2022

PINAKES

LOPDGDD - RGPD

NIS2

DORA

IV Estudio
"Empresas y Ciberseguridad"

La seguridad de la cadena de valor: necesidad y obligación

LEET SECURITY
CyberSecurity Rating Agency

Con la colaboración de:

CLUB EXCELENCIA EN GESTIÓN

Tabla de CONTENIDO

Objetivo del ESTUDIO

Tras las realizadas en 2017, 2018 y 2020, presentamos la 4ª edición del Estudio Empresas y Ciberseguridad, en la que contamos de nuevo con la colaboración del Club Excelencia en Gestión.

Nuestro objetivo, desde la primera edición, ha sido el de contribuir al conocimiento común sobre esta área emergente que es **la ciberseguridad en la cadena de suministro, terceras partes o proveedores**, que está adquiriendo una importancia creciente como parte de la continuidad del propio negocio.

En ocasiones anteriores se han dado circunstancias particulares que, por su notoriedad, sin duda han tenido alguna influencia en las respuestas facilitadas. En 2017, la encuesta se realizó durante el mes de mayo, coincidiendo con los ataques del *ramsomware* WannaCry, posiblemente el de mayor impacto mediático hasta la fecha, y que se convirtió en un impulsor de la concienciación sobre la ciberseguridad en todos los niveles de las organizaciones.

Mayo de 2018 fue el mes en el que se producía la obligatoriedad del nuevo Reglamento General de Protección de Datos, publicado dos años antes. Durante estas fechas, muchas de las preocupaciones en todas las entidades venían derivadas de la implantación (o de las consecuencias de la no implantación) de las medidas necesarias para su cumplimiento.

En la tercera edición, realizamos el estudio en pleno apogeo del confinamiento por la pandemia lo que nos hizo reflexionar sobre el teletrabajo y, como novedad y complementando el contenido, incluimos varias columnas de opinión de profesionales altamente relevantes, así como un análisis estadístico realizado a partir de los resultados obtenidos por los servicios que cuentan con calificación de ciberseguridad.

En esta 4ª edición no ha habido (por suerte) ninguna circunstancia excepcional que afecte a la encuesta que se incluye en el estudio, por lo que hemos decidido mantener las novedades incluidas en la edición anterior: *opinión de expertos* y *análisis estadístico de calificaciones*, así como la temática del teletrabajo para entender cómo había sido su evaluación en estos dos años. Estos elementos, junto al análisis del resultado de la encuesta que realizamos sobre la materia, consideramos que permite tener una visión más holística sobre el Estado de la Ciberseguridad en la Cadena de Suministro y ayudar, a todas las partes interesadas, a tener una visión más general de la situación real en esta materia.

AGRADECIMIENTOS:

A nuestros columnistas:

Carlos López Blanco - Presidente de la Fundación ESYS

Jacinto Muñoz Muñoz - Director Security, Risk & Governance, MAPFRE

Antonio Navas Casado - Client Unit Leader, Kyndryl

Fátima Ballesteros Castellano – Directora de Consultoría, Trescore Proyectos

Al **Club Excelencia en Gestión**

A **todas las personas** que han participado en el estudio

Por Antonio Ramos

Conclusiones del Estudio

ESTADO DE LA CIBERSEGURIDAD EN LA CADENA DE SUMINISTRO

La **creciente preocupación y ocupación sobre la ciberseguridad de la cadena de valor** está en línea con la creciente importancia de la ciberseguridad *per se* (seguimos batiendo récords y el 95,7% de los encuestados declaran estar muy preocupados). De hecho, los niveles de interés de la Alta Dirección siguen creciendo (un 71,0% de los Consejos de Administración y un 81,9% de la Dirección General), en línea con el incremento de responsabilidad de estos órganos corporativos en materia de ciberseguridad (por supuesto propia, pero incluyendo también la de la cadena de valor).

La evolución del tamaño de la superficie a proteger se mantiene en unos niveles muy altos de proveedores relevantes para la prestación de los servicios, que se deriva de la digitalización de los modelos de negocio, y diluye el perímetro tradicional. En concreto, un 53,7% de los encuestados declara tener proveedores que se conectan a sus sistemas (proveedores conectados) y, un 48,9% afirma que gestionan su información en los propios sistemas del proveedor (proveedores no-conectados).

No podemos despreciar otros dos factores que contribuyen sustancialmente al incremento de atención:

- Los **ataques relacionados con los proveedores** que siguen por encima del 40% de los casos, aunque se han reducido ligeramente respecto a 2020 (en concreto, el 40,5% de los incidentes que han afectado a los encuestados fue originado desde sus proveedores).
- La **normativa** que exige la implementación de procesos de gestión de riesgos de terceros **no para de aumentar**. A las normas de la EBA en el sector financiero, tuvimos que sumar luego el RGPD y, a continuación, las normativas del sector asegurador (EIOPA) y para las entidades cotizadas en mercados de valores (ESMA). Y ahora están por llegar las trasposiciones de las inminentes nuevas versiones de Directivas Europeas en materia de ciberseguridad de servicios esenciales (NIS2 –

Network and Information Security) y de infraestructuras críticas (CER – *Critical Entities Resilience*) o el Reglamento sobre resiliencia para el sector financiero (DORA), y otras más lejanas, como la relativa a la ciberresiliencia para productos digitales y servicios auxiliares, que aún está en sus primeros pasos.

La creciente preocupación y ocupación sobre la ciberseguridad de la cadena de valor está en línea con la creciente importancia de la ciberseguridad per se

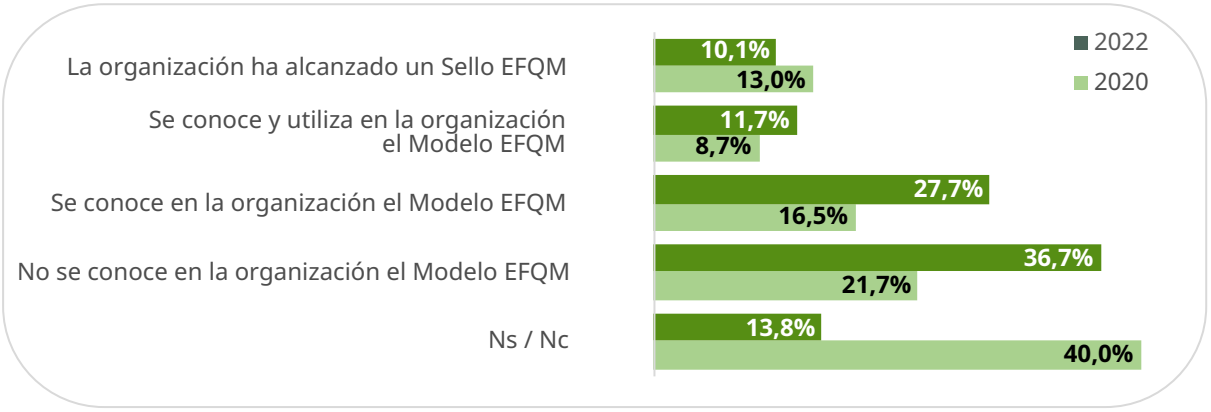
Este incremento de atención está consiguiendo que la mayoría de organizaciones estén avanzado en implementar programas de gestión de riesgos de terceros. Estos programas están orientados a disponer de información sobre el nivel de seguridad de dichos terceros, lo más fiable posible, que permita una mejor toma de decisiones. Sin embargo, implantar estos programas no es trivial dado el volumen y la disparidad de proveedores, y la escasez de recursos que se pueden dedicar al programa. Vamos a examinar a continuación el estado de situación de estos programas en la actualidad:

- En primer lugar, comentar una tendencia inquietante: Vemos que, aunque la preocupación de las áreas de compras – aprovisionamiento aumenta (pasa de un 40,5% a un 49,7%), sin embargo, sus responsabilidades en esta materia decrecen (sólo un 1,1% de estas funciones tiene responsabilidades en materia de ciberseguridad frente al 1,7% del estudio anterior).
- Aunque la concienciación va dando sus frutos y vemos que mejora el grado de supervisión del riesgo de terceros, nos encontramos que todavía sólo el 54,1% de las organizaciones lo hacen anualmente y, lo que es más preocupante, **un 14,9% de las organizaciones no evalúa en absoluto a sus proveedores**.
- Hay **dos indicadores** que siguen siendo **muy alarmantes**:
  - Uno es que **el mecanismo más utilizado, y creciendo, para evaluar proveedores son los cuestionarios de auto-evaluación** (un 63,8% frente al 46,3% del estudio anterior) cuando es comunmente conocido que las respuestas están muy condicionadas por el interés comercial que exista entre las partes. La parte positiva es que esto demuestra que cada vez hay más intención por parte de los usuarios de asegurar que la cadena de suministro cuente con un nivel de seguridad suficiente.
  - El otro indicador es que **el sistema que más confianza ofrece sobre la seguridad de un tercero es la certificación del Sistema de Gestión de Seguridad de la Información** (un 31,1% de las personas encuestadas) **a pesar de que esta certificación no aporta ninguna información sobre el nivel de seguridad del servicio**. Parece que las organizaciones acuden a ella en busca de una solución desesperada al rompecabezas de evaluar múltiples proveedores con mínimos recursos.
- Por último, ante el reto de implementar una "seguridad interdependiente" en todo el ecosistema que asegure una mejora del nivel de protección de toda la cadena de suministro y dado que las certificaciones se enfrentan al reto de la normalización de líneas base para un número casi infinito de casos de uso, **la calificación es utilizada por, prácticamente, 1 de cada 5 encuestados** para conocer de manera eficiente y construir indicadores del nivel de seguridad de todo su ecosistema productivo.

Como se puede observar en el *apartado que dedicamos a analizar los resultados de las calificaciones* en vigor, a pesar de que la mayoría de los clientes calificados tienen un SGSI certificado, la realidad es que los servicios muestran niveles de seguridad dispares, demostrando que este tipo de certificaciones no permite discriminar entre servicios, por lo que parece que se hace necesario disponer de herramientas más específicas -tal como es la calificación- que posibiliten esa diferenciación.

Conclusiones en clave EFQM

Respecto a años anteriores, se mantiene este **mayor nivel de conciencia de los trabajos realizados en gestión del riesgo que conlleva el Modelo EFQM**. Hay un mayor grado de preocupación respecto a los temas de ciberseguridad en organizaciones con Sello EFQM (un 8,8 frente a un 8,3 en organizaciones sin Sello EFQM), aunque las organizaciones con Sello EFQM no tienen diferencias sustanciales respecto un mayor nivel de ciberriesgo en su organización, respecto el año anterior (ambas un 59%).



Evolución del uso del Modelo EFQM (European Foundation for Quality Management) en las organizaciónes.

Esta mayor conciencia también se traslada al ámbito de la detección y la monitorización de la seguridad, un aspecto fundamental en la actualidad, puesto que el 54% de las organizaciones que tienen Sello EFQM son **más conscientes de haber sufrido algún ciberataque o acceso no autorizado** a sus sistemas o información en los últimos 12 meses, frente a una media del 34% en el resto de las organizaciones.

Al mismo tiempo, las organizaciones con Sello EFQM tienen unos **órganos de dirección sustancialmente más preocupados** (Consejo de Administración y Dirección General) por establecer mecanismos de seguridad (aproximadamente un 10% adicional de alta o muy alta preocupación), que es una prueba del nuevo liderazgo necesario para los tiempos que corren. También hay que señalar que un mayor nivel de inversión en medidas de ciberseguridad, respecto al año anterior, es sustancialmente más frecuente en las organizaciones con Sello EFQM, un 77% frente a un 67% en organizaciones sin Sello EFQM. A la vez que las organizaciones con Sello EFQM **disponen en mayor medida de políticas y procedimientos formales** para el desarrollo de la actividad de su organización en Teletrabajo, un 95% frente a un 83% en organizaciones sin Sello EFQM.

El disponer de un Sello EFQM no marca diferencias sustanciales, ni en la percepción que tienen del nivel alcanzado en la gestión de los riesgos y los datos, información y conocimiento desde la perspectiva del tratamiento ético y legal de datos e información (situado entre un 68% y un 70% en Alto o Muy alto), ni en el grado de preocupación por el nivel de seguridad de los terceros/proveedores con los que interactúan (entre un 7,6% y un 7,7%).

Hay que hacer mención que aun teniendo hechos claros que atestiguan este mayor interés, incluida la alta dirección, y dedicación de recursos a la ciberseguridad, la percepción que tienen las organizaciones con Sello EFQM del nivel alcanzado en la gestión de los riesgos y los datos, información y conocimiento, desde la perspectiva de los riesgos tecnológicos, es más bajo un 59% frente a un 69% en organizaciones sin Sello EFQM, sin duda relacionado también con esta mayor consciencia del riesgo.

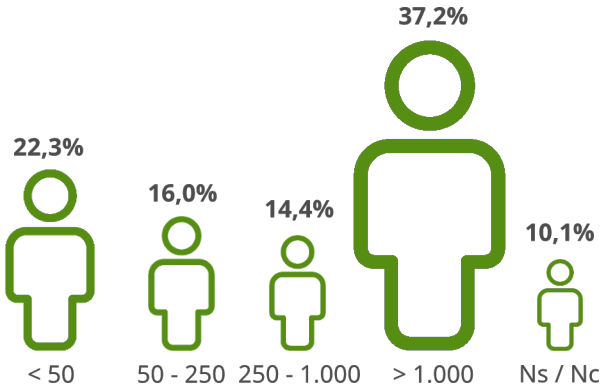
Se podría decir que **una gestión excelente, innovadora y sostenible conlleva un mejor conocimiento de la propia organización** y un trabajo de concienciación en gestión de riesgos que son, claramente, el primer paso para mejorar, y la ciberseguridad no escapa de esta máxima.

Resultados de
LA ENCUESTA

La encuesta ha sido realizada entre el 7 de marzo y el 20 de mayo de 2022 y ha sido respondida por 188 organizaciones (frente a las 115 de la edición anterior, es decir, un 63,5% más de encuestados), representadas fundamentalmente por responsables de seguridad (CSO/CISO), el 25,6%, directores generales (CEO), el 12,5% y responsables de tecnología (CIO), el 9,5% de la muestra, y siendo dos tercios pertenecientes a los sectores de Banca y Seguros, Servicios o Tecnología.

Las empresas a las que pertenecen son fundamentalmente de gran tamaño, lo cual no se corresponde con la distribución estándar del tejido empresarial de nuestro país, y se muestra en el siguiente gráfico.

Distribución de las empresas participantes según el número de empleados



APARTADOS

Los resultados del análisis están divididos en tres apartados:

01 ESCENARIO GENERAL.

En este apartado se recoge el análisis de las cuestiones del Estudio que hacen referencia al contexto general de ciberseguridad en el momento de realizar el Estudio.

02 CIBERSEGURIDAD EN LA CADENA DE SUMINISTRO.

Este apartado central reúne las reflexiones relativas al aspecto principal del Estudio: la seguridad en la cadena de suministro y, en particular, de las preguntas relacionadas con la computación en la nube, como caso paradigmático de servicio externalizado.

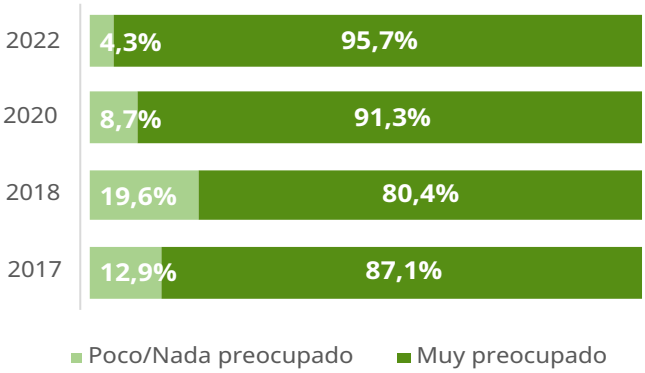
03 TELETRABAJO.

Al igual que otros años, nos gusta incluir un aspecto temático de actualidad a la hora de realizar el Estudio. En esta ocasión, repetimos el teletrabajo para entender cómo ha sido su evolución en este tiempo post-pandemia.

Relevancia de la ciberseguridad

En esta 4ª edición, el nivel de preocupación por la ciberseguridad es el más alto desde que empezamos a realizar la encuesta en 2017. En concreto, el 95,7% de las personas encuestadas han respondido que estaban muy preocupadas (por encima de 7 en una escala de 1 a 10), lo que supone un incremento de más de 15 puntos porcentuales en los últimos 4 años.

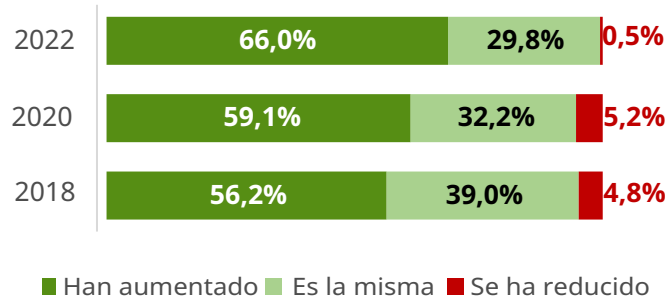
Nivel de preocupación por la ciberseguridad



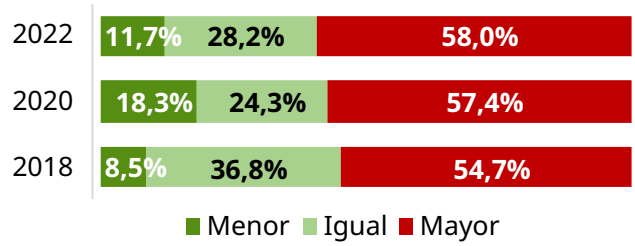
Este crecimiento de la preocupación está en línea con los ligeros crecimientos reflejados, tanto del nivel de riesgo percibido respecto al año anterior, considerado mayor por un 58,0%, frente al 57,4% en 2020, como en la inversión en ciberseguridad, que aumenta en un 66,0% de las organizaciones encuestadas (un 59,1% en 2020). Llama poderosamente la atención que **sólo un 0,5% de los encuestados declare una reducción de los presupuestos dedicados a ciberseguridad.**

Comparando estas tres magnitudes, observamos que el crecimiento de la inversión supera tanto al nivel de preocupación como el nivel de riesgo percibido (un 11,7% frente al 1,0% y el 48,6%, respectivamente) por primera

Evolución de las inversiones en ciberseguridad



Riesgo percibido en comparativa con el año anterior.



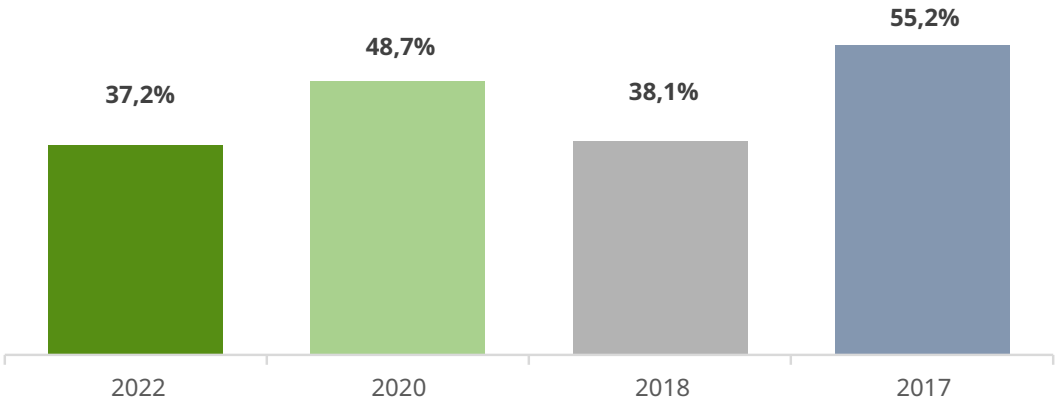
vez desde que realizamos el estudio. Es decir, todo parece indicar que, finalmente, **las organizaciones están siguiendo la máxima de invertir allí donde dicen que más preocupadas están *(put your money where your mouth is)*.**

Evolución de los ciberataques

En este apartado, volvemos a percibir una reducción en el porcentaje de empresas que declaran haber sido conscientes de haber sufrido algún incidente, tras haber aumentado en el Estudio anterior. Concretamente, el porcentaje baja en algo más de 11 puntos – casi un 24% - respecto a la edición anterior, hasta el 37,2% (rango similar al de 2018, cuando se situó en un 38,1% frente al 48,7% de 2020). De esta manera comenzamos a percibir una especie de "oleadas", es decir, años de picos seguidos de años valle. Por suerte, **la tendencia que muestra es favorable, puesto que las magnitudes de ambos se van reduciendo** respecto a los picos / valles anteriores.

Observando esta evolución podríamos decir que la inversión en ciberseguridad ha merecido la pena puesto que ha impactado en la reducción del número de incidentes. De hecho, la percepción del nivel de seguridad implementado por las organizaciones encuestadas ha mejorado ligeramente (2 puntos en materia de privacidad y 3,5 puntos en gestión de riesgos tecnológicos) aunque, nada que ver con la magnitud de la caída en el número de incidentes (recordemos, más de un 24%).

En todo caso, se mantiene cierta contradicción en los datos puesto que, aunque aproximadamente el 70% de las entidades encuestadas opinan que su nivel de preparación



Conscientes de sufrir algún incidente

es alto o muy alto, lo consideran insuficiente puesto que el 59,1% declaran, a su vez, su intención de aumentar las inversiones en ciberseguridad.

Para resolver esta disyuntiva **necesitaríamos disponer de una medida objetiva del nivel de preparación que fuera más allá de la percepción de las personas** encuestadas. Este análisis podemos realizarlo para las terceras partes evaluadas actualmente por LEET Security (*ver apartado siguiente, Ciberseguridad en la cadena de suministro*), pero sería necesario **contar con el nivel de calificación de todas las empresas encuestadas** para poder ir más allá de las sensaciones (dado que la seguridad es tan fuerte como el eslabón más débil, no se puede asegurar que cualquier inversión aumenta el nivel de seguridad, ya que solo aquellas que hagan que el nivel de seguridad de dicho punto débil sea más elevado que el anterior a la inversión, elevan realmente el nivel de seguridad de la organización. Efectivamente, hay inversiones que, aumentando ciertas capacidades de ciberseguridad, no hacen que el nivel de seguridad sea mayor). Por esta razón, la calificación también se puede utilizar como mecanismo de evaluación de inversiones en ciberseguridad, ya que permite dirigirlo hacia aquellas que, como hemos dicho, actúan sobre los puntos débiles.

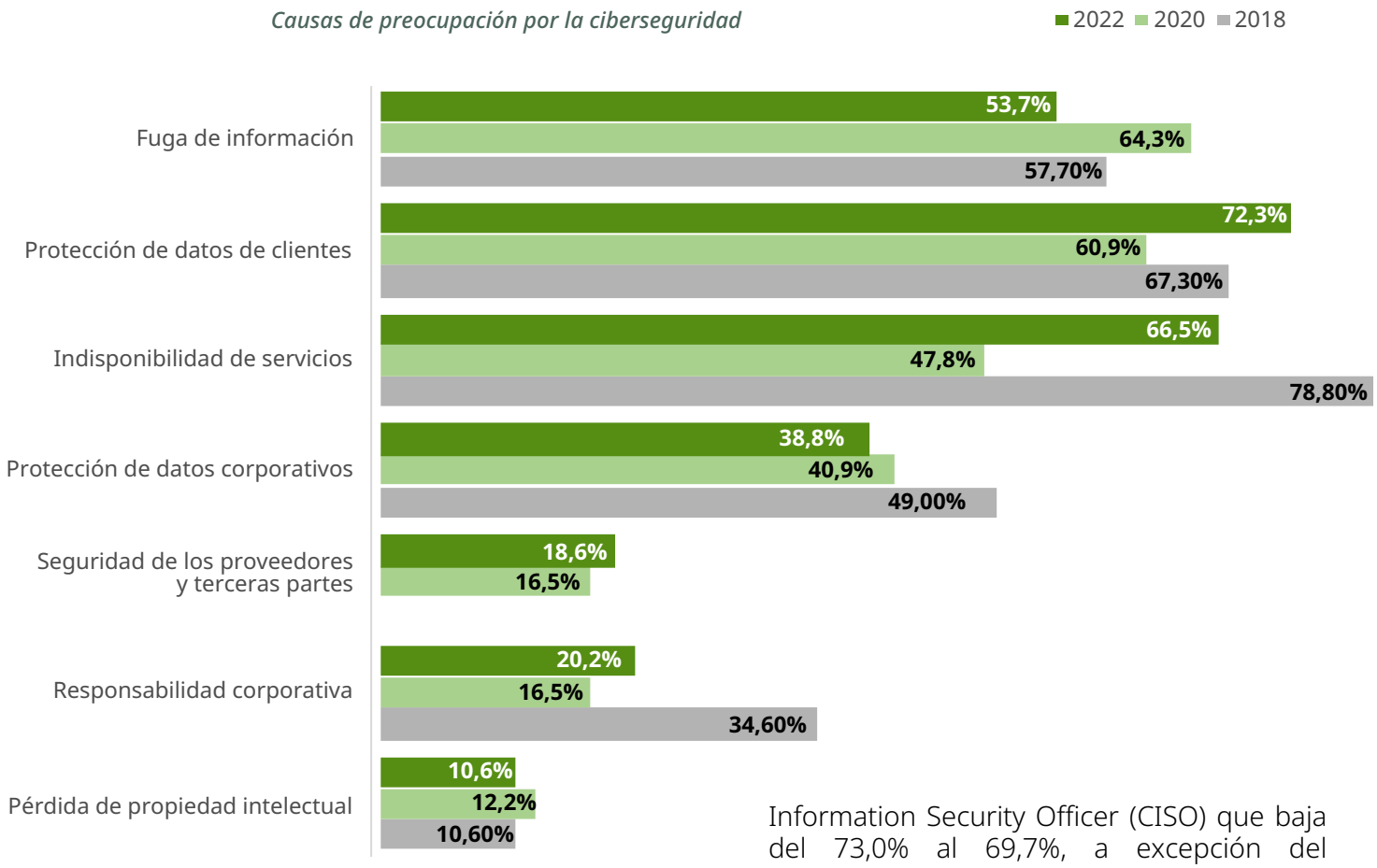
Preocupaciones principales

En función de los tipos de ataques y, en particular, de los efectos de los mismos sobre los procesos de las organizaciones, los aspectos de mayor preocupación pueden variar. En relación a esta cuestión observamos que las preocupaciones se mantienen más o menos parecidas en relación a las ediciones previas, excepto en dos aspectos:

- **La protección de datos de clientes**, que se convierte en la mayor preocupación al ser la causa de falta de sueño de un 72,3% de los encuestados, desbancando a la fuga de información (que vuelve a niveles de 2018, después del crecimiento experimentado en 2020).
- **La indisponibilidad de servicios** que, aunque no recupera los niveles de 2018, cuando preocupa a un 78,8%, sube casi 20 puntos hasta un 66,5% respecto al 47,8% de 2020.

Nivel de preparación percibido

Dado que el foco del estudio es la ciberseguridad en la cadena de suministro no



podemos dejar de analizar su situación. Tras el dato inicial de 2020 (antes no se recababa este dato), la seguridad de los terceros es causa de preocupación de un 18,6% de las entidades encuestadas (un 2,1% más que la anterior edición). Consideramos que este porcentaje es pequeño en relación a la importancia de los terceros como vectores de ataque por lo que auguramos un crecimiento de este valor en próximos estudios.

Responsabilidades en materia de ciberseguridad

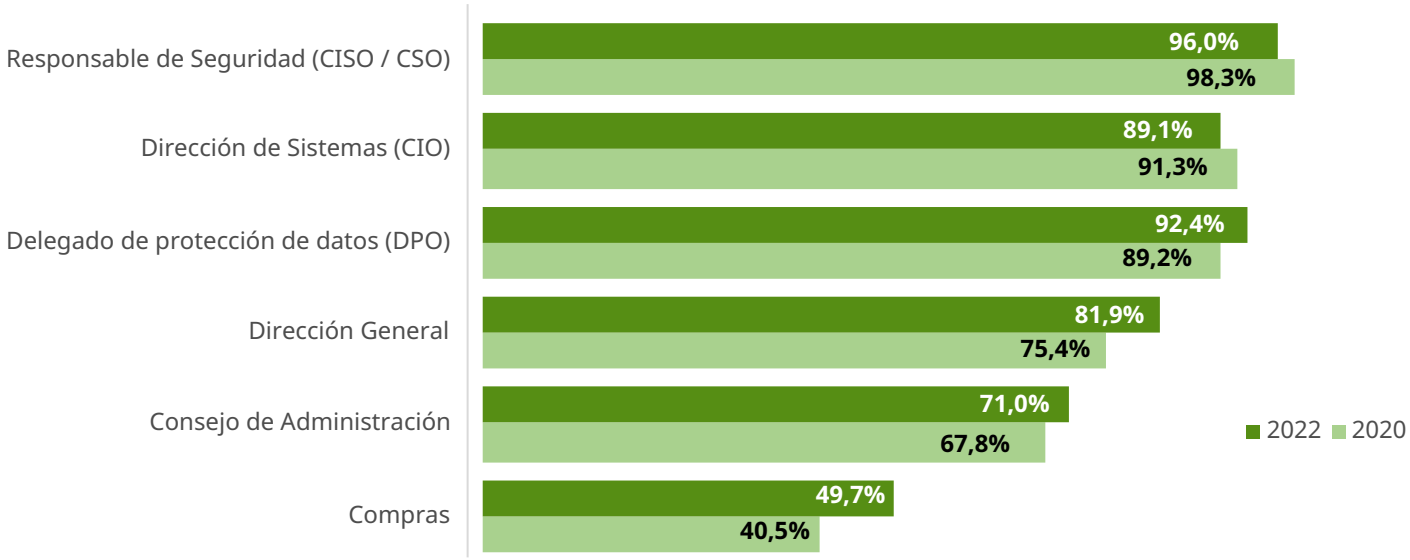
Una vez analizada la percepción del riesgo y la evolución de los ciberataques, pasamos a analizar quién asume en las organizaciones la responsabilidad sobre la ciberseguridad.

En esta 4ª edición se mantiene la importancia relativa de los roles que intervienen en la gestión de la ciberseguridad (*ver gráfico en página siguiente*) si bien es cierto que todos ellos ven reducido su porcentaje, incluido el Chief Information Security Officer (CISO) que baja del 73,0% al 69,7%, a excepción del Responsable de Sistemas (CIO) que aumenta del 44,3% al 47,9%. En todo caso, variaciones estadísticamente insignificantes.

Estas responsabilidades están en línea con la respuesta obtenida al preguntar por la preocupación de las distintas funciones en relación a la ciberseguridad, puesto que también CISO y CIO son las más preocupadas, roles a los que se une el/la Delegado/a de Protección de Datos (DPO), cuya preocupación es el 92,4% (incluso por encima del CIO, aunque sin embargo, sólo tiene responsabilidades en esta materia en un 26,1% de las organizaciones encuestadas).

Otro dato relevante es que en los Consejos de Administración y Dirección General es alta o muy alta en el 71,0% y 81,9% de las organizaciones, es decir, una subida de alrededor de 5 puntos respecto a la edición anterior. Sin duda, **la ciberseguridad es una de las mayores y crecientes preocupaciones de los órganos de gobierno**, lo cual encaja también con los incrementos de presupuestos mencionados anteriormente.

Preocupación por la ciberseguridad por funciones

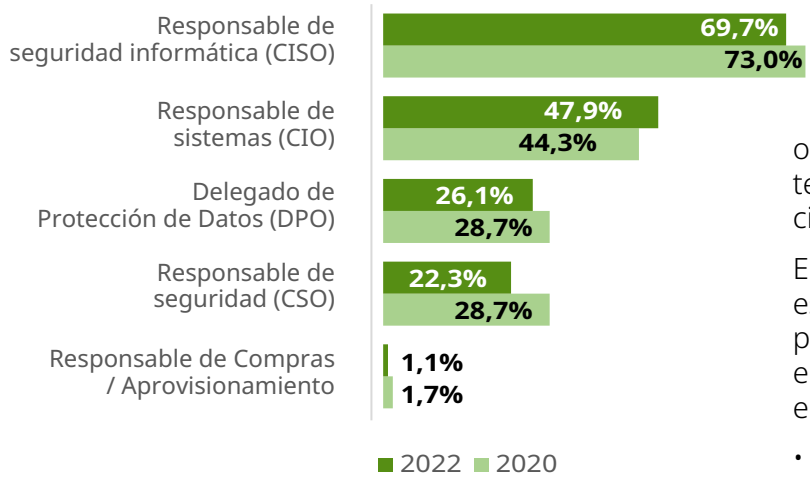


CIBERSEGURIDAD EN LA CADENA DE SUMINISTRO

Gestión de los riesgos de terceras partes

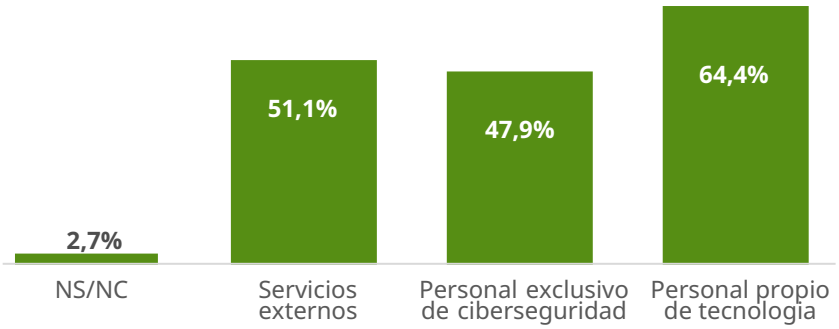
Uno de los retos para incrementar la ciberseguridad de la cadena de suministro es que la implementación de mejoras en este ámbito requiere de la colaboración de los responsables de aprovisionamiento y los de ciberseguridad. De hecho, en esta edición, como nota positiva, podemos comprobar (como se indica en el apartado anterior) que ha aumentado la preocupación de las áreas de compras / aprovisionamiento por la ciberseguridad, habiendo pasado de un 40,5% a un 49,7% los que muestran un nivel de preocupación alto o muy alto. Siendo un avance, sin duda, todavía queda mucho por hacer, sobre todo si nos fijamos en que tan sólo en un 1,1% de las organizaciones encuestadas esta área declara tener alguna responsabilidad en materia de ciberseguridad.

Funciones con responsabilidad en ciberseguridad



En esta edición hemos añadido al análisis de este aspecto el tipo de recursos que se utilizan para la gestión de la seguridad y nos encontramos con una situación muy equilibrada entre las diferentes opciones:

- Dos de cada tres organizaciones utilizan personal propio del área de tecnología



Recursos encargados de la gestión de la ciberseguridad

- Y aproximadamente una de cada dos, utiliza personal exclusivo de ciberseguridad y servicios externos.

En estos momentos en los que contratar personal de ciberseguridad es un reto para muchas organizaciones, prestaremos atención a cómo evolucionan estas cifras.

Evolución del riesgo de terceros

Indudablemente, a medida que la gestión de riesgo de terceros se está convirtiendo en un tema recurrente, el nivel de concienciación va aumentando. De hecho en esta edición, **el 80,3% de los encuestados dicen estar muy preocupados por la seguridad de sus proveedores**, es decir, más de 4 de cada 5 respuestas (con un crecimiento superior a 10 puntos).

Obviamente también contribuye a esta circunstancia la creciente importancia que tienen los proveedores para el funcionamiento de nuestras organizaciones, ya que es habitual que los proveedores se conecten a los sistemas internos de las organizaciones ("proveedores conectados") o también que gestionen información de clientes en sus propios sistemas ("proveedores no conectados"). En esta edición hemos visto cierta reducción en la permeabilidad hacia terceros habiéndose reducido ambas casuísticas alrededor de 7 puntos:

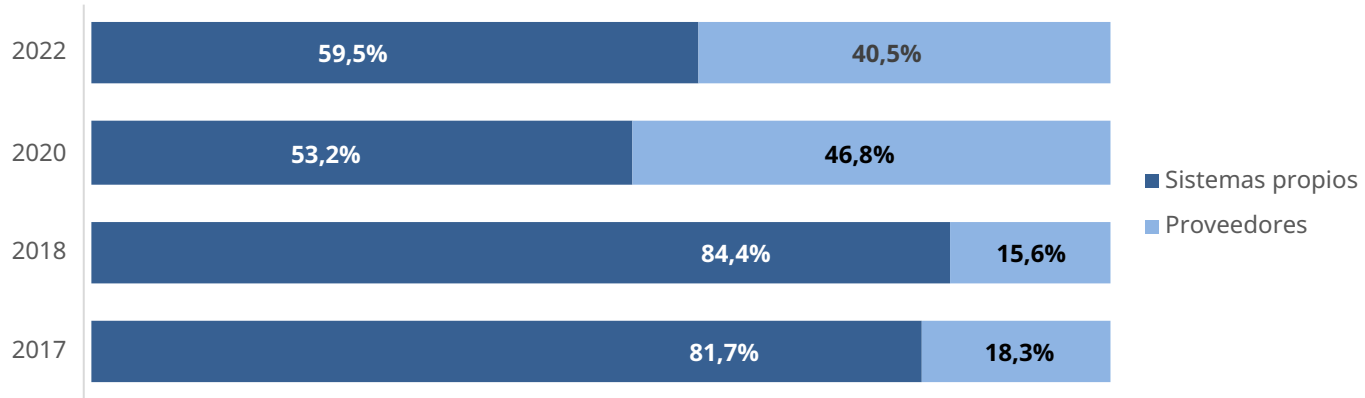
- Los proveedores conectados han pasado de estar presentes en un 60,9% de los casos en 2020 a un 53,7% en esta 4ª edición (recordemos que venían de un incremento de un 55% en el anterior estudio).
- Y los no conectados, también bajan de un 55,7% hasta un 48,9%

En cualquier caso, **en alrededor la mitad de las organizaciones existen proveedores externos que impactan en su nivel de ciberseguridad**.

De hecho, existen motivos para ese nivel de preocupación puesto que, según las personas encuestadas conscientes de haber sufrido un incidente y que son conocedoras del origen del mismo, el 40,5% (6 puntos menos que en la anterior edición) de esos incidentes tuvieron a

Preocupación por la ciberseguridad por funciones

Origen de los incidentes de seguridad



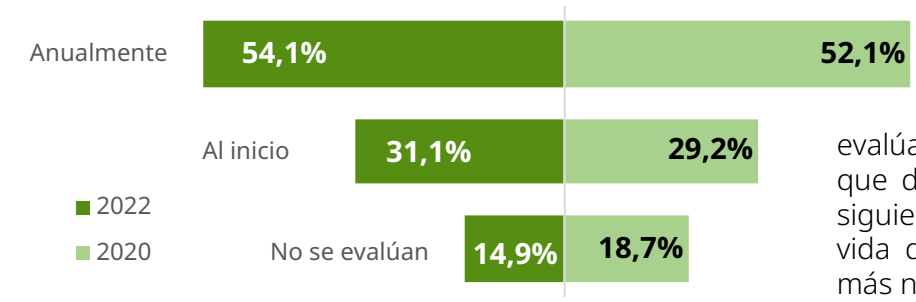
los proveedores como vector de ataque. Este porcentaje supone que **casi la mitad del riesgo de una organización depende del nivel de protección de su cadena de suministro**.

Análisis de los mecanismos de GRT

Al igual que en ediciones anteriores, hemos preguntado también por los mecanismos utilizados para gestionar el riesgo de terceros (GRT) y, como decíamos anteriormente, se aprecia un mayor grado de concienciación de las organizaciones en esta materia, también en los mecanismos empleados.

En primer lugar, respecto a la periodicidad aplicada, aunque la situación sigue mejorando,

Frecuencia de evaluación de proveedores



ya que la evaluación anual de terceros vuelve a crecer ligeramente, pasando de un 52,1% en 2020 a un 54,1% en 2022, sigue siendo **muy preocupante que, a estas alturas, todavía un 14,9% de las organizaciones no realicen ningún tipo de evaluación a sus proveedores** y pone de manifiesto que siguen siendo necesarios esfuerzos de concienciación en esta materia.

Si tenemos en cuenta el tipo de organizaciones que han respondido, cuya madurez es superior a la media, cabe esperar que este porcentaje sea muy superior en un contexto más generalizado

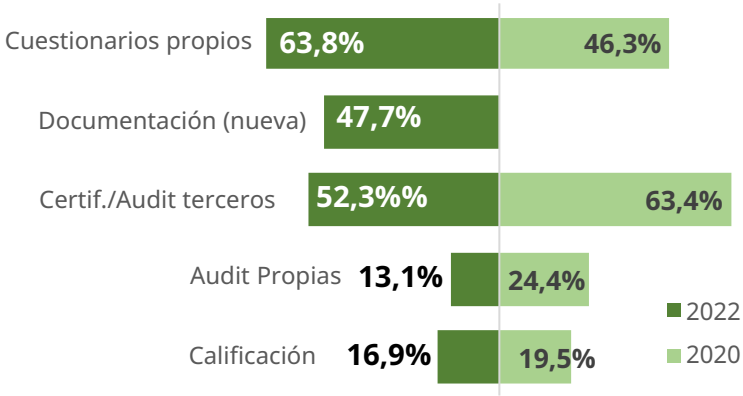
La calificación y la GRT

Una vez visto el contexto de la gestión de riesgos de terceros, analizamos la utilización de la calificación como herramienta para la gestión de la ciberseguridad en la cadena de valor. Tras incluir esta pregunta en la pasada edición, podemos derivar algunas conclusiones de la evolución de las respuestas obtenidas:

- **Los cuestionarios propios se convierten en la opción más utilizada a pesar del reducido nivel de garantía que suponen**; de hecho han aumentado su relevancia en un 38%, pasando de un 46,3% a un 63,8%.
- El resto de métodos baja proporcionalmente (la certificación / auditoría de terceros baja un 17,5%, las auditorías propias en un 46% y la calificación, que es la que menos baja, en un 13%).

Estas respuestas demuestran que, si consideramos el proceso de evolución habitual de los procesos de gestión de riesgos de terceros, estamos en el segundo estadio (basado en hoja de cálculo) en el que cada entidad "valida" sus propios requisitos con las respuestas que el proveedor da a una serie de preguntas.

Y si volvemos por un momento al aspecto de la periodicidad, vemos que hay un 31,1% de organizaciones que evalúa los proveedores al inicio del servicio lo que demuestra que están avanzando hacia el siguiente estadio (integración con el ciclo de vida de servicios), aunque todavía no son las más numerosas.



Métodos de evaluación de proveedores

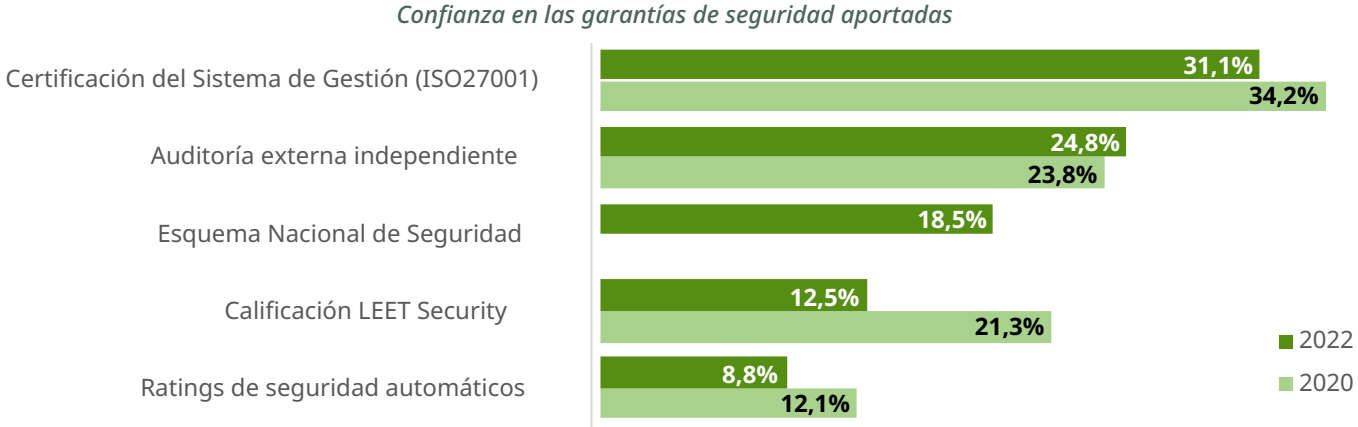
Llama la atención la reducción en el uso de auditoría propias, pero no deja de ser una evolución esperada puesto que las empresas usuarias de servicios no pueden dedicar recursos de manera exhaustiva y extensiva para auditar a sus proveedores, sino que éstos deben llegar a sus clientes perfectamente auditados

(éste es el principio que ha puesto en valor el sector financiero español con el lanzamiento del *servicio Pinakes* para evaluación de la seguridad en la cadena de suministro).

Entrando de manera específica en los usos de la calificación por las organizaciones encuestadas, **el uso más habitual sigue siendo la evaluación del nivel de seguridad de la organización** (54,3%) **y la demostración de cumplimiento** (26,0%).

Finalmente, para poner en relación la calificación con el resto de mecanismos, preguntamos a los usuarios de estos servicios qué mecanismos les aportan más garantías a la hora de entender el nivel de seguridad de los mismos. La mayoría aún se decanta por la certificación del sistema de gestión conforme a la norma ISO/IEC 27001 (en concreto, en un 31,1% de los casos), a pesar de que es ampliamente conocido que **la certificación de un sistema de gestión, como la ISO 27001, no aporta ninguna información sobre el nivel de seguridad de un servicio**, puesto que evalúa otro aspecto, el sistema de gestión que, por definición, es compatible tanto con niveles altos como bajos de seguridad. Esta circunstancia nos parece muy preocupante porque puede conllevar una **falsa sensación de seguridad a los usuarios** de dichos servicios que, obviamente, cuando sean conscientes de ello, será demasiado tarde porque el impacto ya se habrá materializado.

En este aspecto, el mecanismo más detallado, que podrían ser las auditorías independientes son el segundo elemento mejor valorado (un



24,8%), seguido del Esquema Nacional de Seguridad (un 18,5%) que se une en esta edición a las opciones evaluadas.

En cuanto a las calificaciones de seguridad, bajan su porcentaje, aunque la calificación de LEET Security sigue siendo un 50% más fiable que los ratings automáticos. Analizada la diferencia con respecto a la edición anterior, consideramos que la diferencia en este ámbito responde al gran incremento de encuestados que ha supuesto la incorporación de organizaciones con un menor conocimiento de este mecanismo y poniendo de manifiesto la labor de concienciación que queda por hacer en esta materia.

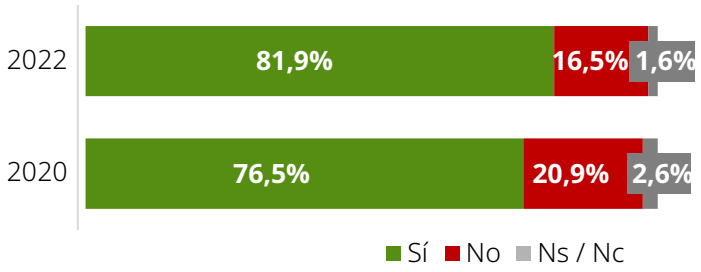
TELETRABAJO

Teletrabajo: pre y post-COVID

Debido al contexto en el que realizamos el III Estudio, en pleno confinamiento al que nos había obligado la pandemia COVID-19, nos parecía útil repetir las preguntas que hicimos en aquel momento para ver cómo había evolucionado la ciberseguridad en el teletrabajo.

La primera conclusión llamativa es que, 2 años después, ha aumentado hasta el **81,9% el porcentaje de organizaciones que dicen disponer de una política de teletrabajo**, lo que supone un incremento de más de 5 puntos. Es decir, 8 de cada 10 organizaciones han regulado ya cómo se puede acceder al teletrabajo.

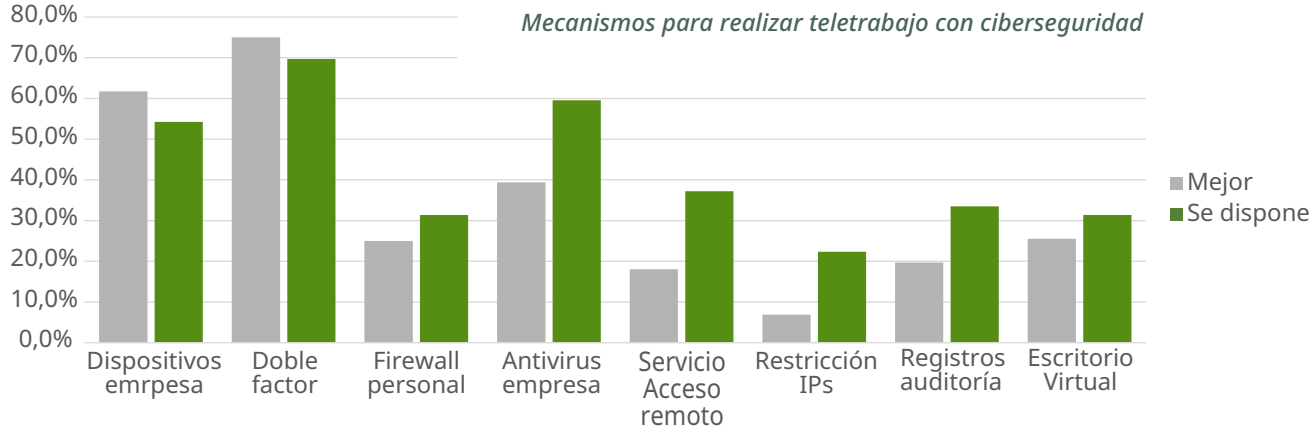
Disponen de políticas de teletrabajo



Al margen de esta preparación, las personas encuestadas siguen considerando que los dos factores fundamentales para teletrabajar con ciberseguridad son el doble factor de autenticación en todas las conexiones remotas (69,7%) y la limitación de las conexiones únicamente desde equipos proporcionados y controlados por la empresa (54,3%). El resto de factores están bastante lejanos siendo el tercero, con un 39,4%, utilizar un antivirus gestionado por la empresa.

Por otra parte, cuando se analizan los mecanismos efectivamente implementados por las organizaciones para habilitar este trabajo nos encontramos con que destacan por encima del 50%, precisamente el doble factor (75,0%), los dispositivos corporativos (54,3%) y el antivirus corporativo (59,6%), aunque podemos decir que **coinciden las medidas de seguridad para teletrabajar más importantes con las más implementadas**.

Mecanismos para realizar teletrabajo con ciberseguridad

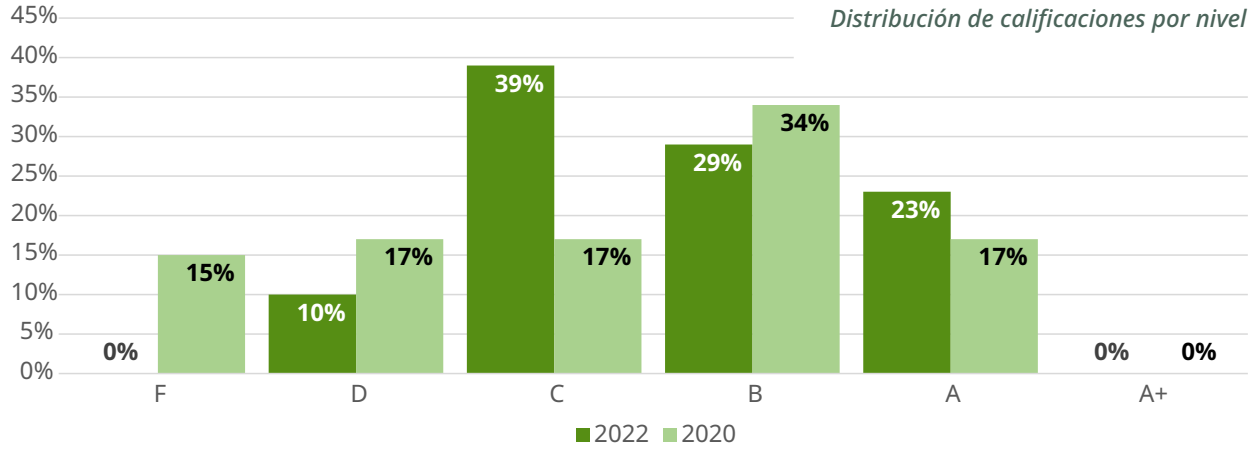


Análisis estadísticos de CALIFICACIONES EMITIDAS

Incorporamos nuevamente a los resultados de la encuesta un análisis de nivel de los resultados obtenidos de las calificaciones realizadas por LEET Security durante los últimos 12 meses.

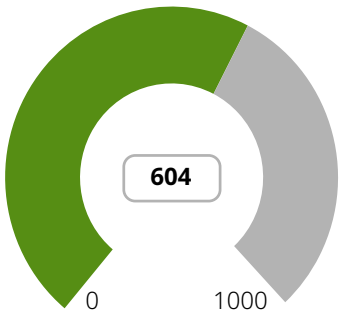
La calificación de LEET Security se otorga en cinco niveles (desde el D, el más básico, hasta el A+, con el máximo nivel de seguridad) en las tres dimensiones de Confidencialidad, Integridad y Disponibilidad. La distribución de los resultados globales obtenidos se refleja en la siguiente tabla:

Distribución de calificaciones por nivel



Teniendo en cuenta que el 90% de los servicios calificados son renovados año tras año, esta gráfica pone de manifiesto que ha habido una mejoría significativa: las calificaciones resultantes en niveles F (no se alcanza el mínimo) y D, se han movido en 2022 hacia el C, que supone un nivel más que aceptable. Y en los niveles altos, ha habido un desplazamiento desde B hacia el A (aunque A+ sigue resultando inalcanzable).

Calificación cuantitativa



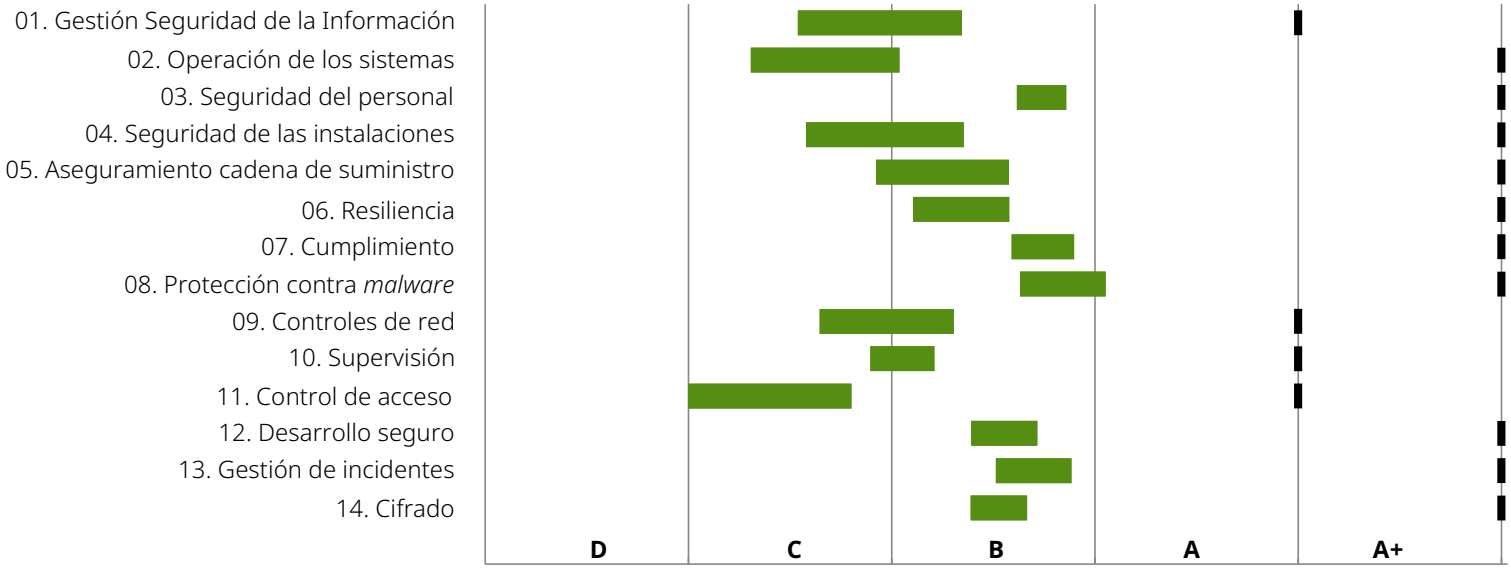
Nuestra conclusión es que **los usuarios de la calificación disponen de una herramienta que no solo les aporta una valoración de su nivel actual, sino que, además, les proporciona un modelo para canalizar sus recursos y mejorar sus capacidades de ciberseguridad.**

Con la versión 3 de nuestra metodología, que entró en vigor en la segunda mitad del pasado año, hemos incorporado la calificación cuantitativa: un valor de 0 a 1000 que muestra un índice global de los resultados obtenidos en las 73 secciones, con especial ponderación de

aquellas que tienen en consideración la prevención y detección temprana y la capacidad de recuperación. La media obtenida para este indicador es de 604, si bien, debido a la aun corta vida de este indicador, el mismo cuenta con 25 calificaciones a la fecha de producción de este dato.

La calificación también proporciona un resultado muy detallado. La siguiente tabla muestra las valoraciones medias (mostrando el rango entre sus resultados base y ponderado), así como las máximas que se han obtenido, para los 14 dominios que constituyen el marco de controles de LEET Security:

Resultado de las calificaciones en 14 dominios



El dominio que presenta un mejor resultado es el de protección frente a *malware*, debido a que el empleo de sistemas antivirus cuenta con un nivel de madurez elevado, al resultar una de las prácticas más generalizadas y tradicionales en la protección de los sistemas. Sin embargo, observamos un claro deterioro de los resultados obtenidos en control de acceso, sin duda derivado del fortalecimiento de los requisitos establecidos para este dominio en la nueva versión.

Aunque han mejorado ligeramente respecto a la anterior edición del estudio, la Operación de los sistemas sigue presentando algunos aspectos débiles, particularmente en las secciones de Gestión de la información y el conocimiento, y de Control de vulnerabilidades, siendo este un aspecto especialmente preocupante dada la importancia del mantenimiento de actualizaciones y 'parcheos' para prevenir todo tipo de incidentes de seguridad.

Aunque los resultados obtenidos en el dominio de Aseguramiento de la cadena de suministro se encuentran en la media, cabe señalar que se ha constatado cierta debilidad en la sección de Gestión de terceras/cuartas partes, en la que debería plantearse un mayor foco, teniendo en consideración el elevado número de incidentes relacionados con proveedores.

Consideramos también importante hacer una valoración relativa a las diferentes tipologías de servicios, de las que mencionamos únicamente aquellos que cuentan con un número relevante de casos calificados, y que se corresponden con el 75% de todos ellos:

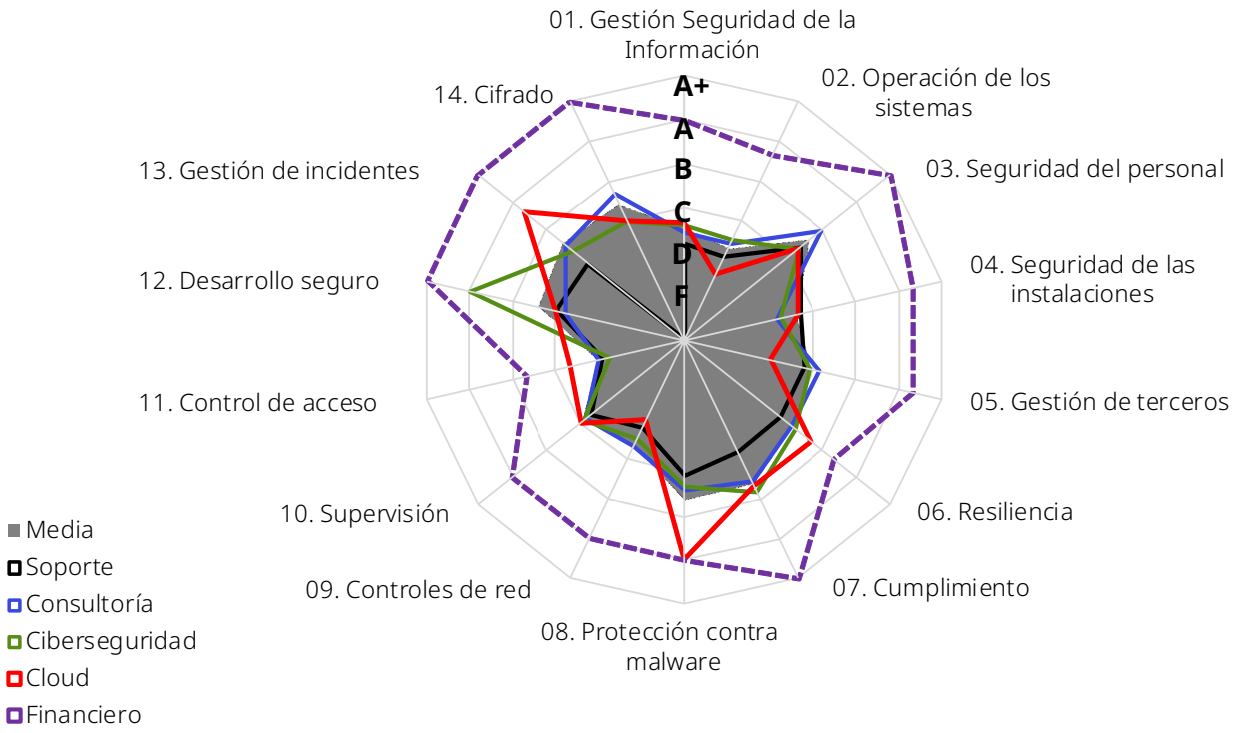
- Soporte de sistemas y aplicaciones mediante conexión remota al cliente
- Consultoría
- Servicios y centros de seguridad gestionada
- Servicios Cloud (IaaS y PaaS)

Los resultados obtenidos para cada uno de los 14 dominios que constituyen el marco de controles de LEET Security se muestran en la siguiente gráfica (el punto central denota que el dominio de Cifrado no ha resultado de aplicación en ninguno de los casos de servicio de soporte).

Adicionalmente, hemos representado los resultados obtenidos por dos organizaciones cuyos servicios son críticos para la operativa del sector financiero, en los que se pone de manifiesto el alto nivel de seguridad ofrecido por ambas, en consonancia con la gran madurez y elevado grado de exigencia del sector.

La calificación de LEET Security es pública, pudiendo consultarse en *www.leetsecurity.com/servicios-calificados*

Comparativa de resultados sectoriales



Cárlos López Blanco
Presidente, **Fundación ESYS (Empresa, Seguridad y Sociedad)**

Los nuevos retos de la (ciber)seguridad

En los dos últimos años hemos vivido varios acontecimientos de carácter distópico, es decir eventos que nadie podía haber imaginado que llegarían suceder: una epidemia/pandemia cuyo precedente más cercano, la mal llamada gripe española, tiene más de 100 años y una guerra, la de Ucrania, más cercana al siglo XX que al siglo XXI. Estos acontecimientos han afectado muy especialmente a la globalización y a la digitalización de la sociedad española y global.

Cuando en 1989 el mundo se asomaba expectante y optimista a la caída del muro de Berlín pocos podían sospechar que el siglo XXI nos iba a hacer testigos de estos eventos excepcionales.

Estos cambios vienen a incidir en numerosos aspectos tales como la Digitalización, la situación económica o la Globalización tal y como la conocemos, pero afectan muy especialmente a una realidad, la seguridad y la ciberseguridad, que ya estaba sometida a desafíos muy radicales en un entorno de transición desde la seguridad tradicional a la seguridad digital.

Para la Fundación ESYS ha llegado el tiempo de dejar de hablar de estas dos categorías para referirnos solo a la seguridad en la Sociedad Digital: la sociedad y la economía están inmersas en un proceso de acelerada digitalización de la que la seguridad no puede permanecer ajeno.

En este contexto general estamos contemplando cambios más específicos que afectan a la realidad de las empresas; permítanme destacar dos de ellos.

Hemos visto surgir, en primer término, nuevos/viejos retos como la continuidad de negocio o la protección de los activos físicos en un entorno de teletrabajo masivo junto con la irrupción de nuevos desafíos provenientes de un mundo de una delincuencia tecnológica cada vez más sofisticada no solo en sus medios sino en sus motivaciones: poco queda del pirata informático en los actuales delincuentes cibernéticos, mucho más sofisticados y movidos incluso por motivaciones no solo económicas sino políticas.

Así, el ataque a Colonial Pipeline nos ha situado frente al espejo de una realidad que se va ampliando, la responsabilidad de la cadena de suministro pero desde una perspectiva nueva: los ataques de triple extorsión invierten la tradicional ecuación del suministrador como fuente de riesgo y nos han puesto de actualidad la realidad de un suministrador víctima colateral de un ataque a su cliente suministrado, con nuevos aspectos de responsabilidad contractuales en materia de seguridad que van a tener importantes implicaciones a medio y largo plazo y cambiar en buena medida la responsabilidad en la cadena de suministro tal y como la conocemos hoy.

El otro cambio viene de la mano del tsunami regulatorio digital que estamos experimentando en Europa y no es otro que la publicación y aplicación de la Directiva NIS 2 y más concretamente su impacto en la formación de los Consejos y las direcciones de las

empresas en materia de Ciberseguridad.

Esta responsabilidad está sometida a nuevos retos cada vez más complejos, pero a la vez se mantiene incólume en cuanto a la extensión de la responsabilidad de los Órganos de Administración. Dicho de otra manera, a muchas empresas - y a todas las grandes - les esperan un horizonte de especial responsabilidad regulatoria que exigirá una diligencia específica mayor y un esfuerzo efectivo de formación.

Vamos a ver en los próximos años un cambio de sensibilidad y actitud en cuanto a la responsabilidad de los Consejos en esta materia, que deberá ser abordada no solo por los especialistas, especialmente los CISOs, sino que se proyectará muy significativamente en unos órganos de Administración compuestos por personas de alta cualificación, pero no siempre un entendimiento cabal de los riesgos y responsabilidades en materia tecnológica y de ciberseguridad.

Jacinto Muñoz
Director Security, Risk & Governance, **MAPFRE**

Buscando el pragmatismo en la gestión del riesgo de seguridad de terceros

Disponer de un adecuado proceso de gestión del riesgo de seguridad de terceros es un elemento absolutamente relevante en la estrategia de protección de las compañías. Estamos inmersos en un escenario de incremento exponencial de la amenaza, con unos ciber ataques altamente sofisticados que utilizan como puerta de entrada terceras compañías que proporcionan productos y/o están conectadas a los objetivos finales de los atacantes. Lo anteriormente mencionado, así como la demanda de información al respecto por parte de reguladores, clientes y resto de grupos de interés, hacen que garantizar que los terceros con los que trabajamos tengan un nivel de seguridad equiparable al nuestro sea un objetivo de primer nivel.

Por otro lado, este necesario proceso de gestión del riesgo de seguridad de los terceros no puede definirse ni ejecutarse como un elemento ajeno o un cuerpo extraño al resto de procesos ya establecidos en las compañías, sino que debe estar perfectamente integrado en la homologación, contratación, supervisión de la ejecución y cierre existentes, y en general, en los procesos de relación entre la compañía y sus proveedores a lo largo del ciclo de vida de dicha relación. Para conseguirlo, una cuestión clave es la involucración y apoyo de las áreas de compras y contratación, tratando por otro lado de provocar el menor impacto operativo posible en las mismas.

En lo que respecta al tercero cuyo eventual riesgo hay que gestionar, en MAPFRE

entendemos que los requisitos de seguridad exigibles al mismo deben ser acordes con el riesgo de seguridad de la actividad, servicio o proyecto que va a prestar, solicitando más requisitos y mayor detalle de información al proveedor que presta un servicio de riesgo crítico que a aquel que va a desarrollar una actuación que tenga un riesgo bajo. De esto modo, se maximiza la eficiencia y eficacia del proceso, prestando más atención y recursos a lo realmente importante.

Para lograr lo anterior, es necesario disponer de un método de evaluación que permita solicitar requerimientos de seguridad (y evaluarlos) en función del riesgo de la actividad y que dicho método esté basado en normas y estándares comúnmente aceptados, de tal modo que el tercero analizado pudiera llegar a obtener valor del propio proceso de análisis (y de su resultado). Por ello, en MAPFRE hemos seleccionado a LEET Security como pieza clave en la evaluación de seguridad de los terceros que trabajan con nosotros, con objeto de disponer de un "rating" que proporcione además el nivel de detalle suficiente como para entender el resultado obtenido y definir planes de acción con el proveedor para mejorarlo (caso de ser necesario).

Antonio Navas
Client Unit Leader (IT Infraestructures, Cloud & Cybersecurity), **Kyndryl Iberia**

kyndryl

Ciberseguridad: dos vectores de ataque contra las empresas, sus empleados, y sus proveedores.

El año 2020 fue un año disruptivo en muchos aspectos, para todos fue el año que empezó con la pandemia de la COVID-19, que en el ámbito de la ciberseguridad ha supuesto un reto sin precedentes para los responsables de proteger nuestras organizaciones, pero además, para dichos profesionales, el año terminó igual de mal, con uno de los mayores ataques a la cadena de suministro conocidos hasta el momento, el ataque de Solarwinds. Tanto la COVID-19 como el ataque de Solarwinds no hicieron más que poner el foco en problemas ya existentes, pero agravando su impacto y acelerando sus consecuencias, y por tanto generando la necesidad urgente de actuar sobre ellos.

Probablemente la principal consecuencia en el ámbito de las tecnologías de la información provocada por la pandemia ha sido la aceleración de la transformación digital de las compañías. Dicha transformación ha conllevado en muchos casos el movimiento de los sistemas a la nube, mientras al mismo tiempo, en las mismas compañías, se ha producido otro

movimiento masivo, esta vez "obligado", al trabajo desde casa.

Por los dos movimientos anteriores, para los profesionales de la ciberseguridad la pandemia supuso un problema fundamental que se puede resumir en tres palabras "incremento (de la) superficie (de) ataque".

Efectivamente, cuando las empresas que se habían preocupado en el pasado por la seguridad creían haber dejado razonablemente cubierta la seguridad de su perímetro, de un día para otro, con la irrupción del teletrabajo masivo, las personas pasaron a ser el perímetro.

En el informe DBIR 2021 se reflejan las consecuencias de lo comentado anteriormente de la siguiente forma: el 85% de las brechas de seguridad estudiadas en 2021 involucran al "elemento humano". Para empeorar las cosas, resulta que nuestros adversarios ya tenían el foco puesto en las personas antes de que empezara todo esto. En el informe DBIR 2019 se refleja que el 94% de las brechas de seguridad comenzaban en dicho año por ataques orientados a personas a través del correo electrónico.

Como hemos comentado, 2020 empezó mal y acabó igual de mal, con uno de los mayores ataques registrados a la cadena de suministro. Este tipo de ataques se caracterizan por cómo empiezan, por ejemplo, manipulando un código fuente en origen, y aprovechando la capacidad del fabricante de dicho código de distribuir dicho software de manera rápida y generalizada a todos sus clientes. Son, como se puede ver, ataques muy creativos, y no son nuevos. Ya en 2012 y 2014 tenemos referencias de ataques a la cadena de suministro que afectaron al fabricante Juniper, en el que los atacantes modificaron su código fuente insertando unas puertas traseras en él.

Y en 2017, como nos cuenta Ben Buchanan en su magnífico libro “The Hacker and the State”, el mayor ataque de ransomware conocido hasta la fecha, empezó también como un ataque a la cadena de suministro. En este caso los atacantes se aprovecharon del sistema de actualización de software de un fabricante de una herramienta financiera muy usada y extendida por las empresas en Ucrania para pagar impuestos. Comprometieron al fabricante de dicho código, accediendo a sus sistemas y robando la clave de administrador. Después realizaron el movimiento clave, la manipulación del código fuente, lo que resultó ser un trabajo minucioso y brillante, pues dicho código ocupaba 1,5 Gb de tamaño (unas 250.00 páginas si estuviera escrito en texto en hojas de papel). Cuando el código estuvo listo para ser descargado, los usuarios que pensaban que estaban descargando una versión mejorada del software descargaron en su lugar software malicioso. dicho código malicioso permitía a los atacantes realizar reconocimientos remotos de los sistemas infectados y además la descarga de software malicioso adicional en dichos sistemas. Así fue como distribuyeron el ransomware que después fue llamado NotPetya.

Los ataques directos a las personas y los enfocados a la cadena de suministro se vienen produciendo y anunciando ya desde hace tiempo y parecen ataques para los que las organizaciones sufren en exceso al enfrentarse a ellos. 2022 puede ser un año magnífico para reforzarse contra los ciberataques teniendo en cuenta cada uno su perfil de riesgo. Empecemos.

Fátima Ballesteros
Directora de Consultoría,
Trescore Proyectos

La ciberseguridad, el mayor de tus riesgos latentes.

Vivimos una época muy complicada. A las secuelas de la COVID-19 en la población se ha sumado un escenario empresarial que es harto complejo. Las empresas que no se han adaptado a los retos de la transformación digital viven una de las crisis más complicadas de la historia. A esto se une que en las pymes españolas se tiene la creencia de que estos asuntos son del informático. Ello hace que se genere un caldo de cultivo perfecto para que los riesgos asociados a la ciberseguridad se conviertan en problemas de mayor índole.

Si este escenario lo extendemos a más allá de las organizaciones, nos damos cuenta de que no estamos siendo capaces de asegurar que no habrá incidencias maliciosas y riesgos graves en toda la cadena de valor. Por ello, tenemos que poner el foco y establecer como prioridad un modelo de gestión en el que prime el control no solo de los sucesos propios sino también aquellos relacionados con proveedores y usuarios.

Las empresas empiezan ahora en pleno 2022 a tomarse en serio estos aspectos de ciberseguridad. Existe un boom de certificaciones ISO 27001 y en la administración pública se comienza a requerir cumplir con el Esquema Nacional de Seguridad (ENS). Estos estándares apoyan que las organizaciones controlen, minimicen y mejoren sus comportamientos en materia de seguridad informática y protección, aunque no son los más avanzados.

En el último año, aquellos sectores que cuentan con procesos críticos están empezando a evaluar la conveniencia de trabajar con estos referenciales. Algunos de ellos, como la banca, cuyos mecanismos con complejos, han puesto foco en dar un nivel más a la gestión y buscan mecanismos que aumenten la seguridad tanto física como informática. Por ello, nacen ratings de ciberseguridad como el que diseña Leet Security o el estándar Pinakes que promueve el Centro de Cooperación Interbancaria (CCI). Estos nuevos referenciales de ciberseguridad tratan de aunar lo mejor de cada enfoque en la materia tanto de buenas prácticas como de control y se están erigiendo en el futuro para asegurar que cada entidad realiza el máximo para minimizar los riesgos.

Aunque pueda parecer complicado, certificarse en un nivel de seguridad Leet o Pinakes no requiere más que ser pertinente en los controles y contar con un apoyo firme de las estructuras directivas y de gestión. En Trescore Proyectos ya hemos conseguido que alguno de nuestros clientes se certifiquen en los niveles más altos. Lo hemos hecho aunando, no solo una integración total con el sistema de gestión que se aplica, sino con una capacidad de generar alertas y mediciones que hacen que la confianza crezca en toda la cadena de valor.

PATH FORWARD

5 Consejos para dominar la gestión del riesgo de terceros

Para aquellas organizaciones que quieran mejorar la seguridad de sus terceros les recomendamos trabajar en los siguientes aspectos:

01 **INVOLUCRAR A TODOS LOS ACTORES CORPORATIVOS**

No es posible gestionar el riesgo de terceros eficaz y eficientemente si no se implican todas las áreas afectadas: Negocio, Compras, Cumplimiento, DPD, Riesgos y Ciberseguridad.

02 **DISEÑAR UN PROCESO HOLÍSTICO**

El hecho de estar en una posición débil de defensa hace que el menor resquicio pueda generar un incidente significativo, por ello el proceso debe abordar todas las relaciones con terceros (no solo proveedores).

03 **INTEGRAR LA CIBERSEGURIDAD COMO OTRO RIESGO MÁS EN EL PROCESO DE APROVISIONAMIENTO**

La ciberseguridad debe formar parte de la negociación con el mismo proveedor en la misma medida que el resto de componentes del servicio.

04 **IDENTIFICAR Y CARACTERIZAR EL INVENTARIO DE SERVICIOS DE TERCEROS**

Lo que no se conoce no se puede proteger; es necesario saber cuántos servicios se han subcontratado y cómo de críticos son para nuestra organización.

05 **CONFÍE PERO VERIFIQUE**

Los cuestionarios no son fiables y tampoco los sistemas de gestión. Es necesario que la información esté confirmada (mejor por el propio proveedor y con un tercero independiente)

LEET SECURITY
CyberSecurity Rating Agency

LEET Security. Una entidad independiente creada para calificar la seguridad de servicios TIC

LEET Security es una entidad independiente, constituida con el único fin de desarrollar y gestionar un sistema de etiquetado para calificar con fiabilidad los niveles de seguridad de la información ofrecidos por los proveedores de servicios TIC, y en particular –pero no únicamente– en entornos cloud.

Desde finales de 2010, la agencia LEET Security compila los controles definidos en las principales normativas, estándares y mejores prácticas internacionales, los clasifica y agrupa en diferentes niveles para proporcionar una "puntuación" a la seguridad implementada en cada servicio calificado, que se pone de manifiesto en el sello LEET.

De esta manera, el sistema de calificación gestionado por LEET Security se convierte en la primera implantación de la recomendación de la Estrategia de Ciberseguridad de la UE, de crear sistemas de etiquetado de la seguridad TIC.

El objetivo final es el de proporcionar confianza a los clientes/usuarios de dichos servicios, aportando total transparencia a las medidas de seguridad implantadas por los proveedores en los servicios que ofrecen.

Escríbenos

LEET SECURITY
CyberSecurity Rating Agency

MÁS INFORMACIÓN
LEET Security, S.L.
López de Hoyos, 125
28002 Madrid

+34 915 798 187
info@leetsecurity.com
@LEET_Security
@Leet Security SL

http:// www.leetsecurity.com