Cuadernos de Dirección Aseguradora

301

El plan de ciberseguridad en las compañías aseguradoras

Máster en Dirección de Entidades Aseguradoras y Financieras

UNIVERSITAT DE BARCELONA

UNIVERSITAT DE BARCELONA

301

El plan de ciberseguridad en las compañías aseguradoras

Estudio realizado por: Ricardo Ibáñez Navés
Tutor: Jesús González Álvarez

Tesis del Máster en Dirección de Entidades Aseguradoras y Financieras

Curso 2021/2022

Cuadernos de Dirección Aseguradora es una colección de estudios que comprende las tesis realizadas por los alumnos del Máster en Dirección de Entidades Aseguradoras y Financieras de la Universidad de Barcelona desde su primera edición en el año 2003. La colección de estudios está dirigida y editada por el Dr. José Luis Pérez Torres, profesor honorífico de la Universidad de Barcelona, y la Dra. Mercedes Ayuso Gutiérrez, catedrática de la misma Universidad.

Presentación y agradecimientos

En primer lugar, quisiera agradecer a mi mujer Núria toda su paciencia infinita y amor demostrado durante este período tan exigente, tanto durante las clases como en la realización de esta tesis.

En segundo lugar, a mi compañía, Seguros Catalana Occidente, por apostar por mí y darme esta oportunidad tan enriquecedora y que, espero, poder demostrar que ha valido la pena esta inversión.

En tercer lugar, a Jesús, mi tutor, que siempre se ha mostrado abierto a cualquier duda o necesidad que pudiera tener y que ha sabido guiarme para poder llevarla a cabo.

Por último, quería agradecer a la dirección del máster, Mercedes, Jose Luis, Ferran, los profesores y también los compañeros de este año de conocimientos, experiencias y buen ambiente. No he participado en otros cursos de este máster, como pudiera ser obvio, pero ha sido un año de gente excepcional.

A todos los que compartimos caminos, feliz de compartirlo, y a los que nos hemos encontrado gracias a éste año, encantado de empezar a compartirlo.

Resumen

Análisis de la situación actual del mundo de la ciberseguridad, que se considera ciberseguridad y de, como las regulaciones y los estándares, nos pueden ayudar a tener un grado de cumplimiento mínimo exigible.

Explicación del ciclo de vida de la ciberseguridad y que tener cuenta para poderla planificar.

Análisis de la situación actual del sector seguros respecto a la ciberseguridad.

Palabras Clave: Ciberseguridad, Plan de ciberseguridad, CISO, TIBER, DORA, EIOPA, INCIBE, ICEA.

Resum

Anàlisis de la situació actual del mon de la ciberseguretat, què és considerat ciberseguretat i com les regulacions i els estàndards ens poden ajudar a tenir un grau de compliment mínim exigible.

Explicació del cicle de vida de la ciberseguretat, i que hem de tenir en compte per poder-la planificar.

Anàlisi de la situació actual del sector assegurances respecte a la ciberseguretat.

Paraules Clau: Ciberseguretat, plà de ciberseguretat, CISO, TIBER, DORA, EIOPA, INCIBE, ICEA.

Summary

This thesis undertakes an analysis of cyber security in the world today. It begins by examining what we understand by cyber security, and how regulations and standards can help companies achieve a minimum level of compliance.

The lifecycle of cyber security is outlined and a discussion of what is needed to plan it correctly is reported.

The thesis concludes with an analysis of cyber security in Spain’s insurance sector today.

Keywords: Cyber Security, Cyber Security plan, CISO, TIBER, DORA, EIOPA, INCIBE, ICEA.

Índice

El plan de ciberseguridad en las compañías aseguradoras

1. Introducción

Vivimos en un mundo donde la tecnología está presente en todas las áreas de nuestro día a día, tanto en nuestra vida personal, como en la laboral.

La tecnología es un elemento básico que ha pasado a considerarse más una *commodity* que algo con lo que soñar. Hoy en día nos rodea casi sin darnos cuenta, podríamos hablar de las Smart Cities, de Smart Phones, de IoT, de Wereables, o de casi cualquier elemento cotidiano. Elementos con los que interactuamos casi sin pensar. Está en constante evolución e innovación para llegar a los sitios dónde todavía no está presente y así poder poner solución a pequeños y grandes problemas cotidianos o de retos empresariales, económicos o de salud.

Las empresas hacen uso de tecnología e innovación para poder ofrecer sus productos cada vez más especializados, y a segmentos de clientes más diferenciados, de una manera más ágil y usable. Se usa en I+D, se usa en medicina, se usa en el deporte. Podríamos decir que se usa, y se va a usar, en todos los sectores o retos que se nos puedan ocurrir.

No obstante, en los Global Risks Reports anuales del World Economic Forum, se puede observar que los riesgos relacionados con la tecnología (color lila) se consideran muy probables desde 2007, los relacionados con ciberataques aparecen en 2012 y, los relacionados con fraude y robo, en 2017. En el reporte de 2021 hay un cambio debido al Covid-19 considerándose los riesgos desigualdad de acceso a la tecnología y excesiva concentración de poder tecnológico en unas pocas empresas y en el sector privado, como los más destacados.

En cambio, en el reciente informe del 2022, en el que se centran en estudiar que riesgos han empeorado más desde el Covid-19, se ve como los riesgos derivados de la ciberseguridad han empeorado un 12.4%, con lo que vuelve a ganar en importancia. Se explica que desde 2020, ha habido un incremento de un 435% en ataques tipo ransomware[1], pero lo más destacable es que ***el 95% de los problemas detectados de ciberseguridad, han sido debidos a un error humano*** (*este dato ya lo daba IBM en su informe anual[2] de seguridad del 2014 de su equipo X-Force en el que ponían como ejemplo el uso de usuarios y contraseñas por defecto en los sistemas, contraseñas fáciles de adivinar, una gestión de actualizaciones de software pobre, pero el peor de todos es la facili-*

[1] Ransomware es un tipo de ciberataque en el que se encriptan datos y se pide un rescate para poder volver a acceder a ellos.

[2] IBM X-Force Threat Intelligence Index

dad en el que las personas abren adjuntos maliciosos de correos o en páginas comprometidas sin pensarlo).

Ilustración 1-1 Risks by Likelihood

Fuente: World Economic Forum, "*Global Risks Report 2021*"

Tenemos muchos casos recientes cercanos y públicos en los que los ciberataques han inhabilitado o dificultado la actividad de las entidades afectadas durante meses, unos cuantos titulares y breve explicación:

- "***Pegasus mobile spyware used zero-click exploits to snoop on Catalan politicians***" (The Dialy Swig). El pasado 18 de abril, un software creado en Israel por la empresa NSO ha sido encontrado en móviles de políticos, activistas, abogados y sus familias, relacionados con el independentismo Catalan, se le conoce como el "CatalanGate" y permite acceder a cualquier contenido del dispositivo móvil donde se ha encontrado, así como acceder libremente a las cámaras y micrófonos de este.

- *"**El ciberatac al grup Llobet és el més important al Bages dels últims mesos***" (Regió 7). A principios de enero de 2022, este ciberataque se encriptaron todos los datos de producción, además de las copias de seguridad. Para no pagar el rescate solicitado por los atacantes, la empresa tuvo que reintroducir los datos manualmente.

- "***Un atac informàtic al Liceu va sostreure noms, correus i DNIs***" (Tot Barcelona). Aunque en un primer momento pareció que no pudieron ac-

ceder a la base de datos entera del teatro, sí que se pudieron obtener datos sensibles en marzo del 2022.

- "***El govern destina més de 3,5 milions d'euros a la UAB perquè es recuperi del ciberatac***" (CCMA). El pasado 11 de octubre de 2021 la Universitat Autònoma de Barcelona sufrió un ataque que paralizó las clases 2 días, dejándola sin red prácticamente hasta navidad. Aquí también hubo afectación en las copias de seguridad. Además, se produjo un intento de extorsión, por parte de los atacantes, con amenazas de filtración datos. Se calcula que se necesitará como mínimo todo 2022 para volver a la normalidad.

Los ciberataques son un riesgo a nivel mundial, a continuación, unos ejemplos:

- "***345,000 People are Affected by a Data Breach at ARcare***" (CySecurity News". El pasado 4 de abril ARCare, una clínica de salud de Arkansas detectó que se había podido acceder a los expedientes de más de trescientos mil pacientes. Esta clínica trata a pacientes crónicos, medicina del comportamiento, pacientes con Sida, con lo que los datos son extremadamente sensibles.

- "***Cyberattack on Toyota's supply chain shuts its 14 factories in Japan for 24 hours***" (CNN). A principios de marzo 14 fábricas de Toyota tuvieron que estar paradas durante un día entero debido a un ciberataque en la cadena de suministros.

Recientemente se ha dado a conocer la existencia de un malware[3] capaz de infectar y permitir control sobre elementos IoT[4] y de control de Schneider Electric y Omron, con lo que se podría hablar de que, en caso de infección, se comprometerían industrias como la Industria Energética.

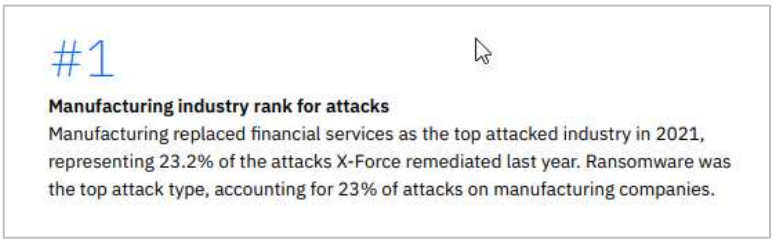
En el reporte anual de ciberseguridad de IBM, este año ha destacado que, por primera vez en los últimos 5 años, el sector de finanzas y asegurador no está como el primer objetivo de los ciberataques, lo que significa que históricamente, los atacantes, han tenido su ojo puesto en nuestro sector. Aunque haya cambiado durante el 2021, y el sector haya pasado a ser el segundo objetivo, no quiere decir que tengamos que bajar la guardia.

[3] Malware manera de referirse a software creado con objetivos maliciosos

[4] IoT "Internet of Things", todos los dispositivos actuales que están conectados y enviando datos (p.e. un sensor de humedad que esté enviando datos a un servidor central)

[4] Phishing, técnica por la que se envía un correo ilícito, pero con el formato de un correo lícito de manera que se intenta engañar al usuario para que abra el archivo adjunto o bien acceda a una página similar a la real para que introduzca sus datos de conexión (usuario y contraseña), de pago (tarjetas de crédito), etc

Ilustración 1-2 Key Stats



Fuente: "*X-Force Threat Intelligence Index 2022*"

No es mi pretensión discutir el papel necesario del uso de la tecnología, si no las precauciones que una compañía de seguros debería tomar al hacer uso de ella, el marco legal en el que se mueve, y como de preparada debería estar para cuando suceda.

Debido a la naturaleza intrínseca del negocio asegurador, y dado que cualquier aseguradora maneja datos muy sensibles, la probabilidad de ser blanco de ciberataques es muy elevada, pudiendo dicho riesgo producir daños reputacionales, pérdida de confianza de los clientes y del mercado en dicha aseguradora.

2. Antecedentes

2.1. Definición de ciberataque

Ç

En primer lugar, debemos conocer la definición de ciberataque. Vamos a ver dos ejemplos de dos institutos conocidos dedicados a ciberseguridad:

Glosario de términos de INCIBE[5]:

> "***Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema***."

Glosario de términos de NIST[6]:

> "***An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information***."
>
> (traducción propia al castellano *"Un ataque, a través del ciberespacio, dirigido al uso que hace una empresa del ciberespacio, con el fin de interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno/infraestructura informática; o destruir la integridad de los datos o robar información controlada*")

Se observa que no existe una única definición aceptada de lo que es un ciberataque. Pero podemos destacar los siguientes puntos en común:

- Sistemas informáticos
- Daños al sistema
- Los datos son un activo importante

2.2. Primeros ataques o ciberataques

Si vinculamos los ciberataques a internet, está claro que tendríamos que mirar la historia reciente. Pero si tenemos en cuenta las telecomunicaciones, podríamos remontarnos a 1834 donde unos hermanos se aprovecharon del sistema francés de telégrafo para enviar información de los mercados económicos en un momento en el que la información nunca había viajado a esa velocidad. La red de telégrafo era usada por el gobierno para defensa. Los hermanos, para enviar esta información añadían, mediante un agente de telégrafos sobornado, caracteres a los telégrafos oficiales. Convirtiéndose en la primera referencia a la modificación de mensajes transmitidos por líneas de telecomunicaciones.

[5] INCIBE "**I**nstituto **N**acional de **Cibe**rseguridad"

[6] NIST "National Institute of Standards and Technology" de Estados Unidos.

Un siglo más tarde, en 1960, ARPA[7] empezó a investigar la tecnología que permitiría en el 1969 la intercomunicación entre las primeras universidades. El uso de ARPANET[8] fue popularizándose hasta que en 1982 se estandarizó el protocolo TCP/IP[9]. A partir de esa fecha se empezó a extender la red por todo el mundo, pero no fue hasta 1989 que empezaron a surgir los primeros proveedores de servicios de internet (ISPs[10]) y un año más tarde se cerraba ARPANET al ver que, a través de estos ISPs, se garantizaba la expansión de una red a nivel mundial. En ARPANET se distribuyó el primer gusano informático, conocido como "Jeepers Creepers". Este gusano informático contaba con 14 líneas de código y hacia aparecer un mensaje por la pantalla "*I'm the creeper: Catch me if you can*". El autor, un profesor del MIT[11], creó un programa informático experimental con el que pretendía demostrar la posibilidad de usar ARPANET para autorreplicarse y realizar una tarea simple en los ordenadores contactados (el mensaje).

En 1975 se dio a conocer el primer troyano[12], se llamaba "ANIMAL". Se distribuyó como juego que, en 20 preguntas, podría adivinar cualquier animal que el jugador pensara. Al ejecutar el programa principal, se lanzaba otro que exploraba todas las carpetas del disco duro copiando el programa principal en todas ellas.

El primer virus informático que uso internet para propagarse apareció en 1988. Se le conoce como "The Morris Worm". Morris, un alumno de la universidad Cornell (Ithaca, NY), ideó un programa que pretendía contar el número de ordenadores conectados a internet.
Para poder realizar dicho conteo, el programa diseñado, iría buscando posibles ordenadores, instalándose en dichos ordenadores y propagándose a partir de ellos a otros nuevos, sumando el contador cada vez que realizara dicha instalación. Morris hizo un diseño pensando en la robustez y para ello, se volvería a instalar en un ordenador, aunque ya estuviera presente. Esto creó un bucle donde cada vez había más instalaciones del programa en los ordenadores, haciendo que cada vez fueran peor. El resultado fue que unos 6.000 ordenadores (alrededor del 10% de internet de aquel entonces) fueran infectados. El gobierno americano estimó que la reparación de los daños estaba entre 200.000$ y 2.9M$. Morris fue acusado de fraude y abuso informático condenado a pagar una multa y a 3 años de servicios comunitarios.

En el año 2000, surgió el primer virus que utilizó el correo electrónico como método de propagación. Dicho virus tenía el nombre de "ILOVEYOU". El correo

[7] ARPA "Advanced Research Projects Agency" del departamento de defensa de los Estados Unidos.
[8] ARPANET "Advanced Resarch Projects Agency Network"
[9] TCP/IP protocolo de intercambio de mensajes en el que se basa cualquier red de datos.
[10] ISP "Internet Service Providers", o lo que es lo mismo, las compañías que permiten la interconexión vía internet de los diferentes clientes.
[11] MIT "Massachusetts Institute of Technology", Universidad privada de Estados Unidos, referente mundial de I+D de cienca y tecnología.
[12] Virus camuflado en una aplicación que el usuario ejecuta para otro propósito

electrónico recibido, contenía un programa con el nombre “iloveyou.txt.vbs” que, al abrirlo, buscaba documentos como fotos, documentos de texto, ficheros de música, para reemplazarlos con su propio código impidiendo su uso. Además, se instalaba en el sistema de arranque, para ejecutarse cada vez que se reiniciara el ordenador. Para continuar su propagación, aprovechaba la agenda de contactos del sistema operativo Windows, y enviaba una copia de sí mismo a todos los contactos encontrados. Se estima que causó un daño por valor de 5.5 a 8.7 B$ y que para eliminarlo se destinaron alrededor de otros 10 a 15 B$.

Cabe mencionar también ataques perpetrados por BotNets[13], que se han convertido en un elemento para tener en cuenta hoy en día, sobre todo a partir de la aparición de los dispositivos IoT. Los BotNets se dieron a conocer en el año 2000, de manera pública, a través de la BotNet “*EarthLink Spammer*” desde la que se enviaron 1.25 Millones de e-mails de phising[14]. El primer ciberataque relacionado con los sistemas IoT fue en 2016, conocido como “*Mirai*”, desde el que se ejecutó un ataque DDoS[15]. Esta red tenía a su disposición 600.000 dispositivos IoT. Con ellos dejaron sin servicio toda la costa este de Estados Unidos. Lo crearon unos universitarios para intentar ganar ventaja en un juego llamado Minecraft.

2.3. Primeros pasos hacia la seguridad de la información

Con la creación de ARPANET en los 60, comentada anteriormente, y la interconexión así de diferentes entidades, fue la primera vez que se tuvo que desarrollar una solución de ciberseguridad. Se desarrolló un proceso consistente en definir franjas (períodos) en los que cada entidad, o conjunto de entidades, que iba a procesar una serie de datos confidenciales, pudiera hacer uso de la red de manera que no colisionara con las demás, una vez acabada la franja, se purgaban (o saneaban) ordenadores para evitar fugas de esa información sensible. A este proceso se le conoció como “Periods Processing” o “Multilevel Processing” y todavía es usado hoy en día.

Con la creación de las primeras redes, se introdujo el concepto de “router” (enrutador) o “gateways” (puertas de enlace), que son los dispositivos de red encargados de hacer interconexiones entre diferentes redes. El uso de estos dispositivos nos permitió empezar a llegar a cualquier red o servicio publicado en internet. En los 80 se empezaron a usar como elemento de seguridad, ya que,

[13] BotNet es una red de dispositivos conectados a internet capaces de ejecutar programas, normalmente ordenadores o dispositivos infectados con un programa de botnet, de manera que puedan ser controlados remotamente para realizar actividades ilícitas como por ejemplo enviar mails de phising o ataques de DDoS.

[14] Phishing, técnica por la que se envía un correo ilícito, pero con el formato de un correo lícito de manera que se intenta engañar al usuario para que abra el archivo adjunto o bien acceda a una página similar a la real para que introduzca sus datos de conexión (usuario y contraseña), de pago (tarjetas de crédito), etc.

[15] DDoS, “Distributed Denial of Service” ataque por el cual se intenta tumbar un servicio concreto a partir de múltiples conexiones al servicio de manera que se queda sin recursos para atender tantas peticiones (es como intentar parar una ola de mar con un cubo de playa). El servicio cae sin remedio.

al estar entre dos o más redes, se empezaron a separar dispositivos que por seguridad no debían estar juntos. En los "routers" se empezaron a definir reglas de seguridad para permitir conexión entre ciertos dispositivos de diferentes redes y no a otros. Esta solución no era completa, se necesitaba ir un poco más allá y se empezó a desarrollar la tecnología llamada "Firewall" (cortafuegos), añadiendo inteligencia a la inspección de tráfico entre diferentes redes, para evitar conexiones indeseadas. El primer firewall comercial fue "DEC[16] SEAL" se puso a la venta en 1991. Ese mismo año se publicaba la primera herramienta gratuita de encriptación de información, PGP[17].

En 1970, después del virus "Creeper" comentado anteriormente, el creado del correo electrónico, Ray Tomlinson, creó un programa para eliminar el virus que usaba un método similar para propagarse y limpiar el virus. Se podría decir que fue el primer antivirus conocido. Pero hasta 1987 no aparecieron los primeros antivirus comerciales masivos que permitían acceder a tecnologías que arrojaban seguridad al mercado de ordenadores domésticos. Ese año se fundó McAfee lanzando "VirusScan" en 1988. Cabe mencionar que los primeros ordenadores personales de distribución masiva se empezaron a vender hasta finales de los 70.

En 2002, Bill Gates[18] inició la iniciativa "TwC"[19], en la que se veía de vital importancia desarrollar software sin olvidar 4 puntos clave: seguridad, privacidad, fiabilidad e integridad de negocio, para conseguir los clientes vieran a Microsoft como un fabricante de software en el que confiar, igual que confiaban en servicios "commodity" como podía ser el agua, la electricidad o el teléfono. Dentro de esa iniciativa, se iniciaron procesos como el de actualización mensual de su software incorporando todas las correcciones necesarias a los problemas de seguridad detectados y publicados, o también la primera conferencia "blue hat", donde se invitaban investigadores de seguridad externos para hablar directamente con sus ingenieros y directivos sobre todo lo que estaban desarrollando.
En 2003 Microsoft anunció una recompensa de 5 M$ a quién ayudara a encontrar a aquellos que explotaban bugs de seguridad[20]. Defendió esta estrategia de recompensas, debido a que ya se estaba haciendo mucha inversión en desarrollar software y necesitaban poder controlar los factores externos de alguna manera. En 2011 cambiaron de estrategia, y esa recompensa la decidieron dar a quién les reportara dichas brechas de seguridad o bugs sin haberlas explotado o publicado públicamente.

Podría decir que desde el momento en que se disponían de este tipo de redes de interconexión entre diferentes actores, y los primeros virus informáticos se empezó a desarrollar la necesidad de empezar a proteger la información.

---

[16] DEC "Digital Equipment Corporation", Empresa de informática desde 1960 hasa 1998 que fué adquirida por Compaq.

[17] PGP "Pretty Good Privacy", programa de encriptación creado en 1991

[18] Bill Gates, fundador de Microsoft.

[19] TwC "Trustworthy Computing"

[20] Bug: manera generalizada de referirse a un defecto de programación en un programa informático con el que se puede llegar a realizar acciones para el que el programa no estaba diseñado

2.4. Profesionalización e incremento de los ataques

En 1986 se publicó el ensayo „*The hacker Manifesto*“, en que se clamaba que las técnicas de hacking van más allá de un deseo egoísta o de la intención de hacer daño a gente. Se describían esas técnicas como necesarias para expandir nuestros horizontes y permitir que el mundo continuara siendo libre. Este ensayo fue escrito en una revista electrónica para hackers, por Lloyd Blankenship, miembro de un grupo de hacking conocido como “Legion of Doom”. Durante esos años, muchos grupos de hacking fueron creados, con la intención de transferir conocimientos a sus miembros de una manera organizada.

En 2002 aparece un servicio descentralizado sobre internet llamado “The Onion Routing Project” (actualmente conocido como Tor) con la intención de permitir el anonimato completo en comunicaciones por internet. Permitir el anonimato en internet crea controversia, pero figuras públicas como Edward Snowden[21], explican su visión de la necesidad de este tipo de servicios, a continuación, un extracto de la entrevista que le realizaron los responsables de Tor:

> “***Tor is a critical technology, not just in terms of privacy protection, but in defense of our publication right -- our ability to route around censorship and ensure that when people speak their voices can be heard***.”
>
> (Traducción propia al castellano “*Tor es una tecnología crítica, no solo por lo que representa a la privacidad, sino también para defender nuestro derecho de publicación -- nuestra capacidad para evitar la censura i asegurarnos que cuando la gente habla, se escuche su voz*”)

Hemos de tener en cuenta que el acceso a internet y el control del mismo, desde que se desmontó ARPANET, mencionada anteriormente, no está regulado, se realiza por empresas privadas y los gobiernos pueden llegar a tomar el control mediante regulaciones accediendo a cualquier información generada por cualquier usuario identificándolo sin problemas. El gobierno Chino por ejemplo no permite acceso a redes como Facebook, YouTube o Twitter, y monitoriza todo uso que hacen sus ciudadanos de internet.

En el report anual de 2016 de IBM X-Force, aparece por primera vez mención a la red Tor:

> “***Subvert access control. Ranking as the third most prevalent attack type targeting the information and communications technology sector was the “Indicator” category, which was due largely to attempted connections from Tor software exit nodes. Tor (an abbreviation of the original project name, “The Onion Router”) is designed to allow full anonymity to the end user. Although not all traffic coming from the Tor network is indicative of an attack, by using a Tor client, a cybercriminal can disguise the attack’s originating network location and its path to the target, making identification virtually impossible***”
>
> (Traducción propia al castellano: “*Subversión del control de acceso, clasificado como el tercer ataque más frecuente, dirigido al sector de las tecnologías de la información y*

[21] Edward Snowden es conocido por haber filtrado información de la National Security Agency (NSA) americana.

comunicaciones, es la categoría "indicador", debido en gran parte a los intentos de este tipo de conexiones desde nodos de salida del software Tor. Tor (una abreviatura para "The Onion Router", está diseñado para permitir el anonimato total a los usuarios. Aunque no todo lo que viene de la red Tor se puede considerar un ataque, al usar un cliente Tor, un cibercriminal puede ocultar su ubicación de red y el camino que sigue para llegar a su objetivo, haciendo virtualmente imposible su identificación.")

Los servicios Tor no solo son usados por ciberdelincuentes como hemos comentado, pero es cierto que la mayoría de los servicios de la "Dark Web" [22] son accedidos y publicados a través de ésta. A partir de este tipo de anonimato se ha ido montando un mercado en este tipo de redes dónde acceder a todo tipo de servicios ilegales (venta de drogas, venta de información, malware diseñado específicamente para afectar a una empresa en concreto, etcétera).

Antes de la aparición de este tipo de mercados, para poder realizar algún tipo de ataque por lo general lo realizaba alguien con altos conocimientos informáticos y de redes y se generaba sus herramientas, podríamos decir que no era fácil que alguien sin esos conocimientos pudiera llegar a realizarlos, y tampoco era fácil que ese alguien sin esos conocimientos pudiera contratar a una persona así ya que no existía una manera de ponerse en contacto. Es por eso que a partir de 2010 se empiezan a encontrar referencias a métodos de hacking como servicio:

- **CaaS** (*Cybercrime-as-a-service*): se usa para referirse a todos los servicios relativos a romper la ciberseguridad ofertados en la Dark Web.

- **MaaS** (*Malware-as-a-service*): se usa para referirse a la contratación de todo tipo de malware, ya sea malware genérico (más barato), o específico para un uso concreto que se haya solicitado (más caro).

- **FaaS** (*Fraud-as-a-service*): se usa para referirse a la contratación de un servicio de fraude (con todo lo que incluya: BotNets, Malware, etc...).

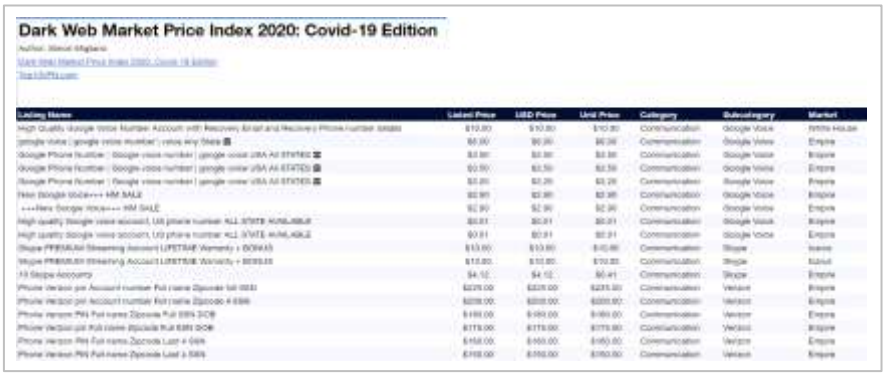
- **AaaS** (*Attacks-as-a-service*): se usa para referirse a la contratación de personal para hacer todo el ataque dirigido que se requiera.

- **RaaS** (*Ransomware-as-a-service*): se usa para referirse a la contratación de este tipo de malware llamado ransomware.

La profesionalización de este sector de ciberdelincuencia permite la contratación de servicios independientemente o un conjunto de ellos por cualquiera con cada vez menos conocimientos. Cada año se publican tablas que recogen los precios de muchos de estos servicios, se pueden encontrar en diferentes sitios web de investigadores de seguridad, a continuación, una muestra:

[22] Dark Web se podría describir como el "mercado negro" de internet, se basa en sitios de descarga, foros y servidores en internet a los que no se puede acceder de manera directa, sin anonimizar la conexión, donde se pueden contratar servicios de toda índole no legal.

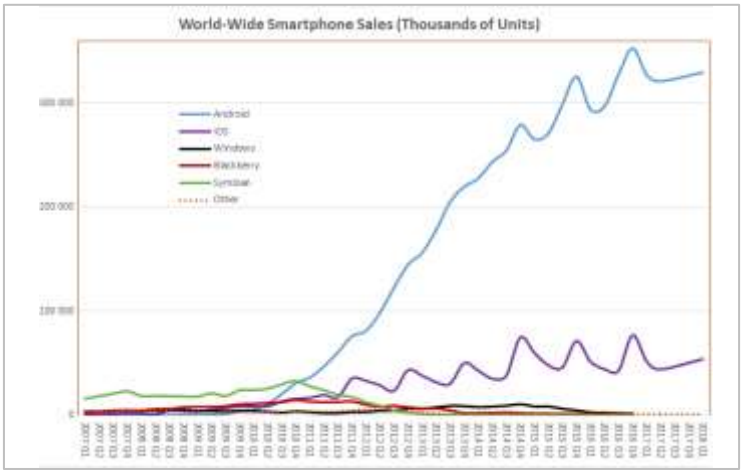
Ilustración 2-1 Extracto de tabla de precios Dark Web Market 2020



Fuente: Top10VPN "*Dark Web Market Price Index 2020: Covid-19 Edition*"

Teniendo en cuenta que hasta la aparición de los smartphones en 2007 los únicos dispositivos capaces de acceder a internet eran los ordenadores personales con dos fabricantes de software destacados, Microsoft con su sistema operativo Windows, y Apple con su sistema operativo MacOs. Windows siempre ha sido el claro dominante de este mercado, actualmente, tiene casi el 75% de cuota según "StatCounter[23]". A partir de la aparición de los primeros smartphones el mercado empieza a cambiar.

Ilustración 2-2 Ventas globales de dispositivos SmartPhones por sistema operativo

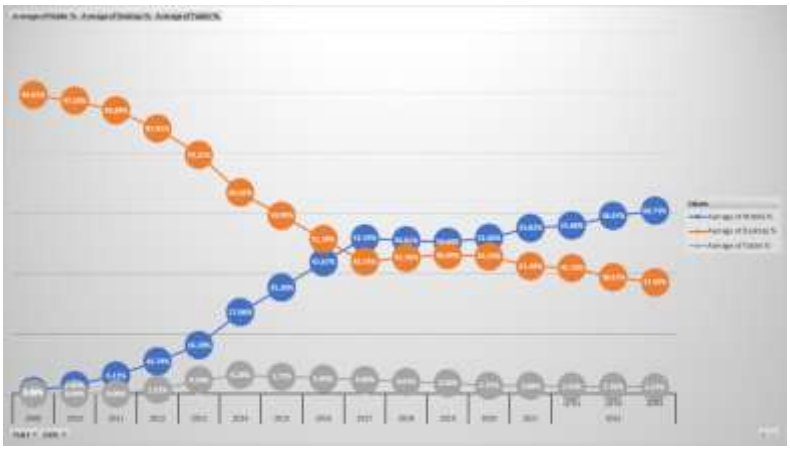


Fuente: Wikipedia "*Usage Share of Operating Systems*"

En 2017, por primera vez, se observa que el tráfico generado/consumido en internet es mayor desde dispositivos móviles que desde ordenadores de sobremesa.

[23] Empresa dedicada a explotar estadísticas de uso de internet.

Ilustración 2-3 Cuota de acceso a internet por tipo de dispositivo

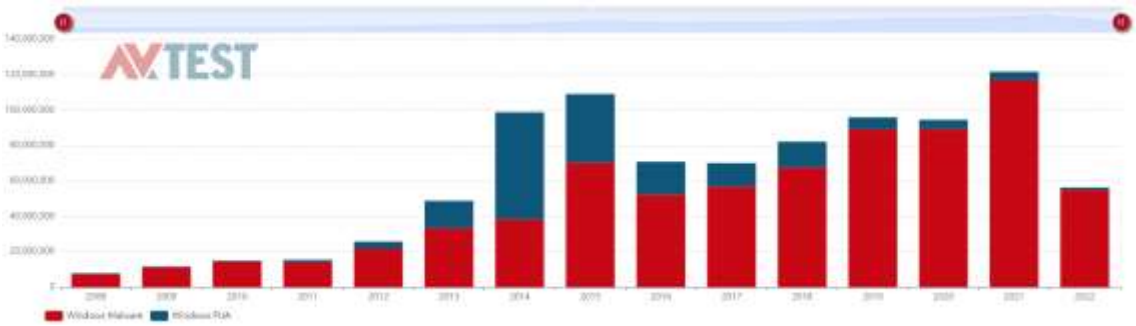


Fuente: Elaboración propia a partir de los datos de "*gs.statcounter.com*" a fecha de Agosto 2022.

En las siguientes ilustraciones se puede ver como después de la primera década del siglo XXI, el malware y programas potencialmente peligrosos detectados por año empieza la escalada a los niveles actuales. De los años 2013 a 2015 es cuando se ve la mayor diferencia respecto a los otros periodos y se ve un gran cambio en la tendencia en el sistema operativo Linux en los últimos dos años.

Windows al ser el claro dominante de la cuota del mercado de ordenadores de sobremesa desde los inicios de internet, es el principal objetivo de malware y programas potencialmente peligrosos. En 2013, se observa cómo, tanto MacOS cómo Android empiezan a despertar interés debido al incremento de los smartphones y la tendencia a usarlo justificado con los gráficos anteriores. Los atacantes tienen en cuenta este tipo de factores para llegar al máximo número de infecciones con el mínimo esfuerzo.

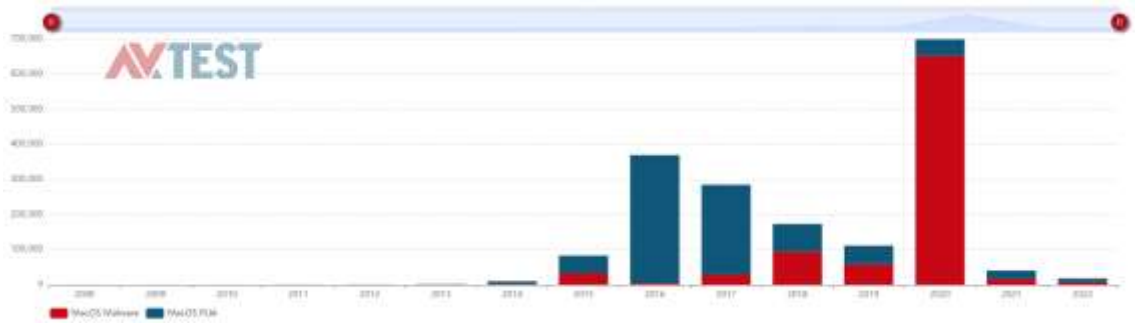
Ilustración 2-4 Cantidad detectada de malware y PUA[24] para Windows por años (*escala 140M*)



Fuente: The independent IT-Security Institute, "*AVTest, AVatlas*" (actualizado 31 de Agosto de 2022)

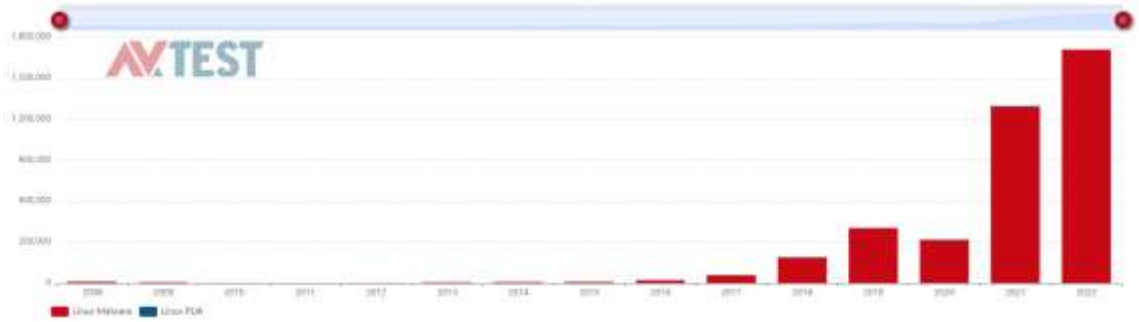
[24] PUA "Potentially Unwanted Application" son aquellas aplicaciones que se instalan de manera automática cuando se está instalando otro programa.

Ilustración 2-5 Cantidad detectada de malware y PUA para MacOS por años (*escala 700k*)



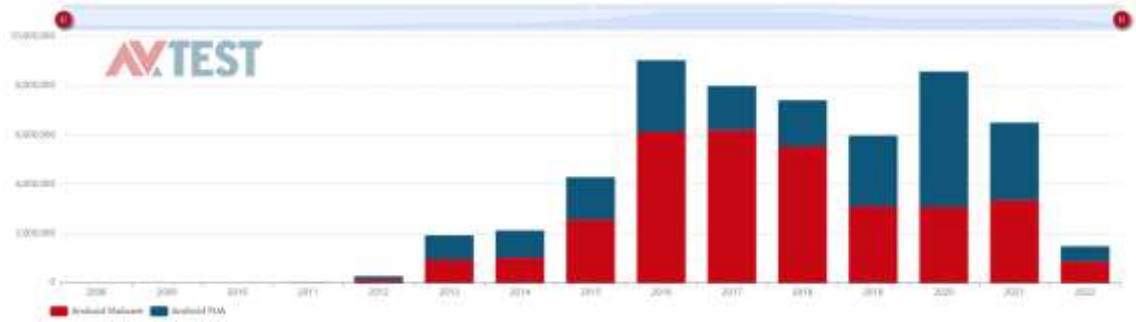
Fuente: The independent IT-Security Institute, "*AVTest, AVatlas*" (actualizado 31 de Agosto de 2022)

Ilustración 2-6 Cantidad detectada de malware y PUA para Linux por años (*escala 1.8M*)



Fuente: The independent IT-Security Institute, "*AVTest, AVatlas*" (actualizado 31 de Agosto de 2022)

Ilustración 2-7 Cantidad detectada de malware y PUA para Android por años (*escala 10M*)

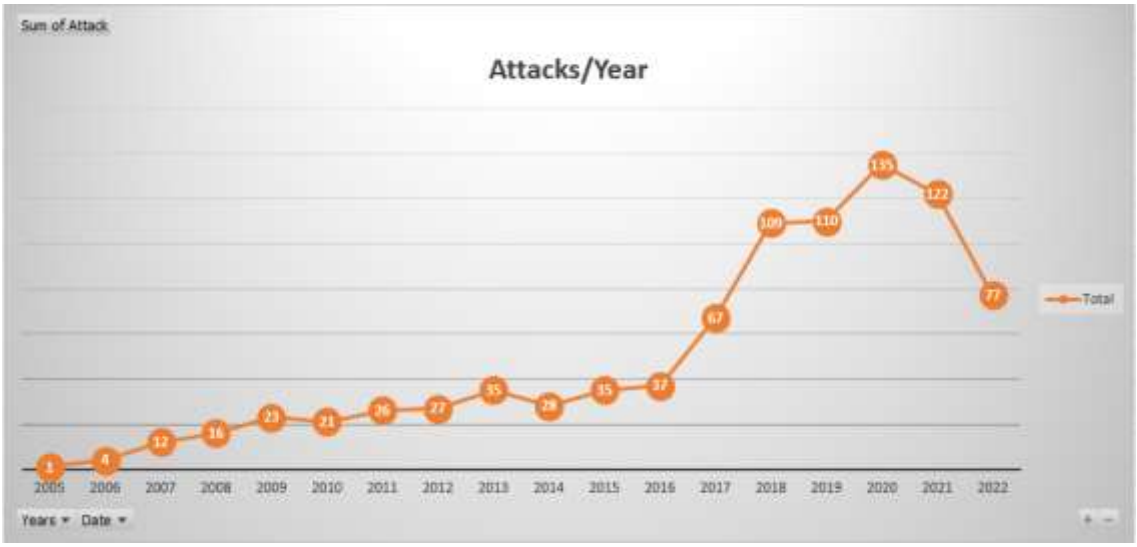


Fuente: The independent IT-Security Institute, "*AVTest, AVatlas*" (actualizado 31 de Agosto de 2022)

Fuera de los grandes números de malware y programas potencialmente peligrosos, el CSIS[25], desde 2006, hace un registro de los incidentes de seguridad dirigidos a agencias gubernamentales, de defensa, compañías de tecnología o crímenes económicos con pérdidas de más de un millón de dólares:

Es en 2017 donde vemos el primer salto casi doblando el número de incidentes graves respecto al anterior, y ahí se dispara. Lo que llevamos de año ya tienen registrado casi tantos incidentes como en 2017.

Ilustración 2-8 Número de incidentes de seguridad significantes registrados hasta la fecha



Fuente: Elaboración propia a partir del registro de CSIS "*Significant Cyber Incidents*" a fecha de 31 de agosto de 2022.

2.5. Regulaciones

Desde que las empresas almacenan datos, ha existido la voluntad de obtener dichos datos de manera ilícita, como por ejemplo accediendo a informes médicos en papel sin autorización, o fotocopiando documentos restringidos.

Según un estudio de IDC[26], se calculaba en 2018 que el volumen de datos generados digitalmente en el 2025 será de 175 Zettabytes[27], esto serían mil millones de Terabytes, o lo que sería lo mismo, el espacio de datos que se podrían guardar en dos mil millones de Iphones 11 Pro Max de 512GB de capacidad. Actualmente, en 2021, se calcula que se llegaron a generar 79 Zettabytes según "statista.com".

[25] CSIS, "Center for Strategic & International Studies", organización sin ánimo de lucro dedicada a la investigación de políticas que sirvan para abordar los retos más grandes del mundo.
[26] IDC "International Data Corporation", proveedor de servicios y analistas para ayuda en la toma de decisiones de IT para alinearse con los objetivos del negocio.
[27] Zettabytes, unidad de medida de la información, son 10^{15} MegaBytes.

A finales de siglo XX se empieza a ver un cambio de tendencia respecto a las grandes inversiones y se empieza a hablar del concepto ESG ("*Environmental, Social and Governance*"). Se va creando una concienciación en 3 pilares, el Medioambiental, el Social y el un buen Gobierno de las compañías. Esto, junto con la concienciación a nivel mundial sobre el cambio climático y la importancia de ser cada vez más sostenibles, hace que la digitalización sea desde hace unos años una de las prioridades de muchas empresas o gobiernos. En Europa existe el objetivo de ser neutral a nivel climático en 2050, o lo que es lo mismo, no emitir ningún gas de efecto invernadero.

E&Y[28], haciendo un análisis de las políticas de ESG, publicó un informe el 30 de abril de 2021 del marco regulatorio y sus posibles impactos. En él aparecía un gráfico comparando la cantidad de legislación que en los últimos diez años se han creado alrededor de ESG, y el número de iniciativas voluntarias.

Ilustración 2-9 Iniciativas legislativas y voluntarias relacionadas con ESG

Fuente: E&Y del informe de Datamaran, 2020

Toda esta presión legislativa y demandas de ir a un modelo de sociedad más respetuosa con el medio ambiente hace que si todavía quedaban empresas que no estuvieran dispuestas a pasar por un proceso de digitalización, no les quede más remedio que empezarlo y por tanto se tenga que dar más importancia a las regulaciones y legislaciones acerca de protección de datos.

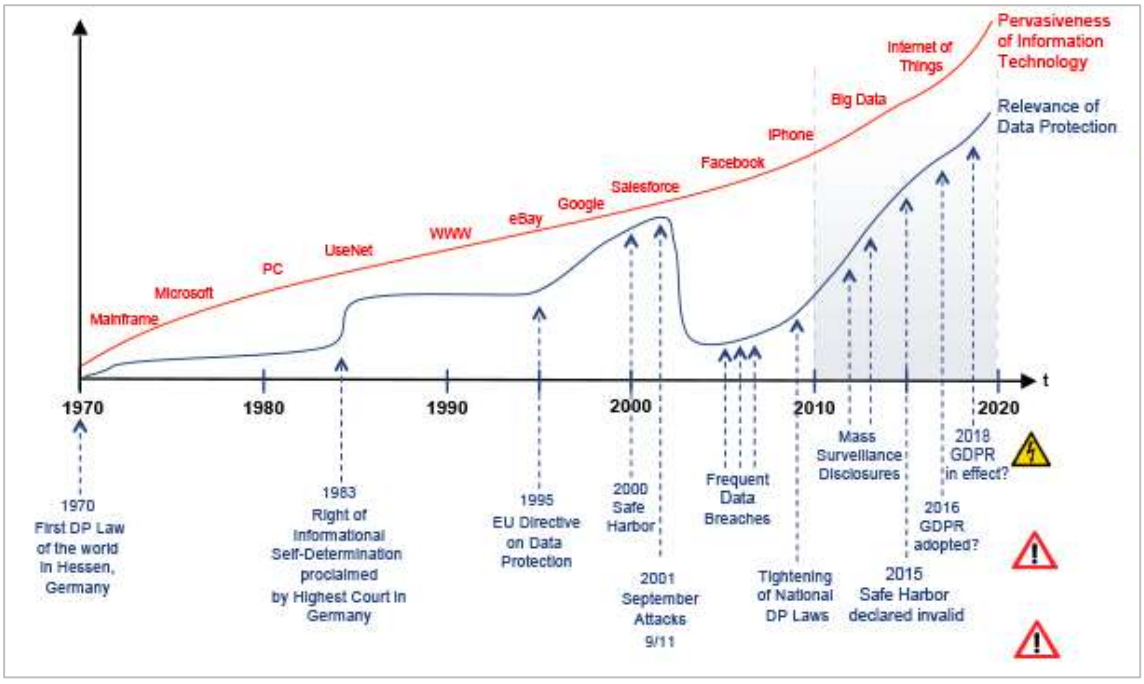
La primera regulación, en este sentido, se publicó en el estado de Hesse, Alemania, en 1970, llamada "Bundesdatenschutzgesetz". Es una ley federal de protección de datos que regula la exposición de datos personales que se tratan o almacenan en sistemas informáticos.

[28] E&Y "Ernst and Young" una de las 4 grandes firmas de contabilidad a nivel mundial.

En Estados Unidos se adoptó el "CFAA"[29] en 1986, como añadido a la ley de control del crimen ("CCCA"[30]) del 1984, prohibiendo el acceso no autorizado explícitamente o en exceso de autorización.

En 1995 la unión europea sacó su propia regulación con la directiva de protección de datos que fue sustituida en 2016 por las directivas 2016/679 (GDPR[31]) y 2016/280. La primera hace referencia a la protección del tratamiento de los datos personales y su libre circulación, y la segunda hace referencia a la protección de las personas físicas respecto al tratamiento de sus datos desde las autoridades competentes.

Ilustración 2-10 Evolución de legislaciones sobre protección de datos a nivel europeo



Wilhelm, A brief history of the General Data Protection Regulation, 2016

En nuestro sector existe un organismo europeo de control que se llama EIOPA[32]. Es un organismo supervisor de las compañías de seguros y pensiones profesionales, con el objetivo de dar estabilidad y confianza al mercado asegurador y de pensiones. Este organismo, en octubre de 2020 publicó unas pautas específicas para las ICT[33] que dan servicio o se integra en el sector asegurador y reasegurador. Estas pautas orientan al sector de cómo aplicar las directivas de Solvencia II (2009/138/CE) y al reglamento delegado de la comisión europea (2015/2356) en el contexto de seguridad y gobierno de las TIC. Estas pau-

[29] CFAA "Computer Fraud and Abuse Act"
[30] CCCA "Comprehensive Crime Control Act"
[31] GDPR "General Data Protection Regulation"
[32] EIOPA "**E**uropean **I**nsurance and **O**ccupational **P**ensions **A**uthority"
[33] ICT "**I**nformation and **C**ommunication **T**echnology" o TIC ("**T**ecnologías de la **i**nformación y la **c**omunicación") en castellano.

tas persiguen clarificar la información mínima y las capacidades de ciberseguridad que ha de tener el sector, evitar un arbitraje regulatorio y fomentar la convergencia supervisora de las expectativas y procesos aplicables en relación con la seguridad y el gobierno de las TIC como clave para una correcta gestión de riesgos.

En septiembre de 2020, la comisión europea publica un borrador sobre la resiliencia operativa digital del sector financiero modificando reglamentos previos, se le conoce como DORA por sus siglas de su nombre en inglés "***D**igital **O**perational **R**esilience **A**ct*". Es una iniciativa legislativa encargada de establecer unas bases claras de cara a los reguladores y supervisores financieros de la UE y se enfoca a asegurar la resiliencia de operaciones a partir de una interrupción operativa grave. Las partes más destacadas de esta proposición serían:

- Incorporación de los CTPP[34] incluidos los CSP[35] al perímetro de regulación, de manera quede definido y certero lo que es permisible o no y el nivel de seguridad de los activos de las compañías del sector financiero en la nube. Este marco también puede ayudar a aumentar el número de compañías que hagan transición de algunos de sus servicios a este tipo de entornos.

- Pruebas de resiliencia digital operativa:

    - Ampliación de aplicación, ya que se van a crear nuevos criterios para definir la obligatoriedad de que compañías deben pasar pruebas de resiliencia digital operativa, por tanto, compañías que hasta ahora no lo tenían como obligado, tendrán que empezar a hacer pruebas de penetración de la infraestructura con terceros o redefinir la gestión de riesgos y planificaciones contando con estas.

    - Estandarización de las pruebas, basadas en el marco voluntario TIBER-EU[36]. Se está trabajando para crear un conjunto de pruebas estándar reconocido por todos los estados miembros de manera que las compañías no tengan que repetir pruebas dependiendo de en qué estado abran líneas de negocio. Las compañías que actualmente ya estén pasando este tipo de pruebas y ya tengan líneas de negocio en diferentes estados de la UE, podrían ver

[34] CTPP "**C**ritical **T**hird **P**arty **P**roviders" de ICT "**I**nformation and **C**ommunications **T**echonology", o lo que es lo mismo los proveedores críticos de servicios de comunicaciones o información.

[35] CSP "**C**loud **S**ervice **P**roviders"

[36] TIBER-EU "**T**hreat **I**ntelligence-**B**ased **E**thical **R**ed **T**eaming – **Eu**rope". Es un framework de trabajo para entidades financieras que define técnicas y procedimientos para poder crear equipos que mimeticen las técnicas que usarían atacantes reales (este tipo de equipos también son conocidos como "***Red Team***"). Este framework y equipos ayudan a las compañías a evaluar su estado de madurez de protección, detección y respuesta respecto a incidentes de este tipo.

como se rebajan los costes al no tener duplicidades, pudiendo centralizar y optimizarlas.

- Centralizar y armonizar la clasificación y notificación de incidentes TIC. Se definirán unas plantillas de notificación estándar para las entidades financieras, y se concretarán los criterios en los que se debe o no notificar de este tipo de incidentes (marco temporal de notificación, umbrales, multas, requisitos). DORA no sustituirá los canales actuales de comunicación de incidentes tipo GDPR. Las notificaciones se harán a las autoridades competentes nacionales, pero con el tiempo se plantea que pueda haber un punto único dentro de la UE de manera que se pueda racionalizar la recogida de información, una mejor supervisión, mejores informes, etc.

- Armonización de las normas de gestión de riesgos que se organiza alrededor de los pilares de "Identificar", "Proteger y Prevenir", "Detección" y ahora se hará especialmente énfasis en el de desarrollar estrategias y planes de "Respuesta y recuperación", incluida la comunicación con las partes interesadas, incluidos los clientes. Se da también mucha importancia al consejo de administración dado que tienen que definir cuál es la tolerancia al riesgo de la compañía en cuestión y revisar los planes de continuidad y recuperación.

En mayo de 2022, se ha publicado una nota de prensa del consejo europeo en el que comunican que se ha llegado a un acuerdo provisional respecto a la tramitación de DORA debido al creciente riesgo de ciberataques. En este acuerdo se destacan varios puntos:

- Los CSP deberán establecer filiales dentro de la UE.
- Las pruebas de penetración podrán incluir autoridades competentes de diferentes miembros de la UE.
- Se aclararán las reglas que tendrán que dar cumplimiento de la directiva NIS[37]
- Creación de una red de supervisión adicional para coordinar a las diferentes autoridades de supervisión europeas de manera transversal.

Este acuerdo provisional, está sujeto a la aprobación por del consejo y parlamento europeo antes de pasar por el procedimiento formal de adopción. Una vez aprobada la Directiva, tanto las autoridades europeas de supervisión, o ESAs[38], como EIOPA desarrollarán los estándares técnicos a cumplir y trasladarán la responsabilidad de supervisar a las autoridades nacionales competentes, en el caso de España seguramente la DGSFP[39].

[37] NIS "**N**etwork and **I**nformation **S**ecurity", como es conocida la directiva europea 2016/1148
[38] ESAs "**E**uropean **S**upervisory **A**uthorities"
[39] DGSFP "**D**irección **G**eneral de **S**eguros y **F**ondos de **P**ensiones"

2.6. Estándares de seguridad

Con el afán de poder crear un marco de herramientas, procedimientos y guías de seguridad para reducir los riesgos de estar expuesto a ciber ataques, existen una serie de estándares a nivel mundial que hacen referencia a los propios usuarios, redes, dispositivos, software, procesos, información almacenada o en tránsito, aplicaciones, servicios y sistemas que están conectadas directa o indirectamente a cualquier red (ya sea privada o pública).

ISO[40] actualmente tiene varios estándares que se han desarrollado en relación con la seguridad, pero de diferentes ámbitos. En la referencia a la confidencialidad de los datos que tratan las compañías, la disponibilidad o la integridad de estos, estaríamos hablando de la ISO/IEC[41] 27001 y ISO/IEC 27002, su última revisión/versión es de octubre de 2013. Además, existe la ISO 22301, revisión de 2019, en la que se especifican los requerimientos de implantar, mantener y mejorar los sistemas de administración para prepararse, responder, protegerse y reducir la probabilidad de interrupciones de negocio cuando ocurran.

Además de estas dos existe la ISO/IEC 15408 dedicada para dar unas pautas comunes de cara a integrar y testear tanto software como hardware de una manera segura.

Para lo relacionado con vehículos autónomos, se está desarrollando la ISO/SAE[42] 21434, se publicó en agosto de 2021 con lo que es bastante reciente.

Existe también un estándar de cara a IoT que se publicó en 2020, es el ETSI 303 645. Establece las líneas base de requerimientos de seguridad en el consumo de los dispositivos de IoT, así como controles técnicos y políticas para desarrolladores y fabricantes. A destacar que para este tipo de dispositivos son especialmente “golosos” para los ciber atacantes ya que hasta la fecha suelen venir con contraseñas por defecto que nadie cambia y los hace una plataforma ideal para convertir en una BotNet.

En la UE existe la directiva NIS, transpuesta en España vía Real decreto ley en 2018, y desarrollada en el real decreto 43/2021. La transposición acaba modificando el “Esquema Nacional de Seguridad” o ENS creado en 2010 y modificado por última vez en mayo 2022 a través del Real Decreto 311/2022.

La directiva NIS y, en consecuencia, el ENS, están enfocados a fortalecer las capacidades de defensa frente a ciber-amenazas en el ámbito público y de las

[40] ISO “**I**nternational **O**rganization for **S**tandardization”, organización mundial que trata de aunar expertos de todo el mundo para crear estándares para cualquier ámbito de aplicación internacional.
[41] IEC “**I**nternational **E**lectrotechnical **C**omission”, comisión que se encarga de crear estándares para cualquier tecnología relacionada con electrónica o electricidad.
[42] SAE “**S**ociety of **A**utomotive **E**ngineers”, asociación de profesionales de empresas aeroespaciales, automotrices y de vehículos comerciales.

entidades que están vinculadas vía servicios o similares a esta administración pública.

La última modificación del ENS establece un plazo de 24 meses para que los sistemas de información alcancen su plena adecuación. Al crearse ENS en 2010 se establecieron 3 principios básicos en los que se debe trabajar relativos a la seguridad, estos son “Prevención”, “Reacción” y “Recuperación”. Con la nueva actualización se ha variado un poco pasando a “**Prevención**”, “**Detección**”, “**Respuesta**” y “**Conservación**”, introduciendo el concepto de vigilancia continua. Además, se pasa de un mínimo de "seguridad por defecto" en cualquier sistema, a “**mínimo privilegio**”, de manera que se pone énfasis en asegurar el control de acceso a cualquier sistema otorgando siempre el nivel de permisos adecuado y no más. Se han añadido 3 disposiciones en las que se establece que:

- CCN[43] y INAP[44] desarrollarán nuevos programas de sensibilización, concienciación y formación dirigidos al personal de entidades del sector público. El CCN-CERT será el coordinador a nivel estatal de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática.
- Desarrollo de instrucciones técnicas de ciberseguridad armonizadas con la UE
- Respecto de principio de “No causar un perjuicio significativo” al medioambiente.

Se incorporan nuevas medidas de seguridad como se puede ver en el extracto de la infografía publicada por el propio CCN:

Ilustración 2-11 Nuevas medidas de seguridad del nuevo ENS

Fuente: CCN, infografía *“Cambios clave 2022”* (*https://ens.ccn.cni.es/es/docman/documentos-publicos/865-infografia-ens-novedades-rd/file)*

[43] CCN “**C**entro **C**riptológico **N**acional”
[44] INAP “**I**nstituto **N**acional de **A**dministración **P**ública”

Analizando el texto del Real Decreto 311/2022 del nuevo ENS respecto las nuevas medidas:

- **Op.nub.1**: Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir las medidas de seguridad en función del servicio que presten definidas en las guías de CCN-STIC que sean de aplicación. Los servicios informáticos que soporten este servicio en la nube deberán ser conformes con el ENS o cumplir con las medidas de auditoría de penetración (o pentesting), transparencia, cifrado y gestión de claves y jurisdicción de datos. Además, los servicios certificados deberán serlo bajo una metodología reconocida.

- **Op.ext.4**: Define la interconexión al establecimiento de enlaces con otros sistemas de información para el intercambio de información y servicios, en los que no se podrán establecer sin autorización previa, se considera no permitido por defecto. Cada documentación deberá estar documentada explícitamente (características interfaz, requisitos seguridad, protección de datos y la naturaleza de la información intercambiada). La interconexión de sistemas en los que la identificación, autentificación y autorización tengan lugar en diferentes dominios de seguridad y diferentes responsabilidades, se deberán coordinar las medidas de seguridad responsabilizando en cada sistema.

- **Op.cont.4**: Se define la disponibilidad de medios alternativos para poder prestar servicio cuando los medios habituales no estén disponibles. Estos medios alternativos deberán cubrir los servicios contratados a terceros, instalaciones alternativas, personal alternativo, equipamiento informático alternativo y medios de comunicación alternativos. Estableciendo un tiempo máximo para que estos entren en funcionamiento. Estarán sometidos a las mismas garantías de seguridad que los habituales.

- **Op.mon.3**: Dentro de las medidas de monitorización y auto ejecución de acciones predeterminadas dependiendo de la matriz de riesgos (creación de alarmas, inhabilitación de servicios, otros) se incluye un nuevo elemento por el que se pide un sistema de recolección automática de todos los eventos de seguridad, a ser posible que pueda correlacionarlos. Además, se insta a disponer de soluciones de vigilancia avanzada que puedan determinar superficie de exposición, amenazas avanzadas (APT[45]). Se aplicarán también medidas para prevenir, detectar y reaccionar frente a intentos de minería de datos, se harán inspecciones de seguridad periódicas y en las interconexiones que lo requieran se aplicarán controles en el flujo de intercambios de información.

- **Mp.eq.4**: Se refiere a los “otros dispositivos conectados a la red” a aquellos estilo **multifunción** (impresoras, escáneres, otros), **multimedia**

[45] APT “**A**dvanced **P**ersistent **T**hread”

(proyectos, altavoces inteligentes, otros), **IoT**, **BYOD**[46], para definir los mínimos de seguridad que deben cumplir, como por ejemplo, disponer de funcionalidad para eliminar información de su memorias, se han de usar productos certificados en la medida de lo posible haciendo referencia a la propia norma, y se deberá hacer uso de soluciones que permitan visualizar los dispositivos presentes en la red, controlando su conexión y desconexión así como verificar su configuración de seguridad.

También es muy conocido el estándar de seguridad americano, promovido por NIST, al que se hace referencia como "*NIST CSF*"[47]. Además de este framework, hay diferentes publicaciones relacionadas que hablan sobre gestión de riesgos, controles de seguridad y privacidad para información federal, guías de identidad digital, u otros.

La última versión de "*NIST CSF*" es la v1.1, de abril de 2018. Este framework organiza la ciberseguridad en 5 fases:

- **Identificación**: En esta fase se deberían identificar los procesos y activos más críticos de una compañía. Aquellos imprescindibles para que la actividad de esta pueda seguir llevándose a cabo. Aquí se tiene que documentar los flujos de información, dónde se guardan los datos, se ha de mantener un inventario de software y hardware, establecer políticas de ciberseguridad para definir roles y responsabilidades de estos roles y definir la gestión de riesgos que se quiere realizar respecto a todo ello.

- **Protección:** Asegurar el acceso restringido a los recursos de la compañía, así como a sus datos. Proteger los datos sensibles encriptándolos, tanto cuando se almacenan en localmente como cuando se envían. Asegurar un backup regular y protegido de manera que no se pueda acceder a este. Proteger los dispositivos con barreras como antivirus y firewalls, configurándolos de manera uniforme y con una política que deshabilite opciones no necesarias. Actualizar los dispositivos y los sistemas operativos de manera regular para evitar que vulnerabilidades conocidas les pueda afectar. Formación a los usuarios para que sean capaces de detectar situaciones maliciosas.

- **Detección:** Desarrollar procesos para testear posibles acciones o entidades no autorizadas, incluidas las actividades de personal. Activar y mantener los logs de los sistemas de seguridad, así como de los dispositivos para poder explotarlos y detectar anomalías y, en la medida de lo posible, centralizarlos y usar herramientas automáticas de detección de dichas anomalías. Aplicar inteligencia a estos sistemas de manera que, si sabemos que flujos de datos se deberían estar dando, se puedan detectar flujos no deseados más rápidos. Si se produce un evento catalo-

[46] BYOD "**B**ring **Y**our **O**wn **D**evice" dispositivos no controlados por la compañía o entidad a la que acaban conectándose.
[47] CSF "**C**yber**s**ecurity **F**ramework"

gado de ciberseguridad, actuar rápido para clasificarlo y ponderar el riesgo e impacto.

- **Respuesta:** Asegurarse que los planes de respuesta se han probado de manera regular para asegurar que todo el engranaje de personas y tecnología es conocedor de todo el proceso. Asegurarse que los planes están actualizados con las nuevas tecnologías que vayan añadiéndose al porfolio de la compañía como con nuevos flujos o necesidades de datos. Coordinación con personas clave tanto internas como externas.

- **Recuperación:** Seguir con la coordinación de las personas clave tanto internas como externas. Actualizar los planes una vez superado el evento con lo aprendido en la experiencia. Controlar las relaciones públicas y reputación de la compañía de una manera ordenada y no reactiva.

2.7. Objetivos de las regulaciones y los estándares de seguridad

Los estándares de seguridad y las regulaciones tienen, entre otros, los siguientes objetivos:

- Dar un marco de confianza tanto a los clientes del sector privado cuando se dirigen a sus compañías, como a los ciudadanos cuando se dirigen con las nuevas tecnologías a la administración pública.

- Introducir elementos y metodologías comunes de manera que sea fácil reconocer y comparar el estado de seguridad de cualquier sector.

- Establecer y estandarizar canales de comunicación y supervisión comunes.

- Promover la gestión continua de la seguridad dada la rapidez de aparición de nuevas tecnologías o riesgos no contemplados.

- Promover la prevención, detección, la respuesta y la conservación para mejorar la resiliencia ante ciberataques y ciberamenazas.

- Centralizar gestión de comunicados y informes para su estandarización y análisis.

- Proteger la información

3. Ciclo de vida de la ciberseguridad

3.1. ¿Qué es un incidente/evento de seguridad?

Al igual de lo que ocurría al intentar definir que es un ciberataque cuesta encontrar una definición única de lo que es un incidente/evento de seguridad. Podríamos pensar que está relacionado con la tecnología, pero los métodos usados para poder ocasionar uno, o para evitarlo, no tienen por qué tener esa relación (por ejemplo: política de mesas limpias para evitar tener información sensible accesible sin control). Ejemplos de lo que se podría considerar un incidente de seguridad:

- Accesos a sistemas o a datos de manera no autorizada.
- Uso de sistemas ajenos de manera no autorizada.
- Distribución de datos no autorizados.
- Modificación de elementos de dispositivos como su software o firmware de manera no autorizada.
- Ataques con la finalidad de dejar sin servicio.

NIST lo define[48] de estas dos maneras:

> "***A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery***."
>
> (traducción al castellano: "*Un evento de ciberseguridad que se ha determinado con un impacto en la organización y que provoca la necesidad de respuesta y recuperación*")
>
> "***An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies***."
>
> (traducción al castellano: "*Un evento que o bien, pone en peligro de manera real o inminente, sin autorización legal, la integridad, la confidencialidad, o la disponibilidad de la información o de un sistema de información; o bien constituye una violación o una amenaza inminente en la violación de la ley, las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptables.*")

[48] https://csrc.nist.gov/glossary/term/cybersecurity_incident

3.2. ¿Qué es la ciberseguridad? ¿Cuál es su labor?

Según el glosario de NIST, la ciberseguridad[49] se define como:

> "***The ability to protect or defend the use of cyberspace from cyber-attacks***"
>
> (traducción al castellano: "*La habilidad de proteger o defender el uso del ciberespacio de ciberataques*")

NIST, además, tiene hasta cuatro definiciones de ciberespacio[50], destaco la más genérica:

> "***A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.***"
>
> (traducción al castellano: "*Un dominio global dentro del entorno de la información consistente en una red interdependiente de infraestructuras de sistemas de información que incluyen internet, redes de telecomunicaciones, sistemas informáticos y, procesadores y controladores integrados*")

Por tanto, NIST define la ciberseguridad como la habilidad de proteger y defender una red de dispositivos conectados entre sí a su propia red y a su vez a internet.

En la orden PCI/487/2019 publicada en el BOE el 30 de abril de 2019, se definen también lo que es el ciberespacio y cuál es el propósito de la ciberseguridad desde el punto de vista del gobierno.

En el capítulo 1 se hace una definición extensa del ciberespacio, sus oportunidades y sus desafíos. Lo definen como un espacio común global, con ausencia de soberanía, jurisdicción débil, y con una facilidad de acceso y conexión universal que facilita el libre flujo de información, servicios e ideas. Es un espacio virtual pero que se sustenta en elementos físicos y lógicos, expuestos a disfunciones o u acciones deliberadas con fines mal intencionados, exponiendo así una serie de riesgos, que normalmente se incrementan al tratarse de elementos que están desplegados por criterios comerciales y no de seguridad. Todos estos elementos interconectados entre sí para dar estos servicios y permitir el libre flujo de información definirían el ciberespacio. Se destaca que esta interconexión de estos dispositivos/servicios/elementos, pueden originar efectos en cascada con relación a eventos de seguridad con resultados impredecibles.

En el capítulo 3 se fija el propósito, principios y objetivos de la estrategia del gobierno nivel nacional de la ciberseguridad. Aquí hacen referencia a la Estrategia de Seguridad Nacional definida en 2017:

---

[49] https://csrc.nist.gov/glossary/term/cyber_security
[50] https://csrc.nist.gov/glossary/term/cyberspace

> "***garantizar un uso seguro y responsable de las redes y los sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para un contribuir a la promoción de un ciberespacio seguro y fiable***"

Como se puede ver, hablan de 3 pilares que definía en su primera versión el ENS comentado anteriormente, "**Prevención, detección y respuesta**", a los que habían añadido en la revisión del 2022 el de "**Conservación**", en la línea, el Departamento de Seguridad Nacional, en la publicación de 2021 de la Estrategia de Seguridad Nacional, al hablar de ciberespacio también los menciona:

> ***"Ciberespacio, En términos de ciberseguridad, se requiere garantizar el uso seguro y fiable del ciberespacio, para proteger los derechos y las libertades de los ciudadanos y promover el progreso socio económico. Para ello es importante incrementar las capacidades (tecnológicas, humanas y económicas) de la ciberseguridad nacional dirigidas a la prevención, detección, respuesta, recuperación, investigación y defensa activa"***

Ya no se habla tan solo de esos 3 pilares, sino también de "**Recuperación, Investigación y Defensa Activa**". De estos 3 mencionados por Defensa, los dos primeros podrían englobarse en el pilar de "Respuesta", y el tercero, el de defensa activa, estaría entre prevención, y conservación. Así que intrínsecamente define la ciberseguridad en base a los 4 pilares del ENS.

Por tanto, podemos ver la ciberseguridad como un conjunto de acciones, protocolos, metodologías o elementos, que engloban todas las medidas para tener en cuenta, y para tomar, tanto previas como posteriores, a un incidente/evento de seguridad.

Los beneficios de la ciberseguridad pueden ser muchos, pero podemos enumerar algunos:

- Alinear la seguridad tecnológica con las necesidades de negocio.
- Asegurar al máximo la continuidad de negocio.
- Tener planes de respuesta definidos para que cuando ocurra algún incidente la reacción esté dentro de los parámetros establecidos.
- Dar visibilidad con métricas del nivel de exposición y intentos al que se está expuesto.

3.2.1. Previo a un incidente: Prevención, protección y detección

En la ciberseguridad se ha de partir de la base en que siempre se va un paso atrás respecto a cualquier incidente, es decir, como comentábamos en la introducción, lo importante no es si va a ocurrir, sino cuando va a ocurrir.

Así que debemos hacer un trabajo previo a dicho incidente no hipotético. Éste trabajo además es "infinito", es decir, siempre se ha de reevaluar y reajustar con el paso del tiempo, así que es importante marcar en los proyectos estratégicos esta revisión ya que las medidas, planes, protocolos tomados en el pasa-

do no aseguran una mitigación/prevención futura. Esto es así dado a que las tecnologías, las técnicas usadas, las vulnerabilidades, etc. evolucionan con el tiempo. La ley de Moore[51], establece que la tecnología dobla su capacidad de procesamiento cada 2 años, cosa que favorece este entorno cambiante al dar posibilidad a usar técnicas antes impensables por falta de procesamiento de cálculo, permitiendo una evolución cada vez más rápida.

En esta fase de prevención, protección y detección, debemos ser capaces de:

- Decidir que exposición al riesgo se debe tener.
- Identificar todos los activos susceptibles de ser protegidos (datos, servidores, redes, oficinas, otros).
- Idear estrategias de protección a estos activos (antivirus, backups, hardening[52], otros).
- Idear estrategias de respuesta a incidentes (planes de recuperación, planes de continuidad de negocio, otros).
- Probar estas estrategias (pruebas anuales).
- Poner a prueba el sistema (pentestings).
- Tener sistemas de monitorización de la seguridad.
- Tener un equipo de respuesta de incidentes.

La prevención y la protección han de centrarse en la disuasión o reducción de la superficie de exposición y debe eliminar o reducir la posibilidad de que una amenaza llegue a materializarse.

La detección ha de centrarse en las medidas que sean necesarias para poder tener sistemas de monitorización capaces de detectar que se está produciendo un evento de seguridad no deseado.

3.2.2. Posterior a un incidente: Respuesta y Conservación

Es tan importante la fase previa a un incidente como la posterior. En esta fase el incidente ya se ha producido, y es cuando se tienen que poner a prueba todo lo ideado y ensayado en la primera.

En esta fase deberíamos ser capaces de, a través de los planes preestablecidos:

- Dar continuidad a negocio en el menor tiempo posible.
- Analizar y detectar la gravedad del incidente.
- Identificar las causas de este.
- Limpiar y arreglar los efectos causados.
- Informar a las autoridades en caso de necesidad y dependiendo de los datos implicados o expuestos en el incidente.

[51] Gordon E. Moore, cofundador de Intel, fabricante de procesadores de cómputo.

[52] Hardening, técnicas de ciberseguridad destinadas a poner difícil al atacante conseguir sus objetivos

- Hacer una buena gestión de las comunicaciones públicas e informar a los clientes en caso de necesidad.
- Restaurar todos los datos que se hayan perdido o estén comprometidos.
- Restablecer la normalidad de operaciones.
- Revisión del incidente para readaptar planes y protocolos adoptando así un proceso de mejora continua en seguridad.

En el Capítulo II artículo 8 del Esquema Nacional de Seguridad hacen mención explícita a la continuidad de negocio y a la conservación y restauración de los datos:

> "***Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.***"
>
> "***El sistema de información garantizará la conservación de los datos e información en soporte electrónico.***"
>
> "***El sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital.***"

3.3. Las nuevas tecnologías al servicio de la Ciberseguridad

La evolución de la tecnología también llega al campo de la ciberseguridad, donde pueden ser un gran factor diferencial hoy en día para asegurar una buena prevención y rápida detección en caso de sufrir un incidente.

Dentro de estas nuevas tecnologías, o tendencias, tenemos:

- ***Inteligencia artificial (IA) y el "Deep Learning"***[53]. Usar la inteligencia artificial y deep learning con el objetivo de procesar infinidad de registros de los diferentes sistemas o elementos de la red de manera que se puedan detectar "agujas en un pajar".

- ***Analítica de comportamiento.*** También conocida como "Behavioral Analytics", esta técnica se encarga de analizar comportamientos habituales de los sistemas y los usuarios, siendo capaz de detectar cambios en dichos comportamientos. Por ejemplo, sería capaz de detectar que un usuario ha intentado acceder a un sistema al que no acostumbra a acceder, o que el acceso se ha producido en un horario no habitual. De esta manera lanzar una alerta para su análisis y una acción automática que realice alguna acción predeterminada.

[53] Tipo de "Machine Learning" en el que se hace uso de redes neuronales artificiales diseñado para poder analizar grandes cantidades de datos de una manera más eficiente y rápida.

- ***Hardware específico de encriptación.*** Para proteger el acceso a los ordenadores y a sus archivos cifrados, los equipos de sobremesa actuales llevan un procesador específico (TPM[54]) según la ISO/IEC 11889 para sistemas operativos Windows y Linux.

- ***Técnicas de blockchain***. Blockchain es una tecnología de firma descentralizada basada en bloques encadenados. Esto significa que una vez has realizado una operación se genera un bloque con una marca de tiempo (o timestamp) concreta y se relaciona con los bloques anteriores, de manera que para modificar un bloque se tendrían que modificar todas los demás. Se puede usar para asegurar comunicaciones o acceso a sistemas lícitos, también para firmar datos de manera que se sepa que no han sido modificados.

- ***Filosofías Zero-Trust***. La filosofía zero-trust parte de la base que nuestros sistemas no son de confianza, con lo que se ha de construir toda la seguridad y acceso etc a partir de esta desconfianza y por tanto verificando toda transacción o similares. También es conocida como seguridad sin perímetros, en contraposición a la filosofía tradicional de pensar que si se está dentro del perímetro de una red corporativa se está seguro.
- ***EDR***[55]***.*** Son los nuevos "Antivirus", se basan en analizar constantemente toda actividad del sistema (incluida la red) para poder aplicar luego las tecnologías de "*Analítica de comportamiento*"[56] o de "*Deep Learning*".

- ***Thread Intelligence***. Son técnicas que se basan en recolección de datos, procesarlos y analizarlos para identificar posibles motivaciones de los ataques, objetivos y comportamientos de los ataques. De esta manera dar visibilidad y conocimiento para adoptar medidas en base a conocimiento y no suposiciones para mitigación, pasando de aproximaciones reactivas a proactivas.

Estas son una muestra, no exhaustiva, de las nuevas tendencias en las que se está trabajando desde el punto de vista de la defensa de los sistemas, pero los ciberdelincuentes no se han quedado atrás, y también hacen uso de las nuevas tecnologías para tener mejor éxito en sus ataques. Con IA o ML[57] por ejemplo pueden calcular y orquestar ataques, coordinar BotNets para hacerlas más eficientes, pueden saber cuándo corren riesgo de ser detectados. Hacen uso del procesamiento natural del lenguaje que se está usando hoy en día para las interacciones robotizadas con los clientes para hacerlas más humanas, pero para redactar correos o incluso publicando un Chat Bot[58] para emular un servicio de atención al cliente con el que engañar a sus objetivos.

---

[54] TPM "Trusted Platform Module"

[55] EDR "**E**ndpoint **D**etection and **R**esponse"

[56] Analíticas de comportamiento o también conocidas como "Behavioral Analytics"

[57] ML "**M**achine **L**earning", similar al Deep Learning, dotar de herramientas a los algoritmos para que se adapten según condiciones que van aprendiendo dinámicamente.

[58] Chat Bot, sistema automático de respuesta basado en texto con el que una persona puede interactuar, típicamente para resolver dudas.

4. Prevenir. Disuadir. Responder

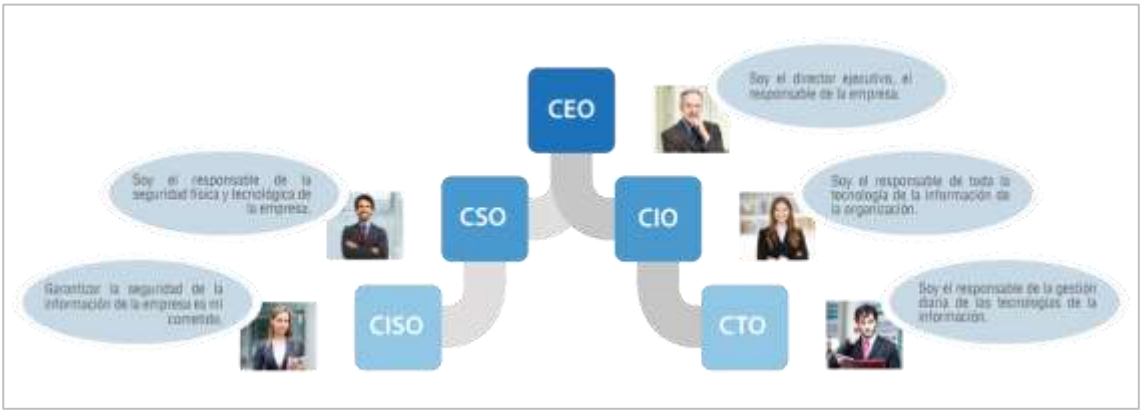
4.1. Adoptar y planificar la ciberseguridad

La ciberseguridad ha de adoptarse en todas las áreas de una compañía. Cualquier proceso tiene que diseñarse para su cometido, pero también entorno a la seguridad, desde el primer momento.

Los efectos de no tener un enfoque global de adopción de seguridad en todas las áreas de la compañía pueden afectar tanto a la compañía como a sus empleados ya que la afectación puede ser grave. En 2019 la compañía inglesa de Telemarketing "The Heritage Company" despidió a 300 empleados cerrando sus puertas por un ataque de ransomware.

La adopción de la seguridad como pilar de desarrollo de negocio no es viable sin una planificación. Esto es un cambio cultural para aquellas compañías que no se hayan planteado este pilar desde un inicio, además, el cambio, puede ser lento y encontrar reticencias. Por esto es imprescindible contar con la figura de un CISO[59]. El CISO es el responsable de la seguridad de la información, y no debería depender jerárquicamente de ninguna figura capaz de tomar decisiones en base a presupuesto o estratégicas de IT, ya que estas pueden primar otras prioridades y alejarse del análisis de la seguridad.

Ilustración 4-1 Organigrama de los principales roles en ciberseguridad



F

Fuente: Blog de INCIBE, "*CEO, CISO, CIO... ¿Roles en ciberseguridad?*"

Es importante la diferenciación de la rama del CSO[60] de la del CIO[61] para garantizar la independencia comentada respecto a decisiones en las que, solo el

[59] CISO "**C**hief **I**nformation **S**ecurity **O**fficer"
[60] CSO "**C**hief **S**ecurity **O**fficer"
[61] CIO "**C**hief **I**nformation **O**fficer"

CEO[62], pueda llegar a tomar una decisión contraria a las recomendaciones del CSO. Aunque incluso en esta situación, debería ser justificado y documentado.

Los beneficios de que el CISO cuelgue directamente del CSO y del CEO, según un artículo de James Carder[63], miembro del consejo de la revista Forbes, serían la comunicación directa de los riesgos potenciales a la organización, la mitigación de estos y capacidad de influenciar en todas las ramas de la organización para crear una mayor consciencia de seguridad. Para ello, recomienda estas mejores prácticas a seguir en esta comunicación:

- Alineación de la seguridad con las prioridades de negocio para asegurar un plan estratégico de seguridad alineado con las necesidades reales de la compañía.

- Comunicación proactiva de los riesgos de seguridad usando un lenguaje que la junta directiva pueda entender, intentando no crear miedo o incertidumbre, demostrando el ROI[64] del plan de ciberseguridad e ilustrando como tienen que ir de la mano los objetivos de negocio con los de seguridad.

- Colaborar para crear planes de respuesta efectivos para negocio en caso de incidente.

Alinear la ciberseguridad a negocio ayuda a crear planes efectivos y presupuestos útiles. Un riesgo que se corre en ciberseguridad es querer adoptar las últimas novedades y tendencias y, sin un plan preestablecido, puede suponer un gasto desmesurado. Si se hace así, además, el riesgo de que esa inversión no surja efecto y que se produzcan incidentes es mayor, y a futuro será difícil justificar nuevos gastos en este sentido.

En seguridad siempre existe el riesgo de que, a pesar de ir alineados, el presupuesto sea corto o justo, pero con lo anterior comentado, si hay comunicación con el CEO y la junta directiva, es más fácil mitigar ese riesgo.

Los beneficios de planificar la ciberseguridad, a parte de los comentados hasta ahora más referente a los presupuestos, podrían enumerarse en los siguientes:

- Reducción de riesgos de exposición de la empresa a incidentes de seguridad.
- Estar al día con las normativas a cumplir referente a la seguridad.
- Alineación de toda la compañía.
- Tener una metodología y un camino definidos para futuras revisiones.
- Reducción de costes futuros derivados de los incidentes de seguridad.

[62] CEO "**C**hief **E**xecutive **O**fficer"

[63] https://www.forbes.com/sites/forbestechcouncil/2021/09/08/why-your-ciso-should-report-directly-to-the-ceo/

[64] ROI "**R**eturn **o**n **I**nvestment", acrónimo para expresar la medida del retorno de una inversión realizada para un proposito en comparación con otros.

- Reducción de parada de servicio no esperada y consecuentes pérdidas económicas
- Prevenir mala prensa que pueda perjudicar a la imagen de la compañía.

Para definir el plan de ciberseguridad lo haremos en base al análisis de la situación actual y a partir del análisis de los riesgos y amenazas tanto internos como externos. Es indispensable hacer este análisis para poder alinear la mitigación de los riesgos detectados con las necesidades de negocio.

4.2. Análisis de la situación actual

Es necesario poder tener claro el punto de partida, tanto si se está empezando a definir un plan de ciberseguridad, como si estamos hablando de las revisiones que se deberían hacer a dichos planes. Este punto de partida o línea base de la situación actual, nos servirá para poder hacernos una idea de la situación actual y establecer el camino que deberíamos recorrer para llegar a nuestros objetivos.

En este punto tenemos que identificar, valorar y listar todos los activos de la compañía. Estos activos pueden ser elementos de nuestra red como lo datos que estamos guardando. Tenemos que saber relacionar todos estos activos a las normativas vigentes que les puedan influir como, por ejemplo, con GDPR la fecha de nacimiento se considera PII[65] y por tanto datos sensibles que debemos tener catalogados para saber en qué sistemas los vamos a guardar y que estado de seguridad tienen.

Es importante poder identificar y valorar los activos de la compañía, debemos también analizar el estado de madurez, de esta, respecto a la ciberseguridad, es decir, que acciones se están tomando ya para proteger dichos activos. Se debería tener en consideración, entre otras cosas:

- Identificar a los responsables de los activos
- Estrategias de actualización del software y hardware.
- Estrategias de acceso físico a los sistemas y activos de la compañía.
- Estrategias de acceso a los sistemas informáticos, así como la contraseña o posibles factores extras de autentificación.
- Formación y conocimientos del personal respecto a ciberseguridad.
- Conocimientos sobre la estrategia de ciberseguridad actual de la compañía.
- Políticas de copias de seguridad.
- Exceso de privilegios en los sistemas y de accesos físicos.
- Políticas de guardado y compartición de información sensible.
- Estado de contratos con terceros y confidencialidad
- Estrategia de continuidad de negocio tanto a nivel informático como a nivel de oficinas o comunicaciones.

[65] PII "***P****ersonal* ***I****dentificable* ***I****nformation*" información sensible no pública de las personas

- Estrategia de segmentación y securización de la red informática.
- De qué herramientas o controles dispone la compañía para detectar posibles problemas.

El listado puede ser más extenso, lo importante en este punto es intentar buscar una visión 360º del estado actual de la compañía y de sus activos.

En este punto es interesante poder disponer de alguna herramienta que nos permita tener toda esta información de manera ordenada y clasificada. Se recomienda que sea una herramienta informática, de manera que perder la información sea más complicado, añadir nueva información más sencillo, en definitiva, que introducir, mantener, actualizar, borrar y buscar información, sea sencillo y se facilite lo máximo posible.

Sería bueno también generar mapas de servicio de los diferentes procesos críticos de la compañía para poder tener documentadas las diferentes relaciones entre diferentes sistemas o procesos, así como la definición de posibles KPIs[66] que permitan poder ver a futuro como hemos evolucionado respecto a la posición inicial.

Es importante que al hacer todo este análisis también se tengan en cuenta las normativas vigentes que puedan afectar para poder detectar puntos de no cumplimiento.

Con toda esta información estructurada se empezará a tener una visión más clara del punto de partida y seguramente ya se empezarán a vislumbrar posibles acciones de mejora o incluso acciones que se deberían abordar con urgencia. Pese a esto, es importante abordar todo el análisis en profundidad y llegando a cubrir los objetivos marcados en el inicio sin desviarse, para poder completar al máximo la información necesaria para el siguiente punto.

4.3. Análisis de riesgos y amenazas

Una vez establecida la línea base comentada en el anterior punto, se ha de hacer un análisis de riesgos y amenazas. También se ha de definir la estrategia de la compañía respecto a los riesgos, es decir, que nivel de riesgos está dispuesta a asumir o no.

Las metodologías de análisis de riesgos y amenazas se pueden clasificar en dos grandes grupos:

- Cualitativas: metodología subjetiva, ya que se basa en la experiencia de los analistas y los equipos vinculados al análisis para crear una matriz de riesgos y amenazas donde se clasifiquen los riesgos y las amenazas

[66] KPI "***K**ey **P**erformance **I**ndicator*" es una medida que ha de servir para poder ver la evolución o estado de aquello que se quiera medir o mejorar.

según su probabilidad de ocurrencia según el analista y su impacto en caso de que ocurra. Aquí se intenta clasificar todos y cada uno de los riesgos. Al ser subjetiva se corre el riesgo de incorporar los sesgos de las personas en este este análisis, que puedan influir negativamente.

- Cuantitativas: En este grupo se analizan los datos para medir los posibles efectos en caso de que ocurra el riesgo y el impacto económico que supondría. Se hace uso de técnicas matemáticas para hacer los cálculos de probabilidad de ocurrencias. El mayor riesgo de este tipo de análisis es no disponer de suficientes datos o de dato alguno en el análisis con lo que los resultados no sean todo lo fiables que se desearía.

Como se puede ver las dos metodologías tienen riesgos, con lo que se recomienda hacer uso combinado de las dos para obtener lo mejor de los dos mundos. Los diálogos que se establecen en la primera para hablar con las diferentes figuras clave de IT y de negocio de la compañía son clave para tener una visión directa del estado actual y los riesgos que quizá no quedarían reflejados directamente por la segunda. A partir de esta visión general, poder focalizar y buscar estrategias que sirvan para cuantificar y hacer seguimiento de los riesgos más importantes y con mayor impacto, usando la segunda, hace que la mitigación sea mejor monitorizada y se pueda presentar sin espacio a errores.

Los objetivos perseguidos con este análisis, independientemente de la metodología empleada, son:

- Identificar los riesgos
- Categorizar los riesgos
- Medir el impacto de los riesgos
- Establecer medidas para monitorizar el estado de los riesgos
- Tener información suficiente para poder tomar decisiones en el plan de ciberseguridad
- Documentación de los riesgos y su causa
- Listado de actores externos e internos que pueden influir en los riesgos
- Decidir si se quiere evitar, compartir, aceptar o controlar los riesgos

4.4. Definición de un Plan

Habiendo recogido toda la información del estado actual, así como habiendo hecho un análisis de los riesgos y amenazas, llega el momento de definir una estrategia a corto, medio y largo plazo. No debemos olvidar, como veíamos en el punto "*4.1 Adoptar y planificar la ciberseguridad*", que esta estrategia debe estar alineada con negocio en todo momento, y acordada con el CEO de manera que podamos garantizar el éxito de implantación y implementación.

En el corto plazo deberíamos centrarnos en intentar poner solución a los riesgos con más impacto y con más probabilidad de ocurrencia. Podemos adoptar diferentes estrategias para la mitigación de los riesgos:

- Cederlos a terceros, como podría ser a través de una póliza de ciberriesgos para mitigar el impacto cuando ocurran, o bien con la contratación de un servicio externo que se dedique solo a aplicar acciones de mitigación para dichos riesgos.

- Eliminarlos, como por ejemplo eliminando procesos ya no necesarios

- Asumirlos. Por ejemplo, quizá vemos un riesgo en que, si se corta el suministro eléctrico en una oficina, los agentes no podrán acceder a sus ordenadores o a través de nuestra infraestructura de red, pero podríamos decidir que comprar un grupo electrógeno supera los costes y los beneficios de esperar a que la empresa eléctrica solucione el problema

- Mitigarlos. En el mismo ejemplo, podríamos instalar un pequeño SAI[67] en lugar de un grupo electrógeno.

Para el medio plazo, deberíamos poder empezar a dibujar qué cambios de más calado se han de planificar para irlos abordando y permitir que el plan de continuidad de negocio esté adecuado a la situación real que tenemos.

Para el largo plazo, hay que diseñar el ciclo de vida de revisiones periódicas que queremos realizar. Revisión de normativas nuevas que puedan aparecer, revisión de posibles nuevos factores que puedan afectar al estudio realizado, en definitiva, revisión constante de los activos y de los riesgos y amenazas internas y externas.

En cualquier caso, siempre se debe prestar atención a la aparición de nuevos activos, y tener previsto poder incorporarlos al plan y la estrategia en cualquier momento. El trabajo realizado hasta ahora con el análisis de la situación actual y el análisis de riesgos y amenazas, dentro de un ciclo constante de revisión se podría resumir en los siguientes gráficos:

Ilustración 4-2 Análisis constante de la ciberseguridad desde los activos de la compañía

Fuente: revista Economía industrial, número 410, artículo "*Gobierno de la ciberseguridad*" de Roberto Baratta Martínez

[67] SAI "***S**istema de **a**limentación **i**ninterrumpida*", son baterías donde se enchufan los sistemas que se quieren proteger de posibles cortes eléctricos y estas, a su vez van conectadas a la toma de corriente donde iría conectado habitualmente ese sistema sin protección hasta la instalación del SAI.

Ilustración 4-3 Implantación de un Plan director de Seguridad por INCIBE

Fuente: Incibe, "*Plan director de seguridad*", colección protege tu empresa, ilustración 1.

Para poner en marcha el plan de ciberseguridad, tenemos que definir:

- Roles y responsabilidades: Quién va a ser el encargado de cada uno de los puntos y qué tendrá que supervisar o cumplir.

- Objetivos y su alcance: Es importante tener claras las metas a dónde queremos llegar, y a que va a afectar, así como que se persigue con ese objetivo.

- Estrategia: Cómo vamos a llegar a cada uno de los objetivos marcados.

- Marco de control e indicadores: Cómo vamos a evaluar y controlar si se están consiguiendo dichos objetivos. Cómo vamos a montar sistemas de control y seguimiento continuo para poder detectar incidentes todo y haber recorrido camino para mitigar riesgos.

- Pruebas: Qué pruebas vamos a realizar para para estresar los planes de continuidad de negocio y los cambios que vamos realizando.

- Normativas: Debemos tener en cuenta las normativas aplicables tanto existentes como a medida que vayan apareciendo para asegurarnos que las cumplimos.

- Gestión de terceros: Usar ayuda de terceros es una posibilidad tanto para la transferencia de riesgos como para la gestión continua de ciberseguridad, hay que plantearlo y decidirlo.

- Revisiones: Periodicidad en la que se revisa la estrategia y los activos protegidos, así como posibles reportes a dirección o a estamentos reguladores.

Se ha extendido mucho la necesidad de disponer de un SOC[68] como departamento que ayuda a tener un marco de control, monitorización e indicadores del plan de ciberseguridad. Algunas optan por montarlo con recursos internos, pero la mayoría optan por cederlo a terceros con capacidad y conocimientos activos de ciberseguridad. Un SOC es un centro de seguridad encargado de monitorizar, analizar, detectar, responder y mejorar, en definitiva, la seguridad de la empresa.

Un SOC por lo general intenta centralizar todos los elementos definidos a monitorizar desde un punto de vista de seguridad, puede correlacionar los eventos de todos ellos para poder detectar patrones o intrusiones no deseadas usando algunas de las técnicas vistas en el capítulo 3.3.

El equipo del SOC es especialista en seguridad informática y está dedicado exclusivamente a ello, de esta manera se consigue descargar a los equipos tradicionales de IT la responsabilidad de mantener el sistema y tener controladas todas las posibles técnicas o vectores de ataques nuevos.

Debido a todo ello, montar o mantener un SOC supone un gasto elevado y se debe analizar su inclusión en el plan de ciberseguridad.

[68] SOC "***S**ecurity **O**peration **C**enter*"

5. Situación sector seguros en España

Actualmente ICEA, en España, ha realizado 3 estudios llamados "***Termómetro de la ciberseguridad en el sector asegurador español***", el último es de Julio de 2022 y han participado 55 empresas del sector, 12 más que en el anterior:

Ilustración 5-1 Entidades participantes en el estudio

Fuente: ICEA, "*III Termómetro de la ciberseguridad en el sector asegurador*".

Gracias a estos informes podemos hacernos una idea general de cómo está el sector en la implementación de normativas o de medidas preventivas de ciberseguridad comentadas en los puntos anteriores.

Podemos decir que en general se observa una buena concienciación del sector respecto a la ciberseguridad, aunque no llegue a ser el 100% se marca una tendencia positiva a ir aumentando en los próximos años.

5.1. Estrategia y Organización

El 87.8% de las empresas cuenta con un plan estratégico de ciberseguridad, un 7% más que el año pasado, aunque el 7.8% de ellas todavía no lo tiene aprobado, y el 11.7 del resto está en desarrollo de uno. Hay que destacar que un 1.1% no dispone de un plan ni está trabajando en ello.

Ilustración 5-2 Existencia de un plan estratégico de ciberseguridad

Fuente: ICEA, "*III Termómetro de la ciberseguridad en el sector asegurador".*

Actualmente el 100% de las empresas tiene una persona responsable de la ciberseguridad, si es cierto que solo el 63% de ellas disponen de un CISO propiamente dicho.

Sigue habiendo más empresas cuyo CISO dependen del CIO, aunque se ha observado que casi se han doblado las empresas que han pasado a depender de Dirección General en lugar del CIO, así que se puede observar cómo cada vez la figura del CISO se considera de más importancia.

Ilustración 5-3 Funciones gestión de riesgos TI y roles asociados

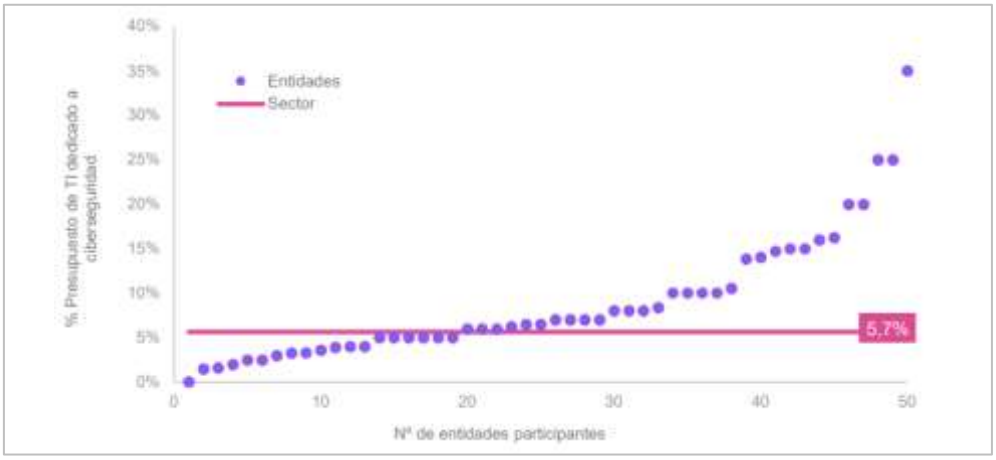
Fuente: ICEA, "*III Termómetro de la ciberseguridad en el sector asegurador*".

Se puede observar como la función del CISO es la encargada de la seguridad de la información en la mayoría de las empresas.

Más del 82% de las empresas hace uso de un SOC 24x7 para poder tener monitorizados sus sistemas desde el punto de vista de seguridad. un 11% está planteando implementar uno, tan solo el 5.6% no considera una prioridad poner en marcha este servicio o departamento.

La media del presupuesto dedicado a ciberseguridad es del 5.7% del total de IT, y se observa que el 62% de entidades que han contestado a la cuestión están por encima de esta media, y que el 30% destinan más del 10% de su presupuesto.

Ilustración 5-4 Presupuesto de ciberseguridad sobre el presupuesto total de IT



Fuente: ICEA, "*III Termómetro de la ciberseguridad en el sector asegurador*".

El presupuesto está gobernado desde TI en el 55.1% de las entidades, aunque el 30.3% de ellas ya dispone de un departamento de ciberseguridad con su propio presupuesto. Un 2.2% no dispone de presupuesto para ciberseguridad. Sorprende este dato dado que tan solo el 1.1% no disponía de plan de ciberseguridad, con lo que el 1.1% restante podría ser debido a aquellas empresas que todavía están implementando su propio plan.

El 92.6% de las empresas han aumentado el presupuesto respecto al año anterior. Esto demuestra un mayor compromiso en general del sector, así como una visión más realista de los posibles efectos de los ciberataques.

Para poder desarrollar los planes de ciberseguridad e implementar las acciones o medidas previstas las empresas encuentran que las tres principales palancas son la presión regulatoria, un incidente de seguridad en organizaciones del entorno y un incidente de seguridad en la propia organización. Estas tres palancas son las que más ayudan al responsable de seguridad a poder justificar o aumentar el presupuesto o el ritmo de implantación de medidas. La continua sofisticación de los propios ciberataques, la evolución continua de las tecnologías y la dificultad de integración de los distintos sistemas de seguridad son las 3 principales dificultades que se encuentran nuestras compañías.

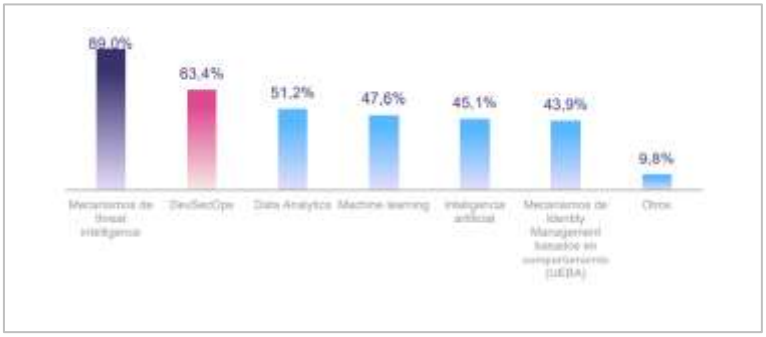
Ilustración 5-5 Dificultades más relevantes a la hora de implementar más medidas de seguridad

Fuente: ICEA, "*III Termómetro de la ciberseguridad en el sector asegurador*"

Las herramientas o técnicas más usadas en el sector para mitigar, y ayudar a prevenir posibles eventos de seguridad son mecanismos de "*Threat Intelligen-*

ce", procesos de "*DevSecOps*"[69], "*Data Analytics*", "*Machine Learning*" y "*Analítica de comportamiento*" además de algún otro.

Ilustración 5-6 Presencia de nuevas técnicas o tecnologías que se utilizan como medidas de protección frente a ciberataques



Fuente: ICEA, "*III Termómetro de la ciberseguridad en el sector asegurador*"

5.2. Ciberseguridad, Riesgos y geopolítica

En caso de ciberataque el 87.8% de las empresas disponen de un plan de respuesta para poder actuar en caso de incidente y, un 46% reconoce haber sufrido algún tipo de incidente de seguridad durante el último año. Aunque el ataque más temido sigue siendo un ataque de ransomware, el tipo de ataques más sufrido por las entidades han sido ataques de denegación de servicio, afectando así a la continuidad de negocio.

En el contexto actual de teletrabajo causado por la COVID-19, para el 53.4% de las empresas de seguridad eso ha implicado que se han incrementado los ciberataques a la tecnología que permite el acceso remoto.

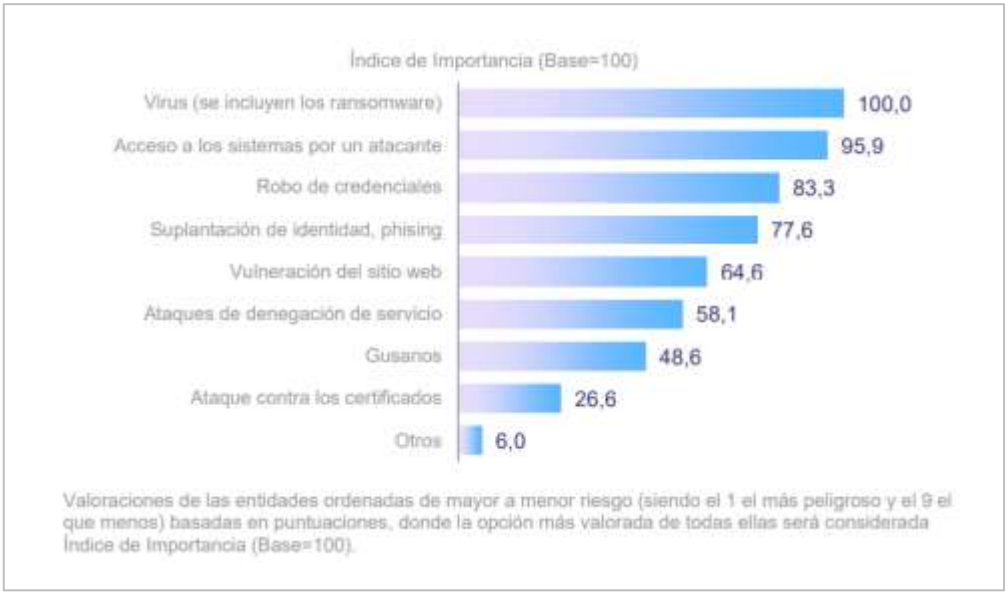
Ilustración 5-7 Efectos de los ciberataques relacionados con el teletrabajo

Fuente: ICEA, "*III Termómetro de la ciberseguridad en el sector asegurador*"

[69] DevSecOps "**Dev**elopment, **Sec**urity, and **Op**erations", cultura que pretende incorporar al flujo de Desarrollo y de operaciones la perspectiva de seguridad y automatización para minimizar error humano y maximizar la seguridad.

A parte del ransomware, como tipo de ataque más peligroso y con más impacto para la continuidad de negocio o reputación de la identidad, las empresas del sector están preocupadas por posibles accesos no permitidos a los sistemas o el robo de credenciales.

Ilustración 5-8 Ataques más peligrosos para el funcionamiento o reputación de una entidad



Fuente: ICEA, "*III Termómetro de la ciberseguridad en el sector asegurador*"

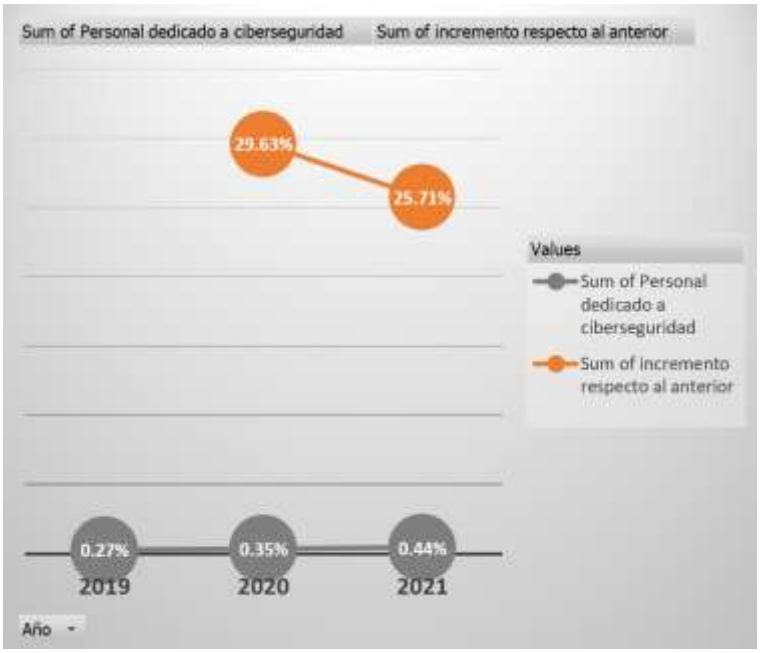
En la situación actual de crisis geopolítica con la guerra de Ucrania, la mayoría de las empresas del sector, un 71.1%, reconocen haber notado un incremento de las ciber-amenazas y, apoyadas por fuentes de ciber-inteligencia externas, han podido actuar en función de las notificaciones relacionadas tanto con la entidad, como con las relacionadas a efectos de la guerra. También la gran mayoría de ellas, el 66.7%, de manera proactiva han buscado la manera de aumentar las medidas de seguridad y, el 15.6% han realizado alguna acción puntual debido al incremento de los ciberataques.

El contexto actual de guerra ha puesto sobre la mesa la posibilidad real de una ciberguerra, cosa que hace que de manera unánime las empresas afirmen que el sector asegurador es crítico, aunque se consideren más críticos el sector público, energético, sanitario o farmacéutico.

5.3. Personal, formación y nuevas tecnologías

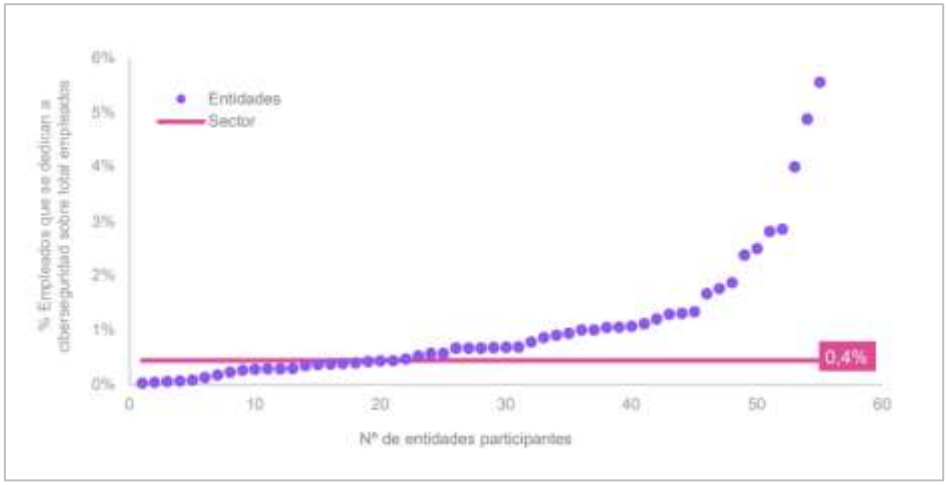
En media, el porcentaje de empleados dedicados a la ciberseguridad ha ido creciendo estos últimos años en las empresas y, el 28.7% de estas, cuentan con un 1% o más de su plantilla dedicada a la ciberseguridad. Aunque este último año, la plantilla no ha crecido tanto como el anterior, de momento se mantiene el interés en reforzar la plantilla para este cometido.

Ilustración 5-9 Evolución de personal dedicado y porcentaje de crecimiento respecto al anterior período



Fuente: Elaboración propia a partir de los datos del informe ICEA sobre el porcentaje de trabajadores dedicados a la ciberseguridad.

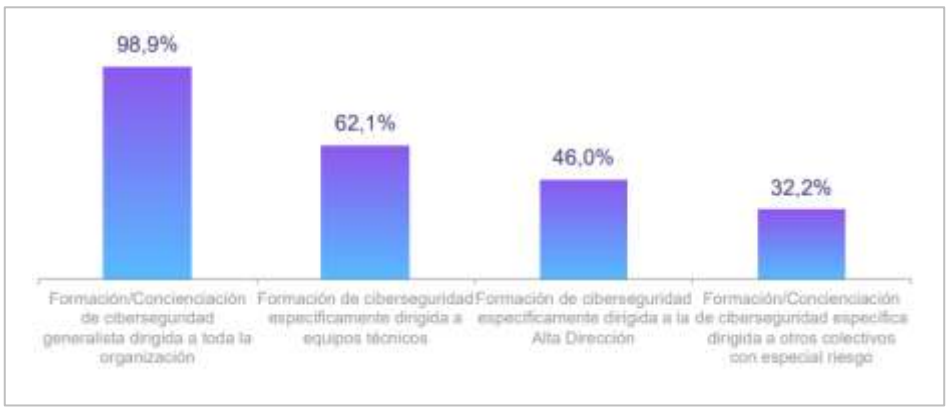
Ilustración 5-10 Empleados que se dedican a la ciberseguridad sobre el total de empleados



Fuente: ICEA, "*III Termómetro de la ciberseguridad en el sector asegurador*"

El 96.7% de las empresas consultadas han realizado alguna formación dirigida a todo el personal en materia de seguridad informática o de riesgos IT. La mayoría han impartido formación para la concienciación de la plantilla, más de la mitad además han impartido formación específica para equipos técnicos, y el 46% han hecho alguna específica para alta dirección.

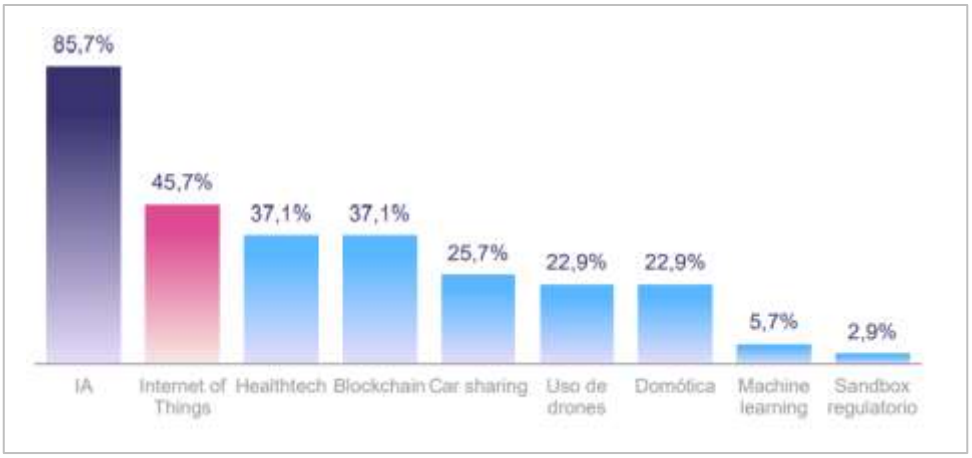
Ilustración 5-11 Presencia de formación en materia de ciberseguridad según segmento al que se dirigía



Fuente: ICEA, "*III Termómetro de la ciberseguridad en el sector asegurador*"

Tres de cada cinco empresas reconocen estar utilizando o valorando utilizar alguna nueva tecnología para influenciar positivamente en sus procesos de negocio, mejorar resultados, nuevas oportunidades de negocio, facilitar el acceso a los usuarios, etc. La Inteligencia artificial es la gran ganadora respecto a este uso, seguido de IoT o de tecnologías de HealthCheck[70].

Ilustración 5-12 Presencia de cada tecnología en las entidades que las están utilizando



Fuente: ICEA, "*III Termómetro de la ciberseguridad en el sector asegurador*"

Junto con el uso de estas nuevas tecnologías las empresas están haciendo los deberes ya que el 90.3% de ellas está valorando activamente los ciber-riesgos asociados a la implantación y uso de estas.

En lo que respecta al uso de la nube (o Cloud) tan solo 2 de cada 5 empresas del sector usa servicios alojados en este tipo de tecnología, y el marco de con-

[70] Las tecnologías de healthcheck permiten de manera remota medir constantes vitales del cliente de manera que se pueden usar para diferentes líneas de negocio: Seguro de salud, crear programa de puntos en base a actividades, etc.

trol que se hace a estas es, en un 61.1%, diferente al que se realiza en los servicios IT propios:

Ilustración 5-13 Existencia de marcos de control específicos para entornos cloud

Fuente: ICEA, "*III Termómetro de la ciberseguridad en el sector asegurador*"

5.4. Protección

El 72.2% de las entidades del sector confirman tener contratada una póliza de ciber-riesgos. En 2 de cada 3 entidades el capital asegurado supera ya los 3 millones de euros, y la prima no supera los 80.000 euros en el casi 40% de las entidades, coste que el 75% de las entidades considera acorde con el servicio contratado.

6. Conclusiones

Vivimos en un mundo en constante evolución, donde la tecnología juega uno de los papeles más importantes, en líneas generales, de cualquier ámbito de nuestras vidas. La tecnología avanza a pasos agigantados y, cosas que hasta hace unos años eran simples ideas, ahora son realidades, y los sueños que tenemos ahora, en breve serán posible.

En este sentido tenemos que ser conscientes que, junto a la evolución de la tecnología, que nos permite la automatización, el análisis y la simplificación de cualquiera de los ámbitos de nuestro negocio, se abre también las puertas a problemas de seguridad. Éstos son, la mayoría, debidos a errores humanos, tanto de los equipos de IT (falta de actualizaciones del sistema, errores en configuración, no cambiar contraseñas por defecto, y un largo etcétera), como de los empleados de la empresa (entrar en sitios web no recomendados, abrir enlaces o adjuntos de correos no confiables, así como tantos otros posibles errores).

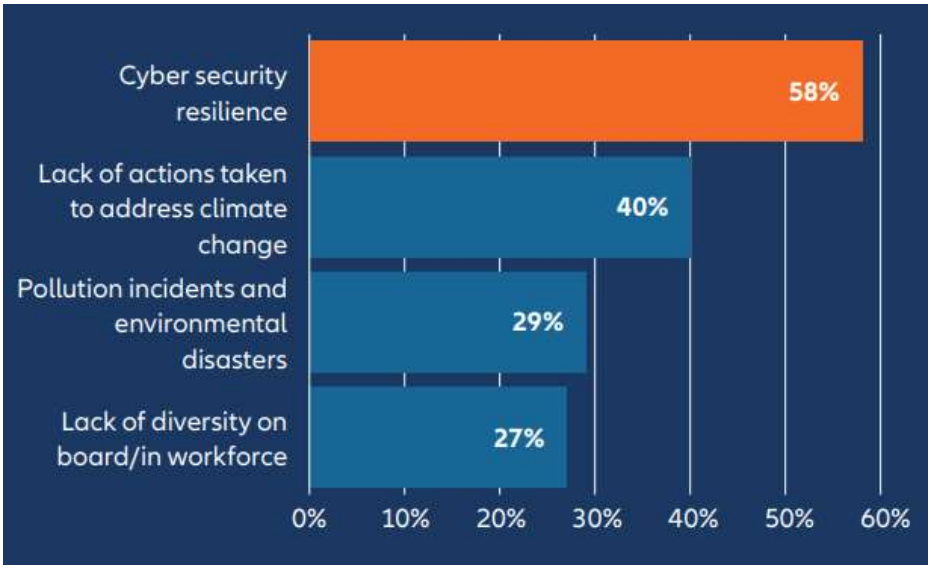
Al igual que la tecnología evoluciona, así lo hacen los delincuentes, que también tienen acceso a ella. Esto es un riesgo muy elevado para cualquier empresa, del sector o no, ya que en la "dark web" se ofrecen todo tipo de servicios a precios asequibles, llegando a un nivel de profesionalización muy elevado y haciendo muy fácil el acceso a poder realizar un ciberataque a cualquier empresa.

Es un argumento antiguo el pensar que nuestra empresa no va a ser objetivo de ningún ciberataque dado que no es una empresa importante o grande, con esta profesionalización de la delincuencia este argumento ya no es válido, y no debería tomarse a la ligera. Con esto no quiero caer en técnicas "FUD"[71], que se basan en generar miedo, incertezas y dudas (de sus siglas en inglés), simplemente intento exponer una realidad existente, a partir de ésta, lo que tenemos que hacer es ponernos a trabajar.

También se ha observado la importancia que tienen para los inversores las empresas que se focalizan en estrategias tipo ESG, y la ciberseguridad ha alcanzado un peso o preocupación importante entre los inversores. Estas estrategias también tienen en cuenta el cambio climático o la paridad en las plantillas de empleados o en la directiva de una empresa.

[71] FUD "***F**ear, **U**ncertainity, **D**oubt*",

Ilustración 6-1 Which ESG risk trends are of most concern to your company



Fuente: “Allianz Risk Barometer 2022”

Las regulaciones y las normativas han venido para ayudarnos, y para mostrarnos la importancia que tiene el proteger a nuestra empresa y a sus datos. Así las regulaciones que han ido evolucionando como la ***GDPR***, cuya última revisión es de 2016 y su objetivo es regular el tratamiento de los datos personales y su libre circulación, o el ***Reglamento delegado de la comisión europea en el contexto de seguridad y gobierno de las TIC*** o, ya en nuestro sector, ***Solvencia II***, o ***DORA*** que, junto con el organismo de control europeo, ***EIOPA***, marcan unas pautas mínimas a nuestros sistemas IT. Así, de esta manera, que se aumente la seguridad en líneas generales y los clientes o ciudadanos europeos ganen, o no pierdan, confianza en las instituciones y en las empresas. No nos tenemos que engañar, las regulaciones ejercen una presión constante y no deja de ser uno de los riesgos que las empresas siempre tienen en cuenta en la afectación de sus negocios:

Ilustración 6-2 Changes in legislation and regulation risk ranking

Fuente: “Allianz Risk Barometer 2022”

Aunque esté el riesgo, y el temor, a este marco cambiante en cuanto a regulaciones, estas nos obligan a hacer un análisis constante y a adecuar nuestros procesos y tecnologías a este mundo cambiante en relación con la seguridad.

También tenemos de nuestra mano los estándares de seguridad, que intentan perseguir los mismos objetivos, pero esta vez dándonos una serie de pautas, herramientas y procedimientos a seguir para adecuar la seguridad de nuestros sistemas y maximizar la protección. Así, en el país tenemos que destacar el esquema nacional de seguridad, modificado por última vez en mayo de este año, y que establece, de obligado cumplimiento para las empresas del sector público o cualquier colaborador de estas, cuatro pilares sobre los que trabajar, ***"Prevención", "Detección", "Respuesta"*** y ***"Conservación"*** y que en esta última revisión habla de conceptos como vigilancia continua, mínimo privilegio o como interactuar con servicios de la nube.

Teniendo en cuenta todo esto, como primera obligación, está claro que debemos que cumplir las regulaciones y normativas vigentes que afectan a nuestro sector, pero también debemos ser capaces de hacer un análisis constante de nuestra infraestructura para minimizar el riesgo de sufrir incidentes de ciberseguridad que puedan afectar a la reputación de la empresa, o incluso llegar a ponerla en una situación de riesgo de fallida. Para ello debemos adoptar la seguridad dentro de cualquier proceso de la compañía. Esto lo conseguiremos definiendo un plan de ciberseguridad global, apoyado desde dirección y con un presupuesto adecuado a nuestras necesidades y aceptación de riesgos que hayamos definido juntamente con dirección para alinearnos a negocio. Sin este plan, o esta alineación con dirección y, por tanto, negocio, el plan o la ciberseguridad no cubrirán las necesidades reales de nuestra empresa, con lo que no conseguiremos mitigar los riesgos a los que no queremos exponernos. Es importante contar con la figura de un CISO, independiente de IT y que por tanto tenga las herramientas para poder forzar, en caso necesario, cambios en estrategias de IT que, de otra manera, supusieran un riesgo no aceptable.

Para asegurar que el plan de ciberseguridad es efectivo, se deben definir objetivos e indicadores medibles, y debemos tener toda nuestra infraestructura en constante vigilancia a través de herramientas como SIEMs[72], pero aconsejablemente montando un equipo SOC, capaz de estar al día del mundo de la ciberseguridad y dedicado específicamente a esta monitorización y reacción a cualquier tipo de incidentes de seguridad.

La clave de los planes de ciberseguridad es definir bien los riesgos a los que queremos estar expuestos y a los que no, y tomar medidas respecto a este análisis como decíamos, pero otro factor muy importante es hacer una revisión cíclica de nuestros activos y exposición al riesgo, debido al entorno cambiante en el que estamos, tanto geopolítico, como tecnológico.

[72] SIEM, "***S****ecurity* ***I****nformation and* ***E****vent* ***M****anagement*", campo de la informática que se va basa en herramientas para proveer de análisis de seguridad en tiempo real de los diferentes sistemas.

Por último, quiero mencionar que tenemos la impresión de que nuestro sector está trabajando duramente en adecuarse a estas nuevas realidades, la prueba de ello es el elevado porcentaje de empresas que tiene un plan o casi preaprobado un plan (el 87.8% de ellas) de ciberseguridad. Qué el presupuesto del 62% de ellas está por encima de la media. Qué el 100% tiene definida una figura responsable de seguridad, aunque solo el 63% tienen definida la figura de un CISO.

El personal dedicado a la seguridad ha ido aumentando los últimos años, y más del 82% hacen uso activo de un equipo SOC. Se están dedicando esfuerzos en la formación tanto de toda la plantilla como la que se dedica a la seguridad.

Además, un gran porcentaje cuenta con una póliza de ciber-riesgos. Así que en general daríamos un aprobado al sector, aunque si queremos destacar otra vez que esto es un trabajo constante, no hay que bajar la guardia en definir nuestra postura de seguridad y en revisarla constantemente.

Intentar alentar al pequeño porcentaje de compañías que todavía no están pensando en estos términos, a empezar a pensar en un plan de ciberseguridad para mitigar cualquier riesgo que puedan tener, consciente o inconscientemente.

7. Bibliografía

7.1. Artículos

Regió 7, "***El ciberatac al grup Llobet és el més important al Bages dels últims mesos***"
<https://www.regio7.cat/fet-divers/2022/01/28/ciberatac-grup-llobet-mes-important-62074303.html>
(Fecha de consulta 14 de mayo de 2022)

Tot Barcelona, "***Un atac informàtic al Liceu va sostreure noms, correus i DNIs***"
<https://www.totbarcelona.cat/successos/atac-informatic-liceu-barcelona-191554/>
(Fecha de consulta 14 de Mayo de 2022)

CCMA, "***El govern destina més de 3,5 milions d'euros a la UAB perquè es recuperi del ciberatac***"
<https://www.ccma.cat/324/el-govern-destina-mes-de-3-5-milions-deuros-a-la-uab-perque-es-recuperi-del-ciberatac/noticia/3131432/>
(Fecha de consulta 14 de Mayo 2022)

The Daily Swig, "***Pegasus mobile spyware used zero-click exploits to snoop on Catalan politicians***"
<https://portswigger.net/daily-swig/pegasus-mobile-spyware-used-zero-click-exploits-to-snoop-on-catalan-politicians>
(Fecha de consulta 14 de Mayo de 2022)

Computer Weekly, "***Incontroller ICS malware has 'rare, dangerous' capabilities, says Mandiant***"
<https://www.computerweekly.com/news/252515949/Incontroller-ICS-malware-has-rare-dangerous-capabilities-says-Mandiant>
(Fecha de consulta 14 de Mayo de 2022)

CNN, "***Cyberattack on Toyota's supply chain shuts its 14 factories in Japan for 24 hours***"
<https://edition.cnn.com/2022/03/01/business/toyota-japan-cyberattack-production-restarts-intl-hnk/index.html>
(Fecha de consulta 14 de Mayo de 2022)

Deloitte, "***The EU's Digital Operational Resilience Act for financial services***"
<https://www2.deloitte.com/lu/en/pages/financial-services/articles/the-eus-digital-operational-resilience-act-for-financial-services-new-rules.html>
(fecha de consulta 5 de junio 2022)

The New York Times, "***TECHNOLOGY; Microsoft Sets $5 Million Virus Bounty***"

<https://www.nytimes.com/2003/11/06/business/technology-microsoft-sets-5-million-virus-bounty.html>
(fecha de consulta 25 de mayo 2022)

Microsoft, "***Celebrating 20 Years of Trustworthy Computing***"
<https://www.microsoft.com/security/blog/2022/01/21/celebrating-20-years-of-trustworthy-computing/>
(Fecha de consulta 25 de mayo 2022)

PrivacySavvy, "***6 times when hackers forced companies to go bankrupt and shut down***",
<https://privacysavvy.com/security/business/6-times-hackers-forced-companies-to-go-bankrupt-shut-down/>
(Fecha de consulta 14 de junio 2022)

INCIBE, "***CEO, CISO, CIO… ¿Roles en ciberseguridad?>***"
<https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad>
(Fecha de consulta 15 de junio 2022)

Forbes, "***Why Your CISO Should Report Directly To The CEO***"
<https://www.forbes.com/sites/forbestechcouncil/2021/09/08/why-your-ciso-should-report-directly-to-the-ceo/>
(Fecha de consulta 15 de junio 2022)

TrustNet, "Qualitative vs. Quantitative Risk Assessments in Cybersecurity"
<https://www.trustnetinc.com/qualitative-vs-quantitative/>
(Fecha de consulta 2 de julio 2022)

Economía Industrial número 410, Roberto Baratta Martínez, "GOBIERNO DE LA CIBERSEGURIDAD"

<https://dialnet.unirioja.es/servlet/articulo?codigo=6815102>

(Fecha de consulta 3 de julio 2022)

7.2. Informes

World Economic Forum, ***The Global Risks Report 2020*** (publicado en 15 de Enero 2020)

World Economic Forum, ***The Global Risks Report 2022*** (publicado en 11 de Enero 2022)

IDC, ***The Digitalization of the World from Edge to Core***. David Reinsel, John Gantz, John Ryding (publicado en Noviembre de 2018)

EY, ***Sostenibilidad, El Tsunami regulatorio que viene***. Junio 2021

<https://www.ey.com/es_es/rethinking-sustainability/sostenibilidad-tsunami-regulatorio>

CSIS, ***Significant Cyber Incidents*** (Actualizado mensualmente)
<https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>

IBM, ***IBM Security Services 2014 Cyber Security Intelligence Index***

IBM, ***X-Force Threat Intelligence Index 2017***

IBM, ***X-Force Threat Intelligence Index 2022***

NIST, ***Getting Started with the NIST Cybersecurity Framework***, NIST Special Publication 1271, Agosto 2021
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271.pdf>

ICEA, ***II Termómetro de la ciberseguridad en el sector asegurador español***, Julio 2021

ICEA, ***III Termómetro de la ciberseguridad en el sector asegurador español***, Julio 2022

Allianz, ***Allianz Risk Barometer 2022,*** Enero 2022

7.3. Fuentes de internet

MindSight, "***History Of Cyber Attacks From The Morris Worm To Exactis***"
<https://gomindsight.com/insights/blog/history-of-cyber-attacks-2018>
(Fecha de consulta 19 de Mayo de 2022)

WikiPedia, "***Internet***"
<https://en.wikipedia.org/wiki/Internet>
(Fecha de consulta 19 de Mayo de 2022)

HerJavec Group, "***Cyber CEO: The History Of Cybercrime, From 1834 To Present***"
<https://www.herjavecgroup.com/history-of-cybercrime/>
(Fecha de consulta 19 de Mayo de 2022)

Podcast Secret history of The Future, „***Human Insecurity***"
<https://slate.com/technology/2018/10/what-an-1834-hack-of-the-french-telegraph-system-can-teach-us-about-modern-day-network-security.html>
(Fecha de consulta 19 de Mayo de 2022)

Statista, “***Ranking de las compañías de seguros con mayor volumen de primas emitidas en España 2022***“
<https://es.statista.com/estadisticas/541648/grupos-aseguradores-por-volumen-de-primas-en-espana/>
(Fecha de consulta 21 de Mayo de 2022)

Wikipedia, “***Bundesdatenschutzgesetz (BDSG)***“
<https://en.wikipedia.org/wiki/Bundesdatenschutzgesetz>
(Fecha de consulta 22 de mayo de 2022)

Uniway, “***Creeper, 50 Years of Virus in the Network***“
<https://www.uniway.es/en/blog/creeper-50-years-of-virus-in-the-network>
(Fecha de consulta 24 de mayo de 2022)

Wikipedia, “***ILOVEYOU***“
<https://en.wikipedia.org/wiki/ILOVEYOU>
(Fecha de consulta 24 de mayo de 2022)

GeeksforGeeks, “***History of cyber Security***“
<https://www.geeksforgeeks.org/history-of-cyber-security/>
(fecha de consulta 24 de mayo de 2022)

Wikipedia, “***Application firewall***“
<https://en.wikipedia.org/wiki/Application_firewall>
(fecha de consulta 24 de mayo 2022)

Wikipedia, “***Computer Fraud and Abuse Act***“
<https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act>
(fecha de consulta 25 de mayo 2022)

Wikipedia, “***Hacker Manifesto***“
<https://en.wikipedia.org/wiki/Hacker_Manifesto>
(fecha de consulta 25 de mayo 2022)

Wikipedia, “***Legion of Doom (hacker group)***”
<https://en.wikipedia.org/wiki/Legion_of_Doom_(hacker_group)>
(fecha de consulta 25 de mayo 2022)

Wikipedia, “***Pretty Good Privacy***“
<https://en.wikipedia.org/wiki/Pretty_Good_Privacy>
(Fecha de consulta 25 de mayo 2022)

Wikipedia, “***Usage Share of Operating Systems***“
<https://en.wikipedia.org/wiki/Usage_share_of_operating_systems>
(fecha de consulta 25 de mayo 2022)

Wikipedia, “***IT security standards***“
<https://en.wikipedia.org/wiki/IT_security_standards>
(Fecha de consulta 25 de mayo 2022)

TorProject, "***This is What a Tor Supporter Looks Like: Edward Snowden***" (entrevista)
<https://blog.torproject.org/what-tor-supporter-looks-edward-snowden/>
(Fecha de consulta 4 de junio de 2022)

Wikipedia, "***Tor (network)***"
<https://en.wikipedia.org/wiki/Tor_(network)>
(Fecha de consulta 4 de junio de 2022)

WikiPedia, "***Mass surveillance in China***"
<https://en.wikipedia.org/wiki/Mass_surveillance_in_China>
(Fecha de consulta 4 de junio de 2022)

InfoSec Insitute, "***Cybercrime as a Service***"
https://resources.infosecinstitute.com/topic/cybercrime-as-a-service/
(Fecha de consulta 4 de junio de 2022)

WikiPedia, "***Ernst & Young***"
<https://en.wikipedia.org/wiki/Ernst_%26_Young>
(Fecha de consulta 5 de junio 2022)

WikiPedia, "***Environmental, social, and corporate governance***"
<https://en.wikipedia.org/wiki/Environmental,_social,_and_corporate_governance>
(Fecha de consulta 5 de junio 2022)

WikiPedia, "***Moore's law***"
<https://en.wikipedia.org/wiki/Moore%27s_law>
(Fecha de consulta 10 de junio 2022)

CrowdStrike "***What is Cyber Threat Intelligence***"
<https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/>
(Fecha de consulta 22 de julio 2022)

7.4. Fuentes Oficiales

NIST, "***Periods Processing definition***"
<https://csrc.nist.gov/glossary/term/periods_processing>
(fecha de consulta 24 de mayo de 2022)

Union Europea, "***EIOPA***"
<https://www.eiopa.europa.eu/about/eiopa-glance/mission-and-tasks_en>
(Fecha de consulta 5 de junio 2022)

European Central Bank (ECB), "***Tiber-EU Framework. How to implement the European Framework for Threat Intelligence-based Ethical Red Teaming***"
<https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf>
(fecha de consulta 7 de junio 2022)

European Council, "***Digital finance: Provisional agreement reached on DORA***"
<https://www.consilium.europa.eu/en/press/press-releases/2022/05/11/digital-finance-provisional-agreement-reached-on-dora/>
(fecha de consulta 7 de junio 2022)

BOE, "***Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información***"
<https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257>
(fecha de consulta 7 de junio 2022)

BOE, "***Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad***"
<https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191>
(fecha de consulta 7 de junio 2022)

BOE, "***DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión***"
<https://www.boe.es/doue/2016/194/L00001-00030.pdf>
(fecha de consulta 7 de junio 2022)

EIOPA, "***Guidelines on information and communication technology security and governance***"
<https://www.eiopa.europa.eu/document-library/guidelines/guidelines-information-and-communication-technology-security-and_en>
(fecha de consulta 7 de junio 2022)

Eur-Lex Access to European Union Law, "***Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II)***"
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0138>
(fecha de consulta 7 de junio 2022)

Eur-Lex Access to European Union Law, "***Regulation (EU) 2015/2365 of the European Parliament and of the Council of 25 November 2015 on transparency of securities financing transactions and of reuse and amending Regulation (EU) No 648/2012***"
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R2365&qid=1654601572467>
(fecha de consulta 7 de junio 2022)

CCN, "***Infografías***"
<https://ens.ccn.cni.es/es/esquema-nacional-de-seguridad-ens/ens-infografias>
(fecha de consulta 7 de junio 2022)

BOE, “***Estrategia Nacional de Ciberseguridad 2019***”
<https://www.boe.es/boe/dias/2019/04/30/pdfs/BOE-A-2019-6347.pdf>
(fecha de consulta 10 de junio 2022)

Departamento de Seguridad Nacional, “***Estrategia Nacional de Seguridad 2021***”
<https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021>
(fecha de consulta 10 de junio 2022)

Ricardo Ibáñez Navés

Nacido en Barcelona, el 1 de mayo de 1981.

A nivel académico, a falta de completar el trabajo final de carrera, estudiado Ingeniería multimedia e Ingeniería informática de sistemas en la Universidad La Salle, Ramon Llull, Barcelona.

A nivel profesional, pasé por una etapa de desarrollador de páginas web y software desde 2002 hasta 2008. A partir de 2008 y hasta ahora, he desarrollado mi carrera profesional dentro del Grupo Catalana Occidente, en el área de sistemas como responsable del área de infraestructuras, llevando redes, servidores, backup, correo, middleware, cloud, y monitorización entre otros.