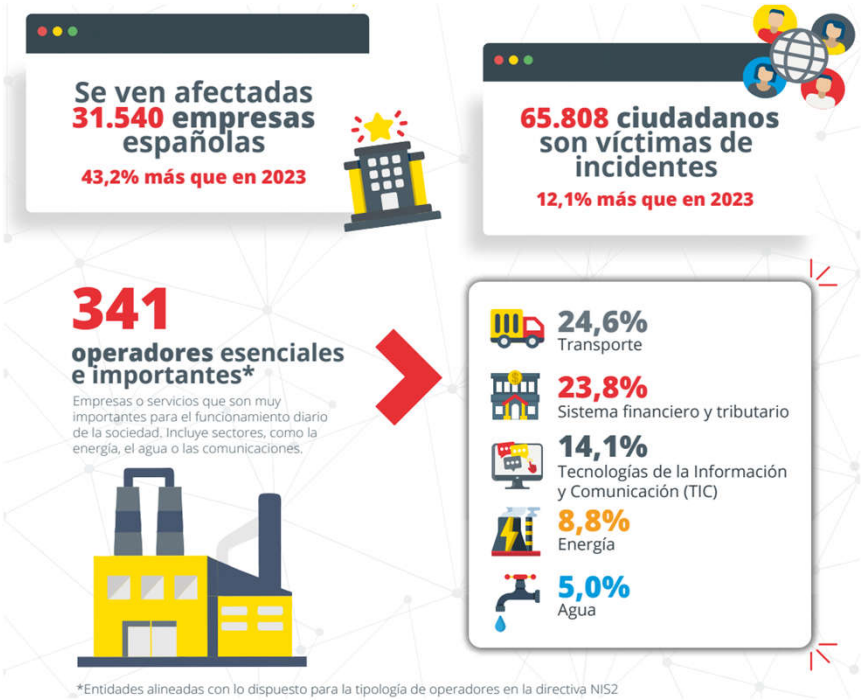
INCIBE presenta su balance de ciberseguridad 2024 con más de 97.000 incidentes gestionados

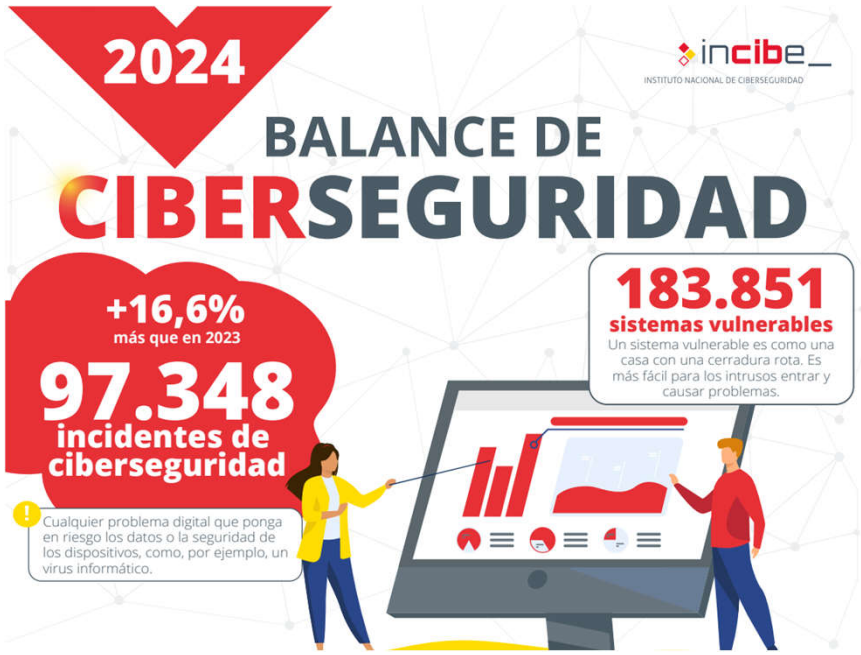
Fecha de actualizacion 26/03/2025

20/03/2025

A lo largo del año 2024, INCIBE a través de su CERT, equipo de respuesta a incidentes de ciberseguridad, gestionó un total de **97.348 incidentes de ciberseguridad**, lo que representa un **aumento del 16,6% en comparación con 2023**. De estos, el 67,6% (**65.808 incidentes**) **afectaron a la ciudadanía** y el 32,4% (**31.540 incidentes**) **a empresas**, incluyendo pymes, micropymes y autónomos.

Mi empresa no es un objetivo





Mundo real vs Mundo digital

Lo que en el mundo real parece absurdo, en el mundo digital lo hacemos a diario, casi sin pensarlo.

¿ Tenemos la misma llave para la casa, el coche o la oficina?

Entonces porque usamos contraseñas repetidas. El 91% de las personas lo hacen.

¿ Le abrimos la puerta de casa a alguien que “parece un repartidor”?

Entonces porque abrimos mails que parecen sospechosos. El 56% los abre sin evaluarlo.

¿ Tenemos la puerta de casa rota y no la reparamos?

Entonces porque demoramos en actualizar los sistemas. El 73% no actualiza.

¿ Le damos nuestro pin bancario a quien nos lo pide?

Entonces porque dejamos la wifi abierta o la compartimos.

Mundo real vs Mundo digital

¿ Dejamos que alguien nos instale en casa algo que no conocemos?
Entonces porque instalamos aplicaciones desconocidas o no confiables.

¿ A quien le damos una copia de nuestras claves bancarias por si pasa algo?
Entonces porque compartimos las contraseñas.

¿ Dejo la puerta de casa abierta cuando voy al super?
Entonces porque dejamos sesiones abiertas al retirarnos.

¿ Dejo un cartel de “no estamos” cuando nos vamos de vacaciones?
Entonces porque publicamos todo en redes sociales, sin filtro.

¿ Tenemos todo lo importante en una caja, sin llave?
Entonces porque no contamos con Backus fiables.

Mundo real vs Mundo digital

Los cibercriminales aprovechan situaciones específicas.

Toda situación de la vida real es una oportunidad para ser utilizado como medio de alcanzar un objetivo.

- Fusión bancaria Liberbank-Unicaja.
- Devoluciones de la agencia tributaria.
- SEPE.
- Bizum inverso.

Un falso George Clooney estafó a una mujer que le transfirió 15 mil dólares

Mediante inteligencia artificial el estafador consiguió recrear la figura del actor de Hollywood que mantuvo un vínculo con la víctima asegurando que estaba a punto de divorciarse.

Algo podemos hacer

Pretexto: “cuando la emoción se enciende, la razón se apaga”. Nos contactan con una excusa que genera emoción o urgencia.

Impostor: no es mas que el disfraz que utilizarán, el rol, el perfil.

Contexto: aquí es donde esta el enfoque. Será algo de actualidad o popularidad creíble.

Oportunidad: ofrecen algo increíble, único, solo para nosotros. Y debe ser ya.

Algo podemos hacer

La ciberseguridad no falla en la tecnología, sino en el descuido humano.

Los cibercriminales no atacan sistemas realmente, atacan personas: clics, contraseñas, configuraciones, decisiones.

Podemos tener el mejor sistema del mundo, pero si hacemos clic donde no debemos, todo fallará.

Es entonces donde debemos centrar todo esto. La parte humana.

Ataques basados en el fallo humano

PHISHING, y variantes (Spear, Whaling, Smishing, Vhishing, BEC, etc).

Engañar a la persona para que nos brinde información confidencial.

“Verifica tu cuenta, ha sido bloqueada”
“Tu paquete está retenido. Actualiza información en…”
“Por políticas de contraseñas debes actualizar antes de…”

Verifica siempre los enlaces.
Verifica siempre el remitente. ¿Realmente es el dominio?
Nada de datos personales.
Utiliza siempre que sea posible, factor de doble autenticación (2FA). Algo que se: “password”, Algo que tengo: “Móvil”, Algo que eres: “Huella, voz, etc”.

Ataques basados en el fallo humano

CONTRASEÑAS

Aprovecharse del uso de contraseñas débiles para acceder al sistema.

“Utilizamos las mismas contraseñas para múltiples accesos”
“Las rotamos cada cierto tiempo de forma correlativa”
“No utilizamos políticas de contraseñas seguras”

Utilizar política de contraseñas robustas.
Utilizar un sistema de gestión de credenciales.
Que no se compongan de cosas fáciles de adivinar.
Utilizar 2FA siempre que sea posible.

Ataques basados en el fallo humano

SOFTWARE NO CONFIABLE

Uso de software aparentemente legal pero que no es cierto.

“Descargamos un Office crackeado para no pagar licencia”
“Descargamos software desde paginas poco fiables, o no validadas”
“Aplicaciones gratuitas”

Utilizar siempre software legal, de pago. Al menos que sea freeware y fiable.
Descargar de los canales oficiales.
Analizarlo mediante el EDR que tengáis instalado antes de hacer nada.
Ante la duda, contactar con un representante del producto.

Ataques basados en el fallo humano

WIFI ABIERTA

Uso de redes inalámbricas abiertas para conexión a internet

“Detectamos que existen muchas wifis abiertas allí donde vamos”
“Algunas nos solicitan información de login tras conectar, como email y número de móvil.”

Preferible plan de GB libres vs Wifi abiertas.
Incluso en el portátil, compartir datos con el móvil es mas seguro.
Desactivar la “conexión automática”, “archivos compartidos”.
Activar VPN y cortafuegos del sistema operativo. O del EDR si es posible.
Perfilar el tipo de conexión como medida adicional de protección.

Ataques basados en el fallo humano

Dispositivos BYOD

Uso de nuestros propios dispositivos para conexiones corporativas

“Que vemos, usamos y compartimos en nuestros dispositivos.”
“Que protección tengo en mis equipos. Y si están sincronizados con otros”.

Segmentar. Lo mío es mío y lo de la compañía es de la compañía.
Utilizar EDR para estos dispositivos.
Utilizar patrones de acceso (huella, patrón, pin)

Ataques basados en el fallo humano

REDES SOCIALES

Publicación de información que puede ser comprometida y/o utilizada

“Identificar que, como y donde estoy publicando.”
“Evaluar si algo de ellos puede ser susceptible de uso malicioso.”

Utilizar los canales oficiales si publicáis en eventos.
Si necesitáis etiquetar, lo menor posible.
Verificar las imágenes antes de subirlas. ¿Que se puede visualizar en ella?

Recomendaciones Globales

Si algo parece raro como para ser verdad, probablemente lo sea.

Ante la mínima duda, consultar con un especialista.

Si alguien nos ofrece protección 100%, no es cierto. Eso no existe.

No apoyarse únicamente en la tecnología. La configuran personas.

Concienciarse de forma continua y ejercitar. Estar preparado es la mejor opción.

Preguntas , dudas y comentarios

Contacto

¿Te ayudamos?

Envío información comercial

marketing@asac.as
www.asacTI.es

MUCHAS GRACIAS