T1 INCREMENTO DE LA CANTIDAD Y LA SOFISTICACIÓN DE LOS CIBERATAQUES

DESCRIPCIÓN

De acuerdo con el estándar ISO/IEC 27032 para la ciberseguridad, el ciberespacio se define como *"un entorno complejo que consta de interacciones entre personas, software y servicios en Internet por medio de dispositivos tecnológicos y redes conectados a ella, y que no existe en forma física"*. En este espacio, la ciberdelincuencia ha vivido un fuerte crecimiento, detectándose una diversificación de métodos, objetivos, complejidad de los ataques y cooperación entre atacantes, que los ha hecho capaces de explotar las vulnerabilidades existentes a lo largo de la cadena de valor de una organización para cometer robos, fraude, extorsión, espionaje, desinformación o interrupción de actividades esenciales para un país, entre otros.

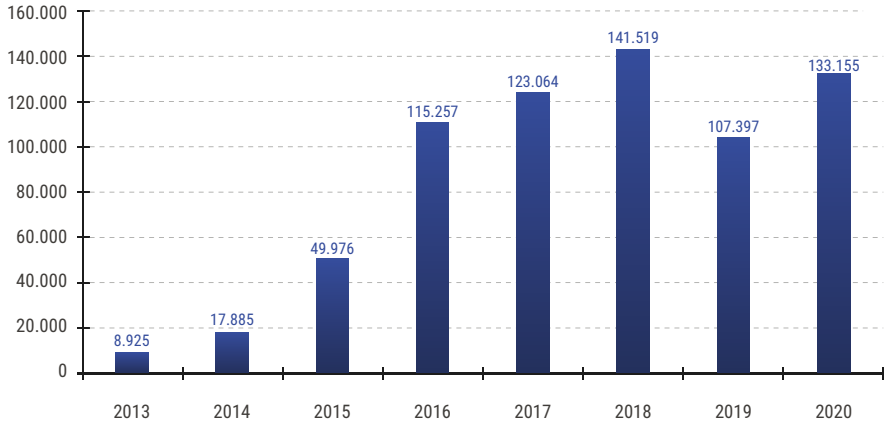
¿Qué está pasando en España?

Se estima que en 2021, cada 11 segundos ha habido un ciberataque a nivel mundial, tiempo que ha ido reduciéndose significativamente en los últimos años, desde los 40 segundos de 2016 (ACCIÓ y Agencia de Ciberseguridad de Cataluña, 2020). En este contexto, **España fue el tercer país más amenazado por los ciberdelincuentes en el 2020**, por detrás de Alemania y Estados Unidos, según un estudio de Ironhack (2021). De hecho, el país sufre diariamente tres ciberataques de peligrosidad crítica o muy alta contra el sector público y empresas estratégicas (CCN-CERT, 2020) y, en el año 2020, el Instituto Nacional de Ciberseguridad (INCIBE) gestionó 133.155 ciberincidentes, un 124% de los de 2019 (Figuras 1 y 2). De ellos, 1.190 fueron dirigidos a operadores críticos y esenciales estratégicos (consultar el riesgo T5 `Fallo de infraestructuras críticas').

MÁS SINERGIAS ENTRE LOS DISTINTOS TIPOS DE AUTORES Y UNA SOFISTICACIÓN DE LOS ATAQUES. La Fiscalía General del Estado afirma en este sentido que "cada vez existe una mayor sinergia entre la actividad criminal derivada de la delincuencia ordinaria y aquella otra vinculada al terrorismo, hacktivismo o incluso la desarrollada en este ámbito por actores estatales mediante estrategias híbridas de desestabilización" (2021).

A esta mayor colaboración entre grupos criminales se le suma la creciente sofisticación de los ataques, ya alertada por el CCN en 2019, ya que sus autores realizan acciones totalmente dirigidas, con un conocimiento del objetivo y sus vulnerabilidades que incrementa las opciones de éxito del ataque (Figura 3).

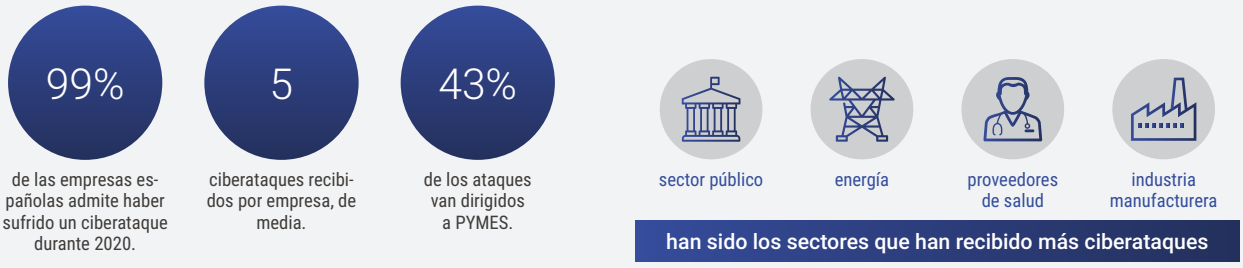
EVOLUCIÓN DE CIBERINCIDENTES GESTIONADOS POR INCIBE Y TIPOLOGÍA EN 2020
(FIGURA 1)



Malware	36%
Fraude electrónico	32%
Ataques a sistemas vulnerables	16%
Otros	8%
Intrusiones	7%

Fuente: INCIBE (2021)

UNA MIRADA A LOS CIBERATAQUES A EMPRESAS ESPAÑOLAS EN 2020
(FIGURA 2)



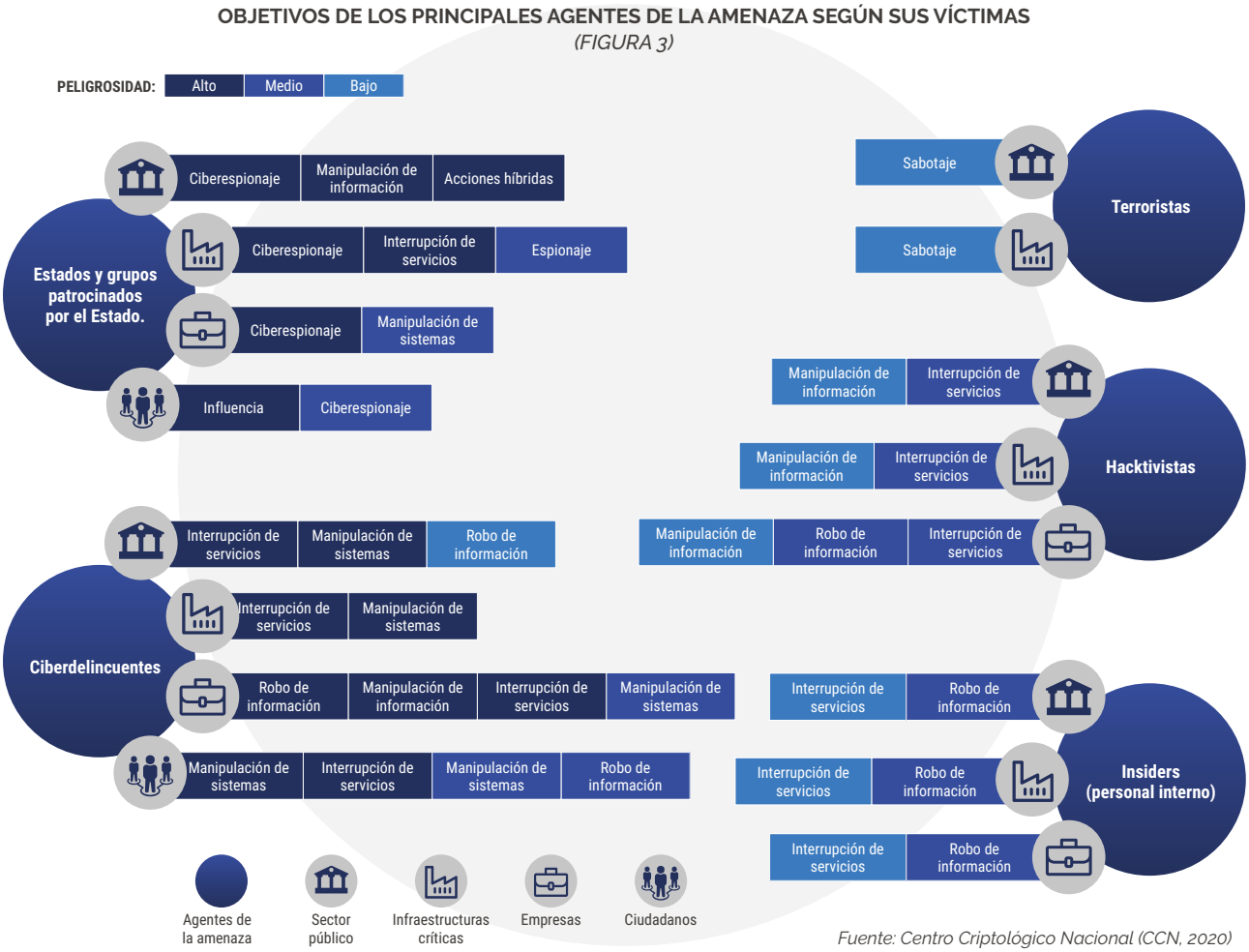
Fuente: ACCIÓ y Agencia de Ciberseguridad de Cataluña (2020)

UN MARCO INSTITUCIONAL AVANZADO, PERO INSUFICIENTES ACCIONES PUNITIVAS.

El compromiso del Estado con la ciberseguridad se ha visto reflejado en distintos esfuerzos materializados en los últimos años. España ocupa la 4ª posición a nivel mundial y la 2ª a nivel de la Unión Europea en el Índice Global de Ciberseguridad de 2020, que mide los compromisos en materia de ciberseguridad de los Estados Miembros de la Unión Internacional de Telecomunicaciones (UIT). La evolución del índice refleja el trabajo realizado en los últimos años (España ocupaba la posición 30 en 2016) obteniendo la puntuación máxima en los pilares legalidad, desarrollo de capacidades y cooperación.

Sin embargo, **la lucha contra los ciberataques se ve debilitada por la dificultad de atribución de estos delitos y su elevada impunidad**. Según la Fiscalía General del Estado (2021), en 2020 se incoaron 16.914 procedimientos por delitos informáticos (frente a 13.143 en 2019), confirmando la tendencia ascendente que se constata en relación con los ciberdelitos desde 2011. Sin embargo, las sentencias condenatorias en 2020 por delitos informáticos fue de 1.202, lo que significa que **más del 90% de los procedimientos iniciados no tienen condena**. Si se tienen en cuenta los datos del Estudio sobre Cibercriminalidad en España del Ministerio de Interior (2021), en el año 2019 los delitos informáticos conocidos alcanzaron la cifra de 218.302 hechos (un 35,8% más que el año anterior); de ellos, los procedimientos incoados por delitos informáticos supusieron solo el 6% de los conocidos y los que contaron con sentencia condenatoria, solo el 0,78%, lo que denota **una impunidad superior al 99% en los ciberdelitos conocidos**.

OBJETIVOS DE LOS PRINCIPALES AGENTES DE LA AMENAZA SEGÚN SUS VÍCTIMAS
(FIGURA 3)



Fuente: Centro Criptológico Nacional (CCN, 2020)

CIUDADANOS CADA VEZ MÁS DIGITALES CONSTITUYEN UNA MAYOR SUPERFICIE DE ATAQUE PARA LOS CIBERDELICUENTES.

Según la agencia We Are Social (2021), en 2020 hubo en España 54,3 millones de usuarios con conexión en dispositivos móviles (lo que supone un 116% de la población), 42,5 millones de usuarios de internet (el 91% de la población) y 37,4 millones de usuarios activos de redes sociales (equivalente a un 80% de la población). Este crecimiento en el uso de la tecnología, sin embargo, no siempre va acompañado de las medidas de seguridad adecuadas. El incremento de las conexiones a partir de dispositivos móviles (personales o de trabajo), que generalmente cuentan con menos medidas de seguridad, son una de las vulnerabilidades a explotar por los delincuentes; además, según el ONTSI (Observatorio Nacional de Tecnología y Sociedad, 2021), en España más de la mitad de los usuarios de PC no identifica que su equipo está infectado por malware y la peligrosidad del malware detectado aumenta paulatinamente, con un 72% de los equipos infectados con malware de peligrosidad alta.

LA PANDEMIA DE COVID-19 HA CONSTITUIDO UN ELEMENTO DISRUPTIVO ACELERADOR DE LA CONECTIVIDAD.

Las medidas sanitarias de confinamiento, distanciamiento social y limitación de las actividades de ocio han incrementado la conectividad desde los hogares, como una forma de escape de la vida doméstica. El aumento del uso de internet es común en todos los grupos de edad, pero más acusado entre las personas de más edad (a partir de 55 años), menos familiarizados con la tecnología y más vulnerables a las campañas de desinformación y phising que han proliferado con la pandemia.

Del mismo modo, las organizaciones se vieron forzadas a adoptar el teletrabajo (antes del COVID-19 solo el 4% de los trabajadores usaban esta modalidad en España), teniendo que encontrar en muy poco tiempo solución a la disponibilidad de equipos, acceso remoto a las redes y sistemas de la organización, aplicativos de videoconferencia, etc. en ocasiones sin acompañarlo de un análisis de los riesgos asociados o de los protocolos de prevención y respuesta. Según un estudio global de HP Wolf (2021), durante la pandemia

el 76% de los equipos de IT priorizaron la agilidad y la continuidad de la actividad por encima de la seguridad y el 83% cree que el aumento del teletrabajo es una "bomba de relojería" para los ciberataques.

Si bien la adopción del teletrabajo en España muestra signos de estabilización en el segundo trimestre de 2021, tras una reducción con la relajación progresiva del confinamiento, hay ciertos comportamientos del teletrabajador que vulneran la ciberdefensa de la organización. Según datos de Fundación Telefónica (2021) para España:

50% utilizan aplicaciones no corporativas en dispositivos de la empresa, y, de estos, el 26% cargan datos de la compañía en ellas.

85% usan el portátil corporativo para su navegación personal y, de estos, solamente el 33% restringen los sitios visitados.

37% acceden a los datos corporativos desde su dispositivo personal con frecuencia.

LOS PRÓXIMOS RETOS DE CIBERSEGURIDAD PARA LAS EMPRESAS.

Los ataques a la cadena de suministro se perfilan como un riesgo creciente para las organizaciones. La robustez adquirida por ciertas empresas a nivel de seguridad ha provocado un cambio en los atacantes, que han puesto el foco en los proveedores como potenciales puertas de entrada a ellos. Los ataques organizados a la cadena de suministro permiten que con un solo ataque exitoso, el impacto se propague en cascada a gran número de clientes que dependen del proveedor. Además, el hecho de que haya al menos dos organizaciones afectadas, dificulta la gestión general del incidente y su análisis forense.

Según ENISA (2020), los ataques a la cadena de suministro aumentaron en número y en sofisticación durante 2020, tendencia que se mantuvo en 2021, con previsiones de cuadriplicar en número los del año anterior. En relación a los ataques analizados:

50% fueron atribuidos a grupos cibercriminales conocidos (o amenazas avanzadas persistentes (APT)), que originan ataques de una complejidad y recursos mayores.

62% de los casos, la técnica empleada fue un *malware* y los ataques se aprovechan de la confianza del cliente en el proveedor como vector de ataque.

58% de los ataques a proveedores buscaban acceder a datos de los clientes, el 16% acceder a personas concretas y sólo el 8% tenían un objetivo económico.

LA FALTA DE TALENTO EN CIBERSEGURIDAD Y TECNOLOGÍA DIFICULTA LA DIGITALIZACIÓN SEGURA DE LAS ORGANIZACIONES.

Mientras crece sustancialmente la concienciación sobre la necesidad de implementar medidas de seguridad, **el porcentaje de empresas que cuentan con perfiles de especialistas en tecnologías se ha reducido en 2020**, como también lo ha hecho el número de compañías de más de 10 empleados que ofrecen formación en tecnología a sus empleados.
Tras estos datos se encuentra la situación de dificultad económica a la que han tenido que hacer frente muchas empresas tras la pandemia y la falta de capacidades que, según ENISA (Agencia de la Unión Europea para la Ciberseguridad, 2020), está dificultando las estrategias inversoras de más del 70 % de las firmas europeas y el 79% de empresas a nivel mundial afirma que encontrar el talento adecuado en materia de ciberseguridad es muy difícil o extremadamente difícil (ACCIÓ y Agencia de Ciberseguridad de Cataluña, 2020).

CIBERATAQUE AL SERVICIO PÚBLICO DE EMPLEO ESTATAL (SEPE)

El 9 de marzo de 2021 el sistema informático del SEPE, que gestiona el pago de las prestaciones por desempleo, sufrió un ciberataque que afectó tanto a los puestos de trabajo en oficinas como a los portátiles de los empleados que se encontraban realizando teletrabajo, que tuvieron que apagarse para evitar la propagación de la amenaza.

El ciberataque, dejó sin servicio informático al SEPE durante 4 días, en los que la actividad se vio interrumpida tanto en las oficinas físicas (710) como telemáticas (52) de este organismo, se interrumpió el acceso a su web, se mantuvo únicamente la recepción de solicitudes de forma manual a través del teléfono y se acumularon retrasos en la gestión de citas, agravando la situación que se arrastraba de la pandemia.

Para paliar las 225.000 horas de trabajo perdidas por el ataque, el SEPE propuso a los trabajadores recuperar horas de trabajo de forma voluntaria durante algunos sábados, iniciativa que tuvo una acogida inferior al 10% del personal.

El ciberataque se basó en el ransomware Ryuk, cuyo principal vector de entrada suele ser el 'e-mail'. Este software malicioso tiene la capacidad de cifrar archivos y propagarse rápidamente a otros ordenadores conectados a la red, para cifrarlos uno a uno en pocos minutos. El ataque del SEPE se suma a una tendencia que se percibe a nivel global de ataque a instituciones públicas.

EL RIESGO PARA LAS **EMPRESAS**

El coste de un ciberataque varía mucho según la compañía y el autor y objetivo tras el ataque. Además del coste económico directo (por robo, fraude, rescate pagado, etc.), en el cálculo del daño debe considerarse la interrupción de la actividad durante el ataque (si esta queda comprometida), el daño a la reputación de la organización, la recuperación de los datos y sistemas, etc. Adicionalmente, puede considerarse la inversión necesaria en protección, monitoreo y neutralización de amenazas.

Cybersecurity Ventures (2021) estima que el cibercrimen ha tenido en 2021, un coste global de 6 billones de dólares anuales, lo que representa el 1% del PIB mundial. En el caso de España, se estima que el 45% de los ataques han provocado daños por valor de más de 400.000 € y que el coste medio de un ataque a una PYME es de 35.000 € (ACCIÓ y Agencia de Ciberseguridad de Cataluña, 2020).

IMPACTOS EN LA EMPRESA

- Afectación a la imagen de la compañía.
- Pérdida de reputación.

- Posibilidad de conflicto interdepartamental.
- Dificultad total o parcial para acceder a los puestos de trabajo.
- Afectación a la seguridad y salud de las personas, menor disponibilidad o indisponibilidad de personal crítico.
- Menor rendimiento laboral (bajas, huelgas, dificultad de conciliación...).
- Aumento de la conflictividad laboral.
- Mayores necesidades formativas de los trabajadores.
- Pérdida de reputación del propio personal directivo.

- Paralización o aplazamiento de proyectos o decisiones estratégicas.
- Incertidumbre en la reconversión de procesos.

- Pérdida de posición de mercado por afectación a productos o servicios.
- Pérdida de posición de mercado por afectación de la reputación o imagen.
- No adaptación del modelo de negocio.
- Aumento de costes de operación.
- Mayor gasto en recuperación de datos y/o sustitución de equipos.
- Aumento de la siniestralidad y de las primas de aseguradoras.

- Interrupción o disminución del nivel de producción.
- Disminución del nivel de servicio.
- Problemas de calidad de los productos o servicios.
- Desajustes en la programación de la producción o servicio.
- Problemas de mantenimiento de instalaciones y maquinaria.
- Problemas de personal para llevar a cabo la producción.

- Incremento de la complejidad de las cadenas de suministro.
- Problemas en la gestión del aprovisionamiento y compra.
- Problemas en la cadena de suministro, transporte y distribución.

- Necesidad de obras de seguridad, adecuación o reconversión de instalaciones o entorno de trabajo.
- Inhabilitación completa o parcial de edificios, sistemas o recursos productivos.