

**Deloitte.**



**Servicios Anti-Ransomware**

Alianza Deloitte & Panda Security

# Contenidos

¿Qué es el Ransomware?	03
Tendencias y evolución	05
Nuestro objetivo	07
Tecnología	08
Despliegue del Endpoint Adaptive Defense	09
Respuesta inmediata: Cyber Incident Response	10

De *software*: programa

# ¿Qué es el Ransomware?

Del inglés *ransom*: rescate

# 1.445.000

Es un tipo de programa informático malicioso que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.

## **Crecimiento exponencial**

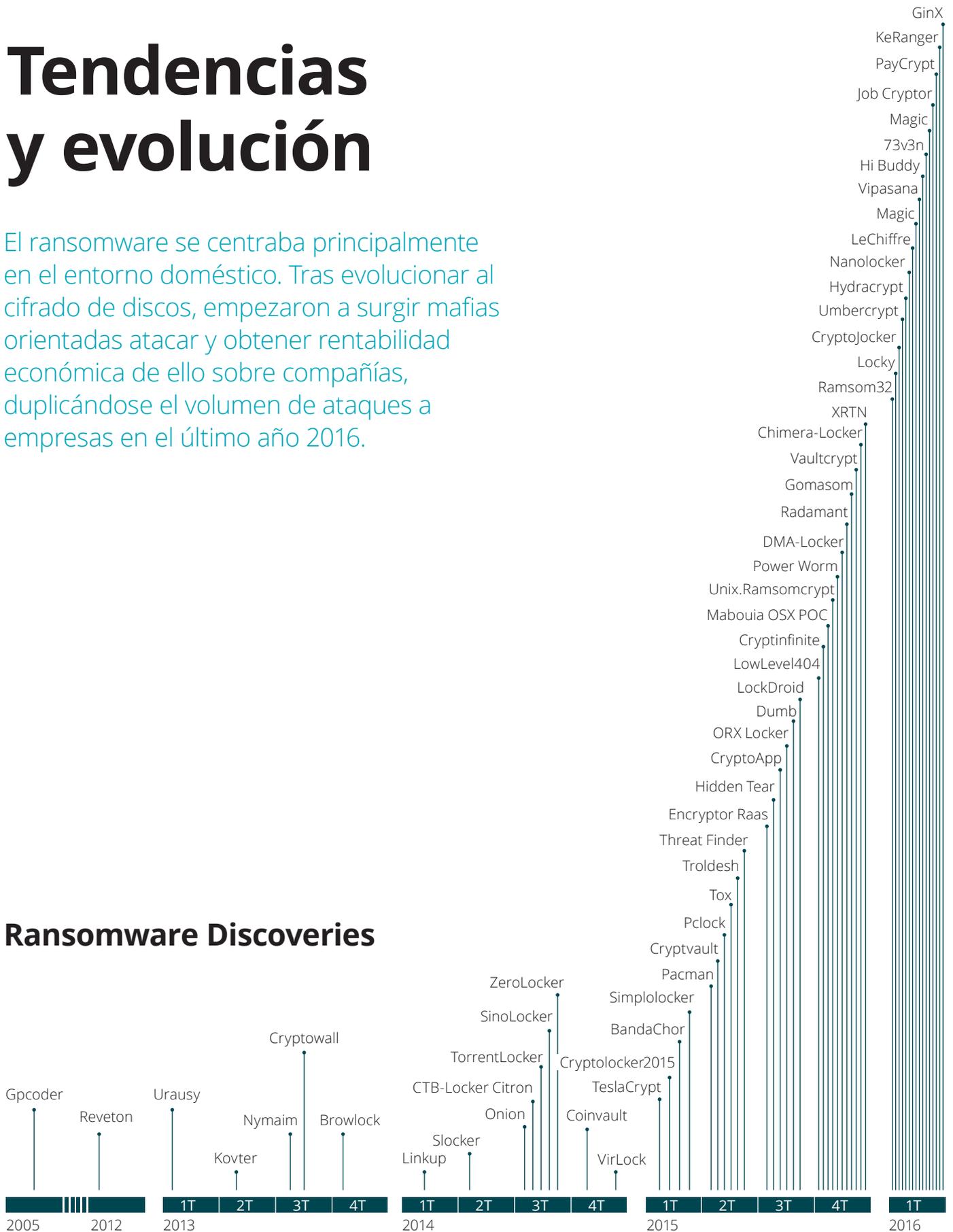
Se hicieron populares en Rusia y su uso ha ido creciendo exponencial e internacionalmente hasta día de hoy con casos tan masivos y preocupantes como Wannacry, Petya, etc...

En 2016, más de 1.445.000 usuarios (incluidas empresas) de todo el mundo fueron víctimas de este tipo de *malware*

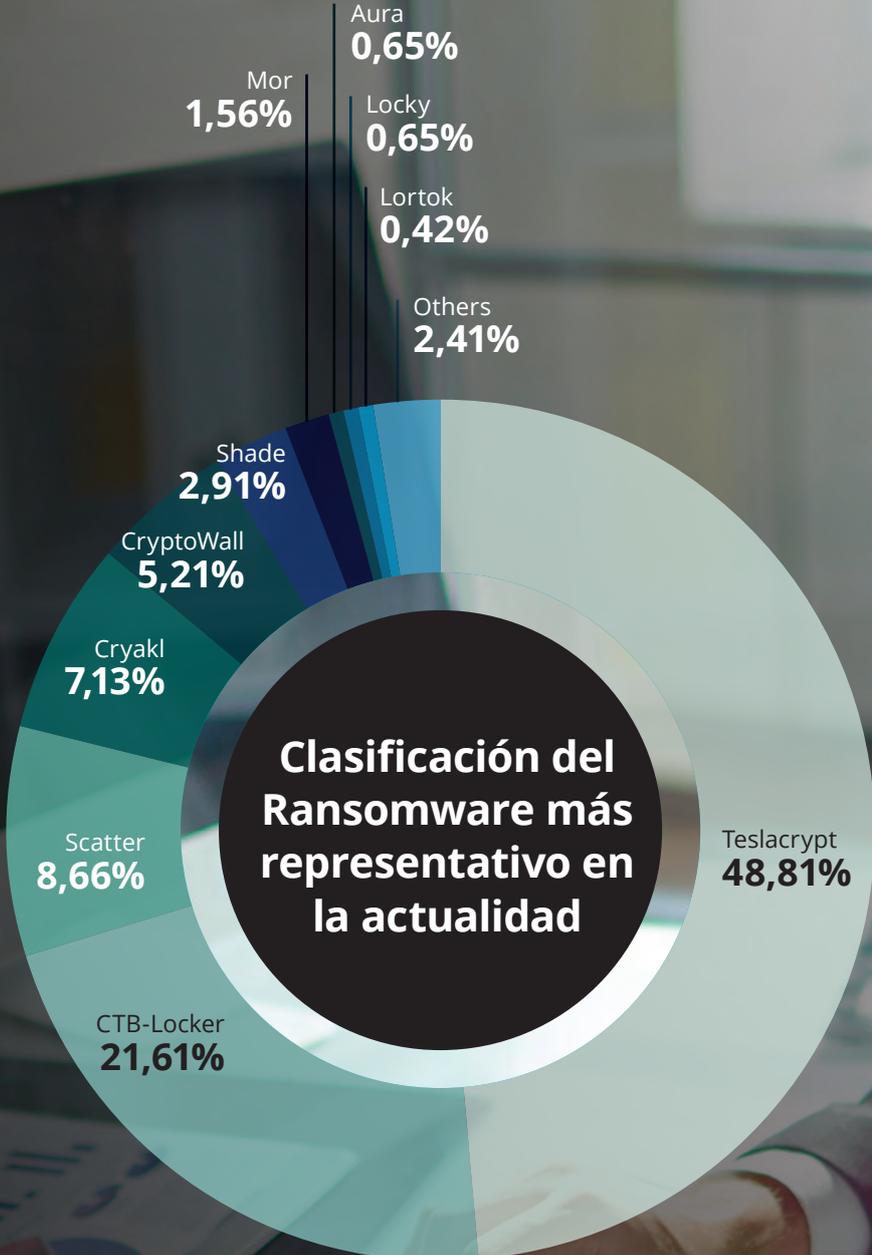
# Tendencias y evolución

El ransomware se centraba principalmente en el entorno doméstico. Tras evolucionar al cifrado de discos, empezaron a surgir mafias orientadas a atacar y obtener rentabilidad económica de ello sobre compañías, duplicándose el volumen de ataques a empresas en el último año 2016.

## Ransomware Discoveries



Fuente: Backtrack Academy



# Nuestro objetivo

El objetivo es hacer frente común, en estructura y metodología por parte de Panda Security y Deloitte EMEA

Panda Security y Deloitte EMEA han cerrado un acuerdo de colaboración para desplegar un servicio gestionado de seguridad sobre su tecnología Adaptive Defense.

Ejemplo de ello, es el uso propio por parte de Deloitte del Endpoint Anti-Ransomware de Panda Security (Adaptive Defense) para todos sus empleados de la firma española.

Los servicios construidos alrededor de la tecnología son los siguientes:



## Despliegue del Software

Despliegue centralizado y automático del software Adaptive Defense.



## Adaptive Defense Management

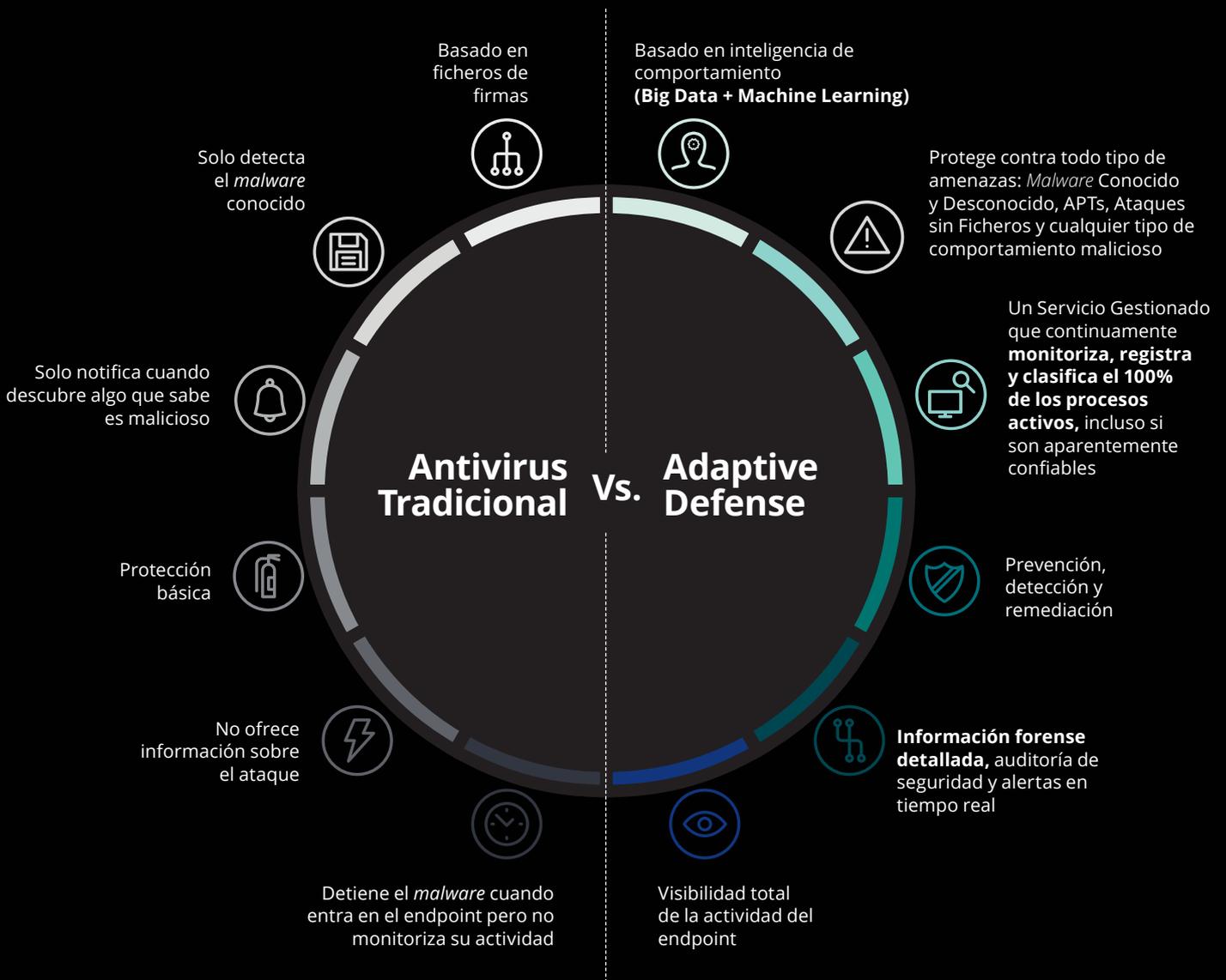
- Mantener actualizado el producto es algo crítico, o solo desde el punto de vista de versionado si no teniendo en cuenta la evolución continua del resto del software del endpoint protegido.
- Reducción y aprendizaje sobre la cantidad total de incidencias, garantizando el funcionamiento óptimo de los dispositivos.
- Control los resultados y certeza de que todo funciona correctamente



## CIR – Respuesta ante Incidentes

El objetivo de C.I.R. es gestionar la situación de manera que se limite el daño y permita al negocio retomar su operativa normal tan pronto como sea posible.

# Tecnología Adaptative Defense



# 100%

Panda Adaptive Defense es un servicio gestionado de ciberseguridad avanzada basado en tres principios: Monitorización continua del endpoint, Clasificación del 100% de los procesos activos gracias a tecnologías Big Data y Machine Learning, y Analítica de comportamiento llevada a cabo por técnicos expertos.



### Endpoint Detection and Response

Monitoriza, analiza y categoriza el 100% de los procesos activos en todos los endpoints de la red corporativa. Certificando absolutamente todas las aplicaciones en ejecución.



### Dynamic Exploit Detection

Su tecnología anti-exploit neutraliza el ataque en cuanto se detecta un intento de explotación de una aplicación confiable, identificando los exploits conocidos y desconocidos.



### Malware Intelligence Platform

La correlación de datos configura un sistema de inteligencia de seguridad capaz de revelar patrones de comportamiento malicioso, para adelantarse a las amenazas.

0,02%

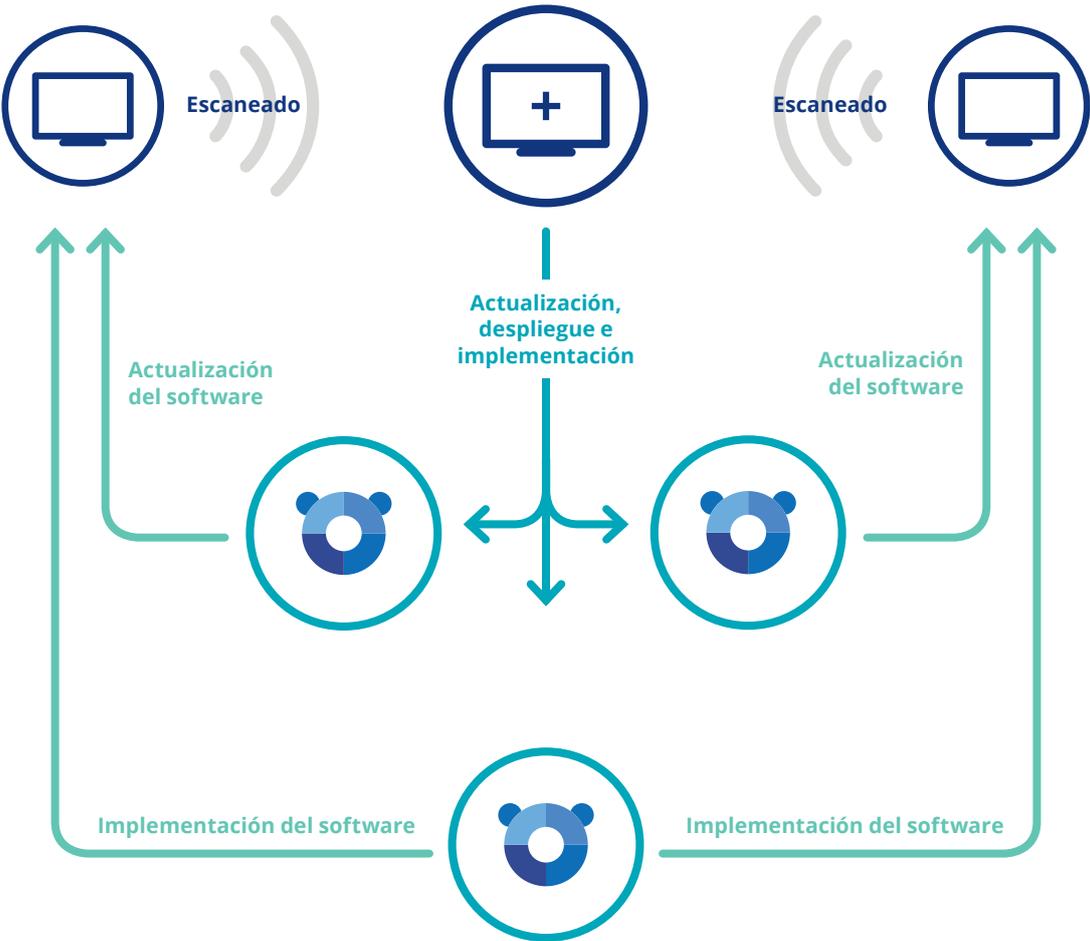
99,98%



SERVICIOS ASOCIADOS

# Despliegue del Endpoint Adaptive Defense

Como primer punto al comienzo de la prestación del servicio Anti-Ransomware, Deloitte ofrecerá el despliegue de la solución Panda Adaptive Defense en los dispositivos de la compañía (en estrecha coordinación con su propio equipo de Sistemas)



SERVICIOS ASOCIADOS

# Respuesta inmediata (CIR)

El objetivo de C.I.R. es gestionar la situación de manera que se limite el daño y permita al negocio retomar su operativa normal tan pronto como sea posible.



Con nuestro servicio se aportan capacidades para identificar, contener y minimizar el riesgo ante este tipo de incidentes, así como medidas para evitar que este no se vuelva a producir.

La casuística de este tipo de incidentes puede ser, por ejemplo:

- Gestión de incidentes de seguridad
- Análisis forense
- Análisis de *malware*
- Programación Shell scripting, perl, Python u otros.
- Revisión de sistemas
- Revisión de Logs

## Cyber Incident Response

24/7/365



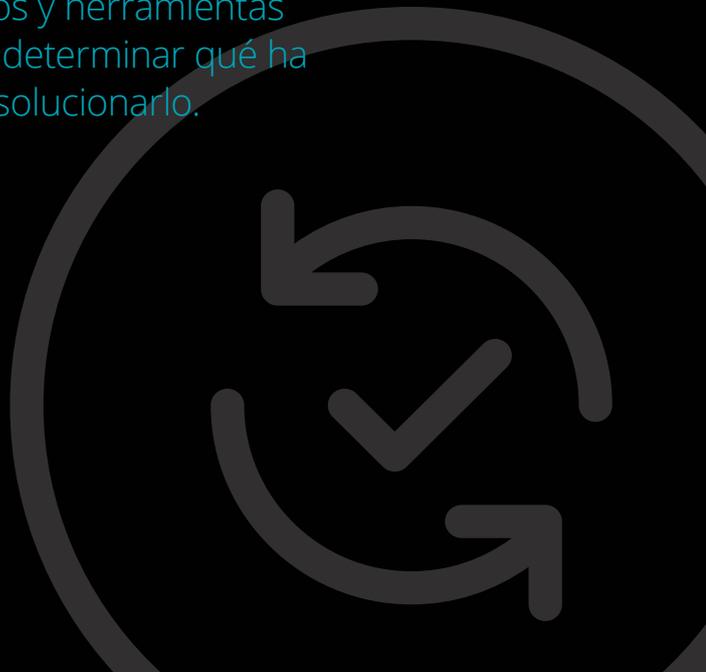
Atención telefónica inmediata

154

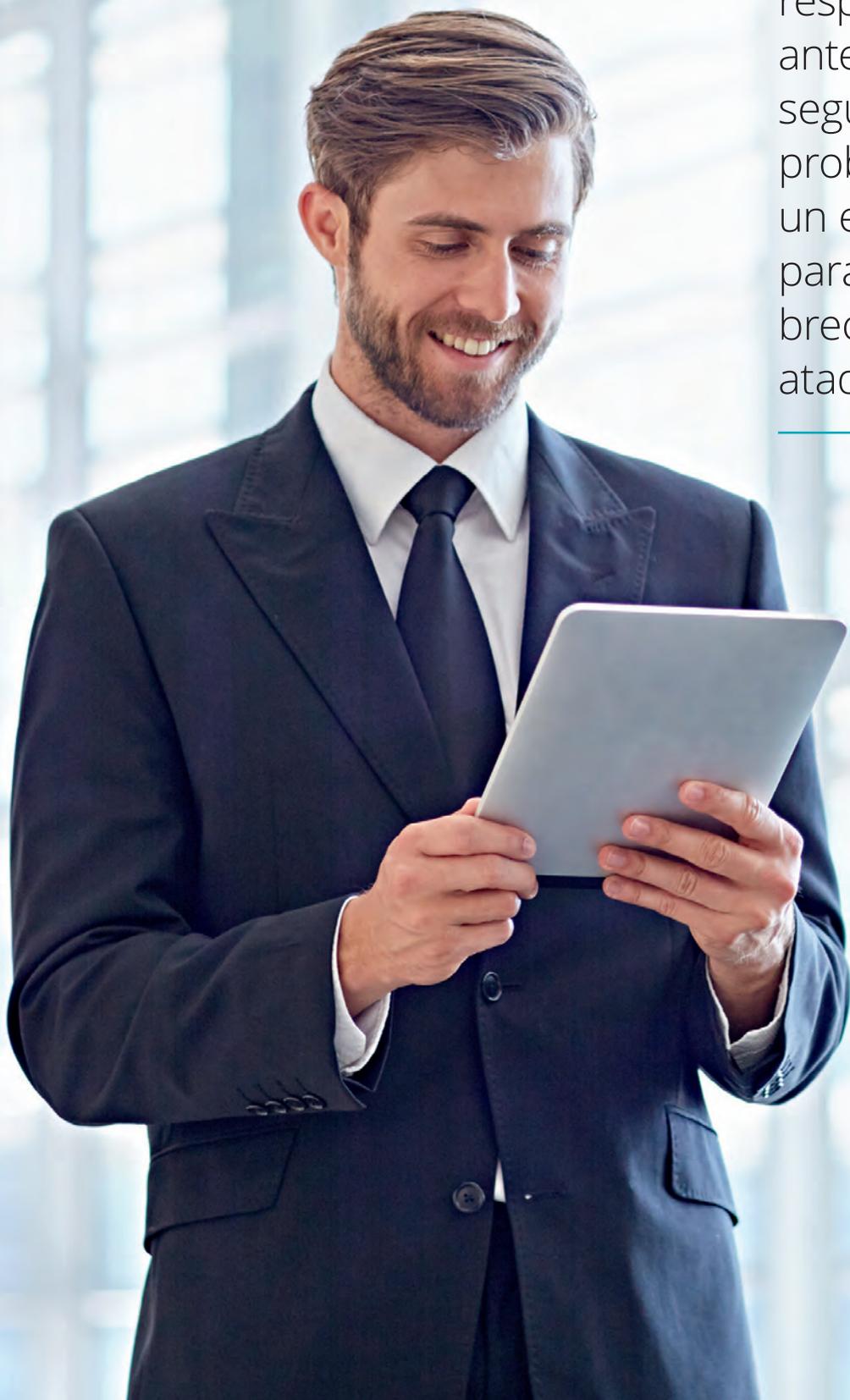


En 154 países

Nuestro equipo le ofrecerá respuestas inmediatas y le ayudará a superar la crisis. Nuestros especialistas aportan los conocimientos y herramientas necesarias para determinar qué ha pasado y cómo solucionarlo.



El servicio de Cyber Incident Response es un servicio avanzado y preparado para dar respuestas inmediatas ante un incidente de seguridad, sea cual sea su problemática ofreciendo un enfoque organizado para la gestión de una brecha de seguridad, ataque o incidente





Si desea información adicional, por favor, visite [www.deloitte.es](http://www.deloitte.es)

Deloitte hace referencia, individual o conjuntamente, a Deloitte Touche Tohmatsu Limited ("DTTL"), sociedad del Reino Unido no cotizada limitada por garantía, y a su red de firmas miembro y sus entidades asociadas. DTTL y cada una de sus firmas miembro son entidades con personalidad jurídica propia e independiente. DTTL (también denominada "Deloitte Global") no presta servicios a clientes. Consulte la página [www.deloitte.com/about](http://www.deloitte.com/about) si desea obtener una descripción detallada de DTTL y sus firmas miembro.

Deloitte presta servicios de auditoría, consultoría, asesoramiento fiscal y legal y asesoramiento en transacciones y reestructuraciones a organizaciones nacionales y multinacionales de los principales sectores del tejido empresarial. Con más de 244.000 profesionales y presencia en 150 países en todo el mundo, Deloitte orienta la prestación de sus servicios hacia la excelencia empresarial, la formación, la promoción y el impulso del capital humano, manteniendo así el reconocimiento como la firma líder de servicios profesionales que da el mejor servicio a sus clientes.

Esta publicación contiene exclusivamente información de carácter general, y ni Deloitte Touche Tohmatsu Limited, ni sus firmas miembro o entidades asociadas (conjuntamente, la "Red Deloitte"), pretenden, por medio de esta publicación, prestar un servicio o asesoramiento profesional. Ninguna entidad de la Red Deloitte se hace responsable de las pérdidas sufridas por cualquier persona que actúe basándose en esta publicación.

© 2017 Para más información, póngase en contacto con Deloitte, S.L.

Diseñado y producido por el Dpto. de Comunicación, Marca y Desarrollo de Negocio, Madrid.