2024

V ESTUDIO "EMPRESAS Y CIBERSEGURIDAD"

LA CADENA DE SUMINISTRO ANTE NIS2 Y DORA

LEET SECURITY

CyberSecurity Rating Agency

Con la colaboración de

CLUB EXCELENCIA EN GESTIÓN

AGRADECIMIENTOS

Columnistas:

- Javier Palacios, Director Operaciones Servicios Gestionados de Avvale
- Mª Elisa Vivancos, Responsable de Ciberseguridad para los Sectores Estratégicos de Cadena de suministro, Pymes y Despachos Profesionales en INCIBE-CERT
- Ignacio Babé, Director General - CEO del Club Excelencia en Gestión
- Daniel Gil - Miembro de la Junta Directiva de Centro de Cooperación Interbancaria (CCI) y Director de Compras de Unicaja
- Andy Lawrence, Executive Director of Research de Uptime Institute

Club Excelencia en Gestión

Todas las personas que han participado en el estudio

CONTENIDO

OBJETIVO DEL ESTUDIO

Después de 7 años pulsando la opinión del sector, presentamos la 5ª edición del Estudio Empresas y Ciberseguridad de LEET Security, orientado a la seguridad de la cadena de suministro, que, como en ocasiones anteriores, hemos realizado de manera conjunta con el Club Excelencia en Gestión.

Nuestro **objetivo**, desde la primera edición, ha sido el de contribuir al conocimiento común sobre esta área, que era emergente cuando comenzamos en 2017, de **la ciberseguridad en la cadena de suministro**, terceras partes o proveedores, y que está adquiriendo una importancia creciente como parte de la resiliencia 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 fue el WannaCry, en 2018, la entrada en vigor del Reglamento General de Protección de Datos, y qué decir de 2020, en pleno confinamiento por el COVID19. En esta edición, el escenario normativo es quizás el elemento que marca la actualidad con la Directiva NIS2, que al escribir estas líneas está aún en proceso de trasposición y la inminente entrada en vigor del Reglamento DORA (Resiliencia Digital Operativa, aplicable al sector financiero).

Lo que sí es diferente en esta ocasión es que es el primer estudio que hacemos como parte, ya, de Uptime Institute, motivo por el cual, en esta edición hemos incorporado cuestiones de ciberseguridad específicamente pensadas para infraestructuras digitales. Por este motivo, el lector encontrará también una sección dedicada a analizar la encuesta específica de la Unidad de Inteligencia global sobre este aspecto a propietarios y operadores de centros de proceso de datos de todo el mundo, y una columna que reflexiona sobre el tema.

CONTEXTO

La encuesta de base sobre la que se ha realizado este estudio se realizó entre febrero y junio de 2024, es decir, a pocos meses de la trasposición / entrada en vigor de dos normas europeas que, según la opinión generalizada del sector, tendrán un impacto muy significativo en el escenario europeo y, en particular, en la ciberseguridad en la cadena de suministro:

- El Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero (en adelante, **Reglamento DORA)**; y
- La Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (en adelante, **Directiva NIS2**).

Ambas normas coinciden en la necesidad de mejorar los niveles de protección y respuesta de las infraestructuras tecnológicas que dan soporte a servicios esenciales para el funcionamiento de la sociedad (como son los servicios financieros) y, concretamente, en dos aspectos como son:

- La **responsabilidad (*accountability*) de la Alta Dirección** de las organizaciones en la definición, aprobación, asignación de recursos y supervisión de un programa de seguridad adecuado a la criticidad de los servicios prestados.
- El **establecimiento de mecanismos de gestión de riesgos ciber de la cadena de suministro** para asegurar que las terceras, cuartas y sucesivas partes implicadas en la provisión del servicio también implementan medidas de seguridad como para no suponer un riesgo para dicha prestación.

Este último aspecto ha supuesto en los últimos meses un foco creciente sobre los procesos de gestión de riesgos de ciberseguridad de la cadena de suministro que ha llevado, por ejemplo, a la creación de un subgrupo de trabajo en el seno del **Foro Nacional de Ciberseguridad** en el que hemos podido trabajar junto a otros expertos en la definición de mejores prácticas y consejos para elevar la seguridad de todo el ecosistema empresarial, sobre los principios de objetividad y transparencia asociados a la calificación de ciberseguridad.

CONCLUSIONES DEL ESTUDIO - ESTADO DE LA CIBERSEGURIDAD EN LA CADENA DE SUMINISTRO

*[Por **Antonio Ramos**, Executive Manager de LEET Security]*

La **creciente preocupación y ocupación sobre la ciberseguridad de la cadena de valor** está en línea con la importancia de la ciberseguridad *per se* (siguen siendo más del 90% de los encuestados los que declaran estar muy preocupados). De hecho, los niveles de interés de la Alta Dirección siguen creciendo (un 80,2% de los Consejos de Administración y un 88,3% 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 de la cadena de valor). Máxime cuando este aspecto es uno de los pilares de las nuevas normas europeas (Reglamento DORA y Directivas NIS2).

La evolución de la superficie a proteger se eleva hasta los máximos de la serie consecuencia de la creciente digitalización de los modelos de negocio que diluye el perímetro tradicional. En concreto, un 63,6% de los encuestados declara tener proveedores que se conectan a sus sistemas (proveedores conectados) y, un 60,5% afirma que tiene proveedores que gestionan su información en los propios sistemas del tercero (proveedores no-conectados).

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

- Los **ataques relacionados con los proveedores** que han vuelto a aumentar hasta alcanzar el 48,6%, es decir prácticamente 1 de cada 2 organizaciones han experimentado ataques originados en terceros.
- La **normativa** que exige la implementación de procesos de gestión de riesgos de terceros **no para de aumentar**. Al Reglamento General de Protección de Datos hay que sumar las normas europeas que adelantábamos en la 4ª edición del Estudio: las Directivas Europeas en materia de ciberseguridad de servicios esenciales (NIS2 – *Network and Information Security*), de infraestructuras críticas (CER – *Critical Entities Resilience*) y el Reglamento sobre resiliencia para el sector financiero (DORA).

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 (lo más fiable posible) sobre el nivel de seguridad de dichos terceros que permita una mejor toma de decisiones. Sin embargo, implantar estos programas no es trivial dado el volumen y la disparidad de pro-

veedores, y la escasez de recursos que se pueden dedicar al programa, como indican los datos resultados que estudiamos a continuación:

- En primer lugar, la situación de las áreas de compras/aprovisionamiento se mantiene respecto al año anterior y, aunque el nivel de preocupación es similar (49,6%), sólo el 3,1% de las mismas tienen alguna responsabilidad en la ciberseguridad de la cadena de suministro (aunque, al menos, ha subido desde el casi insignificante, 1,1% de la edición anterior).
- La concienciación sigue dando sus frutos: Aumenta el grado de supervisión anual del riesgo de terceros hasta un 55,3% y se reduce hasta un **7,0% las organizaciones que no evalúan en absoluto a sus proveedores**. Aunque son mejores cifras que en ediciones anteriores, sigue siendo necesario continuar con el esfuerzo.
- Otro aspecto que también mejora es el de los mecanismos de evaluación utilizados. Mientras que en ediciones anteriores el cuestionario era el mecanismo más utilizado, en esta edición se ha emparejado con las evaluaciones documentales y las auditorías / certificaciones de terceros. En este sentido, vemos como **los procesos de gestión de riesgo de terceros aumentan su nivel de madurez**, ampliando los mecanismos utilizados, a la par que decrece la confianza que se deposita en las certificaciones de Sistemas de Gestión (en un 28,7% que supone el mínimo de la serie).

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 4 encuestados** (un aumento del 55% respecto a la edición anterior) 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 (**'Análisis estadísticos de calificaciones emitidas'**), 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.

Y, por lo que respecta a la sección temática de esta edición sobre la ciberseguridad en las infraestructuras digitales, se constatan dos circunstancias muy interesantes:

- **Que la oficina del CISO y los profesionales de ciberseguridad no son los que más peso tienen en esta materia** (cayendo más en el área de TI y con un peso significativo de los propios proveedores de la tecnología operativa de los CPD – en un 12,2% de los casos); y
- Que las tecnologías operativas (OT) que se utilizan en la gestión de las infraestructuras habitualmente no han sido diseñadas incluyendo requisitos de seguridad por lo que suponen un potencial riesgo para dichas infraestructuras.

Conclusiones en clave Modelo 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 percepción del nivel de ciberriesgo en las organizaciones que utilizan el Modelo EFQM (un 63% considera que hay un riesgo mayor respecto al año pasado frente a un 57% en organizaciones que no utilizan el Modelo EFQM), aunque en las organizaciones que utilizan el Modelo EFQM el grado de preocupación respecto a los temas de ciberseguridad es menor (un 61% respecto el 70% de media), probablemente por haber implantado acciones y medidas al respecto.

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 80% 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 53% en el resto de las organizaciones.

Al mismo tiempo, se ha producido un cambio de tendencia, las organizaciones con Sello EFQM tienen unos órganos de dirección (Consejo de Administración y Dirección General) en los que se ha reducido su nivel de preocupación por establecer mecanismos de seguridad, y actualmente están básicamente al mismo nivel de preocupación (un 83% en “alta” o “muy alta preocupación”) que el resto de las organizaciones, probablemente una prueba de la mayor madurez y especialización del sector.

También hay que señalar que las organizaciones con Sello EFQM dan una mayor importancia a la ciberseguridad en la perspectiva de la “Gestión 5.0-Gestión del Futuro” (3 puntos superior), apreciando en mayor medida la importancia que tendrá en el futuro.

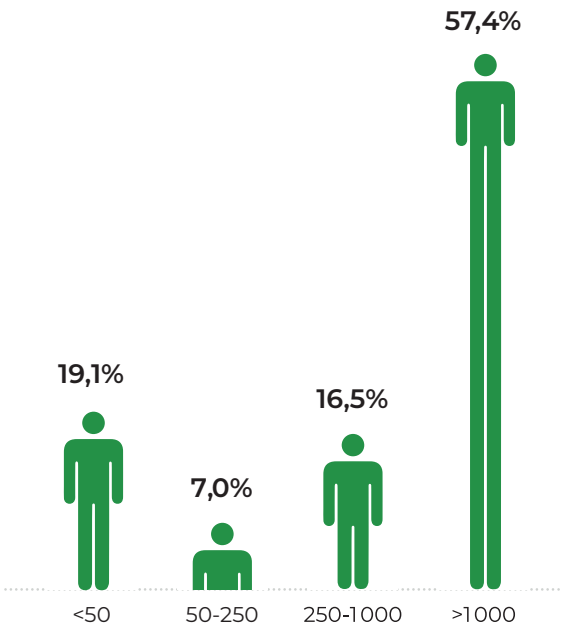
Se podría decir que la utilización del Modelo EFQM, como herramienta referencial y holística para una gestión excelente, innovadora y sostenible, conlleva un mejor conocimiento de la propia organización y un trabajo de concienciación en gestión de riesgos que son, claramente, el primer paso para la mejora de los mismos, y la ciberseguridad no escapa de esta máxima.

RESULTADOS DE LA ENCUESTA

La encuesta ha sido respondida por 161 organizaciones (frente a las 188 de la edición anterior), representadas fundamentalmente por responsables de seguridad (CSO/CISO), 28,6%, responsables de tecnología (CIO), el 12,5% y directores generales (CEO), el 8,0% de la muestra y, por sectores, 64,6% pertenecen a Banca y Seguros, Servicios o Tecnología.

Las empresas a las que pertenecen son fundamentalmente de gran tamaño (según se muestra en la **Figura 1**), lo cual no se corresponde con la distribución estándar del tejido empresarial de nuestro país. Esta respuesta parece indicar que la preocupación por la seguridad de la cadena de suministro todavía es un aspecto que no ha permeado a todas las empresas, sino que se ha desarrollado, especialmente, en las de mayor tamaño.

Figura 1. Número de empleados de las organizaciones participantes



Los resultados de la encuesta están divididos en tres apartados principales:

1. **Escenario general**, donde se analizan los resultados referidos al contexto general de ciberseguridad en el momento de realizar el Estudio.
2. **Ciberseguridad en la cadena de suministro**, es el 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.
3. **Seguridad en las infraestructuras digitales.** Al igual que otros años, incluimos un aspecto temático de actualidad que, en esta ocasión, dada nuestra reciente incorporación a Uptime Institute, hemos incluido aspectos relacionados con la ciberseguridad en los centros de proceso de datos.

Escenario general

Relevancia de la ciberseguridad

En esta 5ª edición, **el porcentaje de encuestados muy preocupados por la ciberseguridad se mantiene por encima del 90%, aunque ligeramente por debajo el año pasado.** En concreto, el **90,1%** de personas han respondido que estaban muy preocupadas (por encima de 7 en una escala de 1 a 10), lo que supone 5,6 puntos menos que el año pasado y volver a niveles parecidos a los de 2020.

Este alto nivel de preocupación está alineado con la percepción de riesgo, puesto que el 57,7% de las respuestas consideran que el riesgo sigue creciendo (por un 58,0% en 2022) y que continúa aumentando el ritmo al que se invierte en ciberseguridad que, este año afecta a un 69,0% (el mayor porcentaje desde que comenzamos a recabar datos en 2018). Desde que incluimos esta pregunta ha ido creciendo de manera consistente el número de organizaciones que incrementan sus inversiones (casi 13 puntos en estos 6 años).

Figura 2. Nivel de preocupación por la ciberseguridad

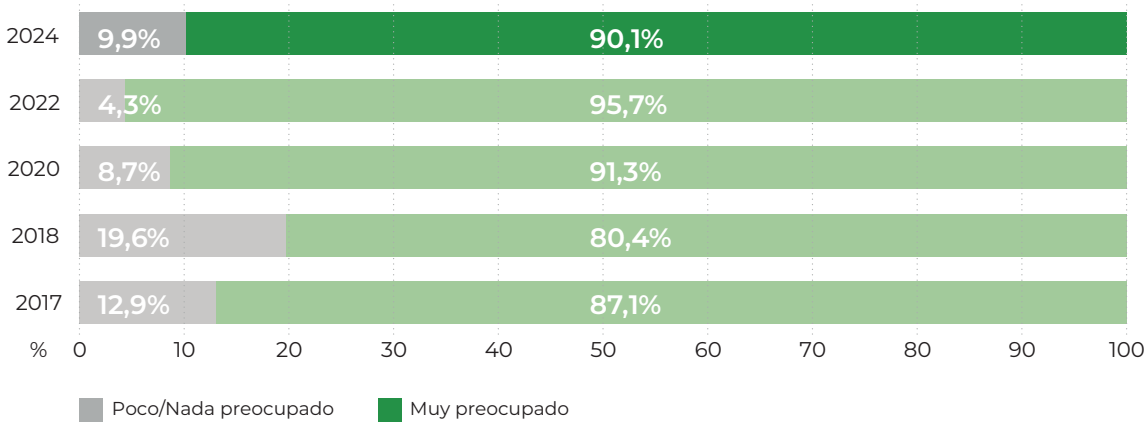


Figura 3. Evolución de las inversiones en ciberseguridad

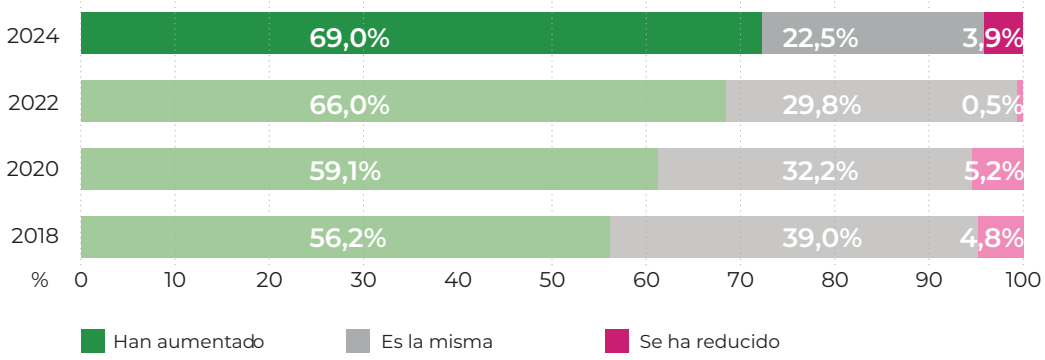
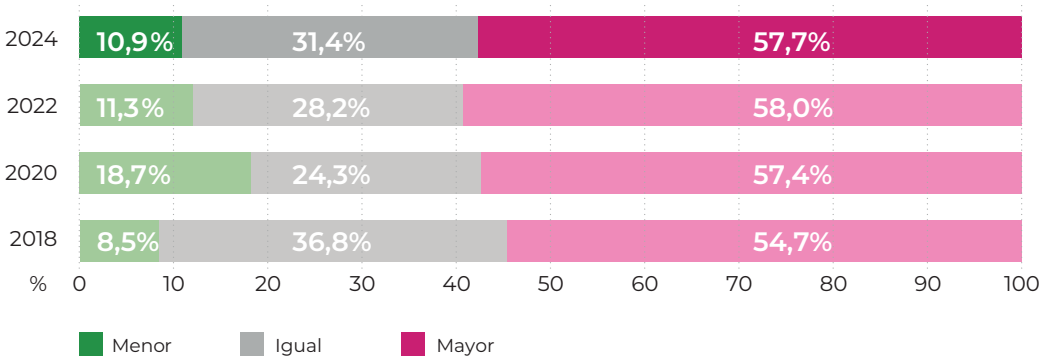


Figura 4. Evolución de la percepción de riesgo



Comparando estas tres magnitudes se observa una reducción del ritmo de crecimiento, ya que todas ellas se mantienen relativamente estables respecto a los datos observados en la edición anterior (de hecho, sólo las inversiones crecen a mayor ritmo que en el pasado). Es decir, todo parece indicar que, finalmente, las organizaciones están siguiendo la máxima de invertir allí dónde dicen que más preocupadas están (*put your money where your mouth is*).

Evolución de los ciberataques

Contando ya con cinco ediciones del Estudio podemos ver que es este un dato con más oscilación que otras series más estables. Analizando el histórico, vemos que el promedio se sitúa en el 47%, es decir, **aproximadamente la mitad de las organizaciones encuestadas dicen haber sido objeto de un ciberataque.**

Este año, adicionalmente, hemos incluido la consideración de la magnitud de las consecuencias, es decir, si la organización ha sido capaz de contenerlo o si, por el contrario, tuvo algún impacto. El resultado es que, del 55,9% de organizaciones con algún ciberataque declarado (por cierto, el dato más alto de todas las ediciones), el 41,0% de ellas consiguió frenarlo sin que tuviera un impacto relevante. Es decir, sólo tuvo impacto en el 14,9% de las organizaciones (o dicho de otra forma, más de 1 de cada 4 ataques consiguió tener impacto, en concreto, un 26,7%).

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 sigue creciendo desde 2020 (3,7 puntos en materia de privacidad y 7,4 puntos en gestión de riesgos tecnológicos) alcanzado los valores más altos también en esta edición.

Figura 5. Organizaciones conscientes de haber sufrido algún incidente

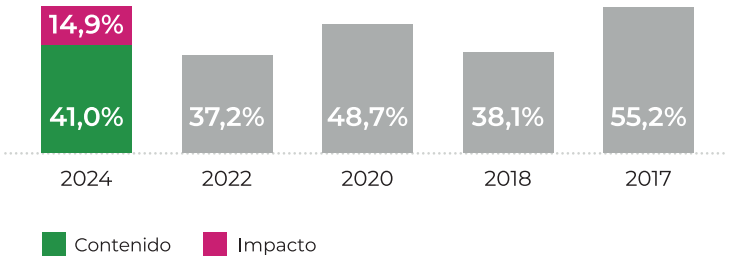
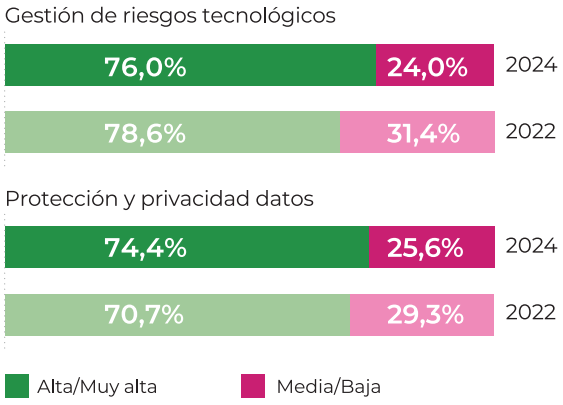


Figura 6. Nivel de preparación percibido



En todo caso, se mantiene cierta contradicción en los datos puesto que, aunque aproximadamente el 75% de las entidades encuestadas opinan que su nivel de preparación es alto o muy alto y, al mismo tiempo lo consideran insuficiente puesto que, el 69,0% declara, a su vez, la 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[1]. Por esta razón, también se puede utilizar la calificación como mecanismo de evaluación de inversiones en ciberseguridad, ya que permite dirigirlo hacia aquellas que, como hemos dicho, actúan sobre los puntos débiles.

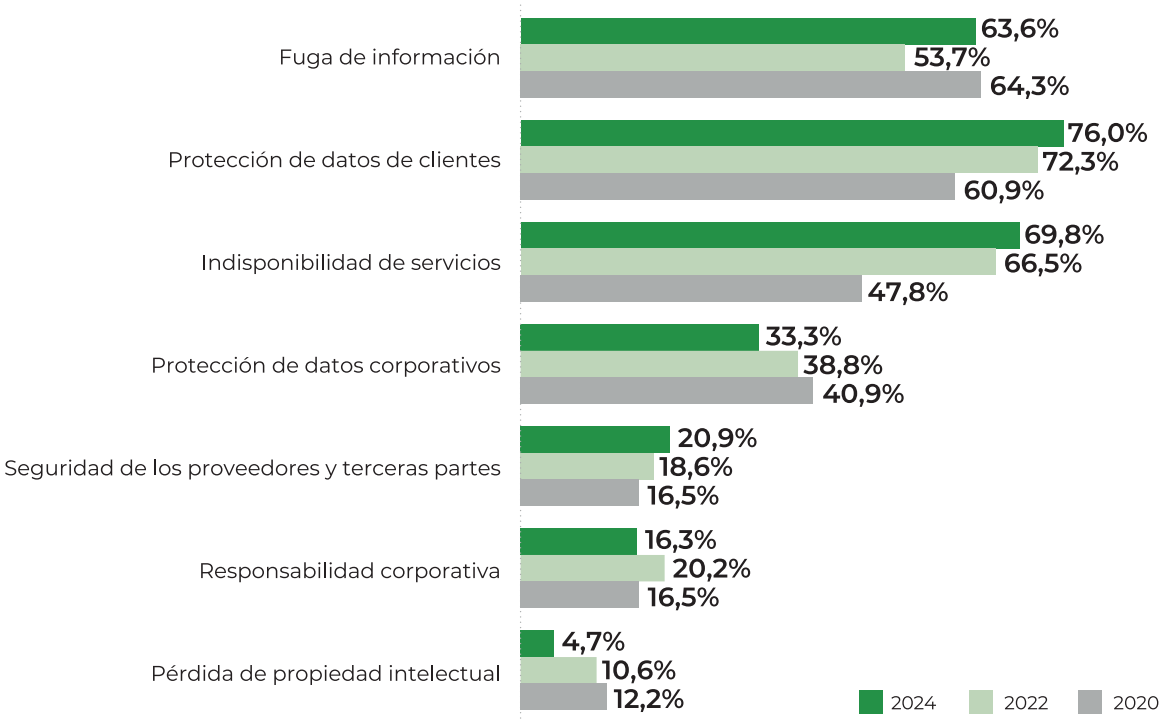
Preocupaciones principales

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 esto observamos varios aspectos interesantes al comparar los resultados con ediciones anteriores:

- La **indisponibilidad de servicios** que, aunque no recupera los niveles de 2018, cuando preocupaba a un 78,8%, sigue subiendo hasta el 69,8%. En nuestra opinión esta circunstancia responde a la **creciente dependencia de la resiliencia corporativa en las TIC.**
- La **protección de datos de clientes** sigue siendo la mayor preocupación al ser la causa de falta de sueño de un 76,0% de los encuestados.
- El otro elemento que continúa en crecimiento continuado, aunque a un nivel inferior, es la **seguridad de los proveedores y terceras partes** que supera, por vez primera, el veinte por ciento (en concreto, el 20,9% lo recogen como su principal preocupación).

Dado que el foco del estudio es la ciberseguridad en la cadena de suministro no podemos dejar de analizar su si-

Figura 7. Causas de preocupación por la ciberseguridad



1. 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

tuación. Como decíamos, para 1 de cada 5 personas encuestadas, esta área es ya un aspecto relevante y pensamos que, dado el peso que tiene la gestión del riesgo de terceros en las normativas europeas recientemente aprobadas (Directiva NIS2 y Reglamento DORA), nuestra predicción es que veremos como este valor sigue creciendo de manera significativa en futuras ediciones.

Responsabilidades en materia de ciberseguridad

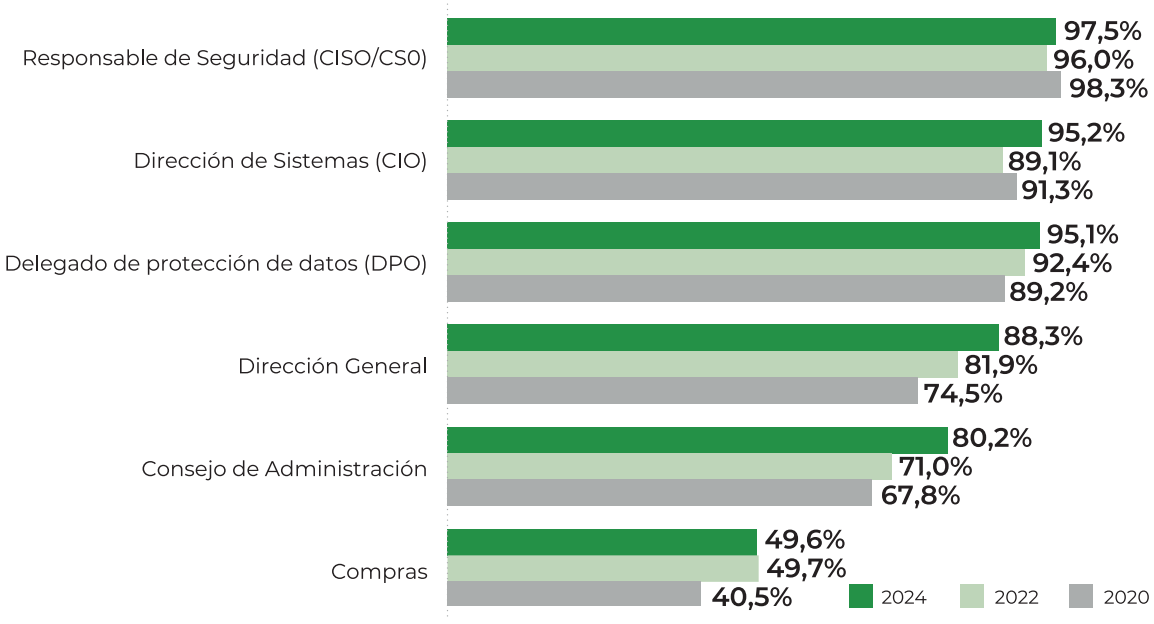
Una vez analizada la percepción del riesgo y la evolución de los ciberataques, pasamos a analizar quién asume en las organizaciones la responsabilidad sobre la ciberseguridad.

En esta 5ª edición se mantiene la importancia relativa de los roles que intervienen en la gestión de la ciberseguridad (ver **figura 9**) si bien es cierto que se produce un cambio de tendencia muy interesante, ya que sube en 11,7 puntos (hasta el 81,4%) el porcentaje de las organizaciones que asignan esta responsabilidad a un Chief Information Security Officer (CISO), y baja en 10,7 puntos en las que esta responsabilidad es el Responsable de Sistemas (CIO). Este aspecto es muy relevante puesto que parece poner de manifiesto la consolidación de las/os CISO como rol relevante en las organizaciones en relación con la gestión de la ciberseguridad.

Estas responsabilidades están en línea con la respuesta obtenida al preguntar por la preocupación de las distintas funciones en relación a la ciberseguridad **(Figura 8)**, puesto que también CISO y CIO son las más preocupadas, roles a los que se une el/la Delegado/a de Protección de Datos (aunque sólo tienen responsabilidades en esta materia en 1 de cada 4 de las organizaciones encuestadas).

Otro dato relevante es que la preocuopación en los Consejos de Administración y Dirección General es alta o muy alta en el 80,2% y 88,3% de las organizaciones, respectivamente. Es decir, una subida de casi 10 puntos respecto a la edición anterior (en la que ya había subido alrededor de 5 puntos). **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. Por otro lado, considerando las mencionadas normativas europeas recién aprobadas, que enfatizan la responsabilidad de dichos órganos en la gestión de los programas de ciberseguridad, este aspecto seguro que continúa creciendo en futuras ediciones del Estudio.

Figura 8. 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, vemos cómo se estabiliza en esta edición la preocupación de las áreas de compras /aprovisionamiento por la ciberseguridad (49,6% frente al 49,7% de la edición anterior). Sin duda, todavía queda mucho por hacer, pero se percibe un cambio significativo (aunque pequeño en volumen) puesto que se triplica el porcentaje (de un 1,1% a un 3,1%) de las organizaciones encuestadas en las que esta área declara tener alguna responsabilidad en materia de ciberseguridad.

Desde la edición anterior, analizamos también el tipo de recursos que se utilizan para la gestión de la seguridad. Comparando con el año anterior, sólo percibimos un cambio significativo en las organizaciones que declaran emplear personal exclusivo de ciberseguridad que crece un 29,6% (del 47,9% al 62,1% de las encuestadas).

En estos momentos en los que contratar personal de ciberseguridad es un reto para muchas organizaciones, vemos sin embargo que cobra importancia el personal que se dedica sólo a ciberseguridad, lo que debería redundar en una mejor capacitación de esta función en las organizaciones.

Figura 9. Funciones con responsabilidad en ciberseguridad

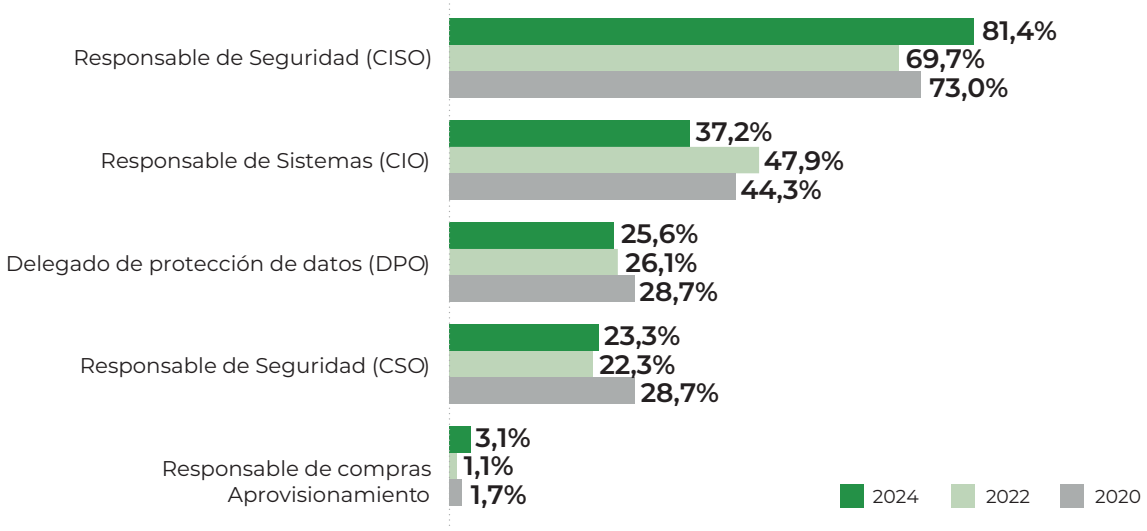
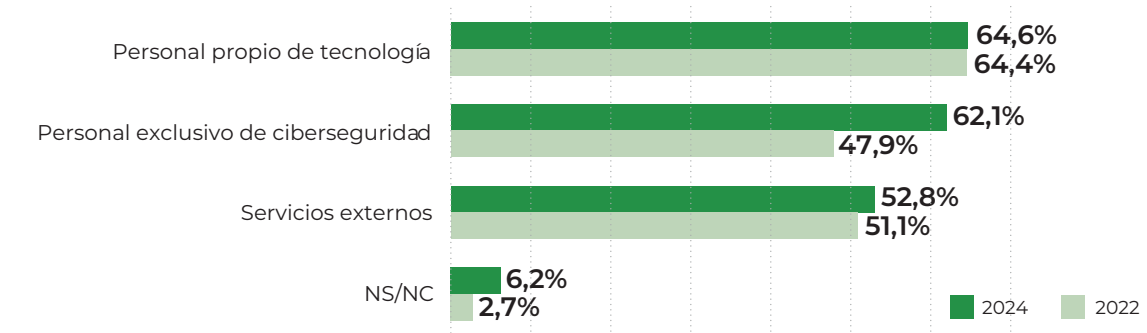


Figura 10. Recursos encargados de la gestión de la ciberseguridad



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 sigue aumentando en cada edición. De hecho, en esta ocasión se alcanza **el 83,7% de los encuestados que dicen estar muy preocupados por la seguridad de sus proveedores**, es decir, más de 4 de cada 5 respuestas.

Obviamente, también contribuye a esta circunstancia la creciente importancia que tienen los proveedores para el funcionamiento de nuestras organizaciones, ya que es habitual que 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"). Tras el parón puntual de la pasada edición, en esta ocasión vemos como ambas tipologías alcanzan su máximo de toda la serie con valores superiores al 60% en ambos casos.

Figura 11. Acceso de proveedores a la información de sus clientes

Es decir, **en 3 de cada 5 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 48,6% (8 puntos más que en la anterior edición) de esos incidentes tuvieron a 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 el 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, ya que la evaluación anual de terceros vuelve a crecer ligeramente, pasando de un 54,1% en 2022 a un 55,3% en 2024, sigue siendo **preocupante**

Figura 12. Origen de los incidentes de seguridad

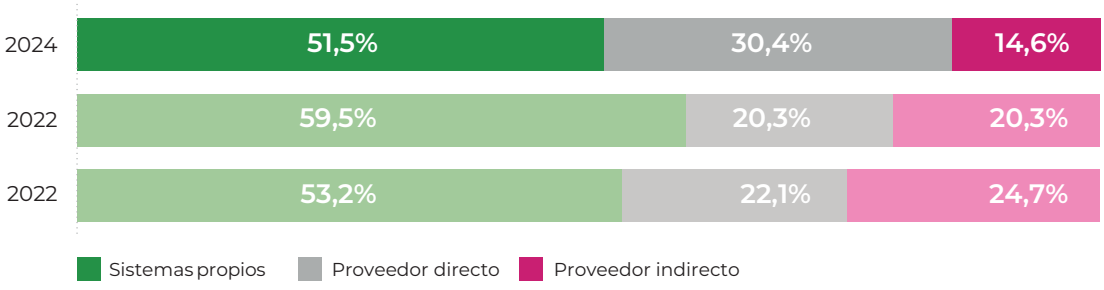
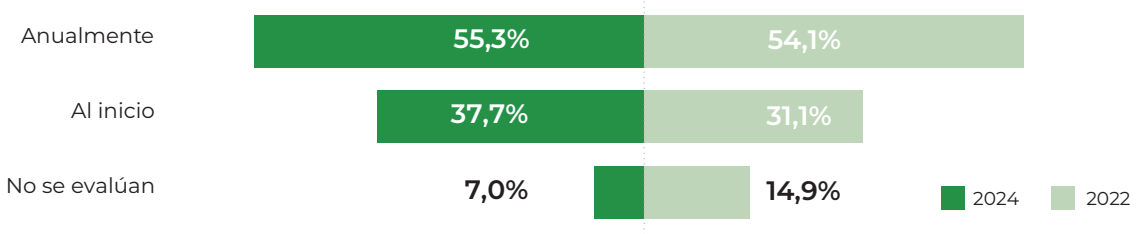


Figura 13. Frecuencia de evaluación de proveedores



que, a estas alturas, todavía un 7,0% 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, aunque hay que valorar muy positivamente que se haya reducido a la mitad este porcentaje (no obstante, 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).

Y, en relación a quién asume esta responsabilidad en las organizaciones vemos que recae, principalmente, en la función del CISO (de hecho, ha aumentado su porcentaje de un 23,9% a un 30,2%) aunque el rol de Responsable de la Gestión de Riesgos ha aumentado su participación significativamente (pasando de un 12,8% en la pasada edición a un 19,4%), mientras que el área de Compras / Aprovisionamiento se mantiene en un 20,2%. Por el contrario, la función de DPO se reduce de un 7,4% a un 3,1% aunque la seguridad de los encargados de tratamiento de datos personales es uno de los principales *drivers* para este proceso.

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:

- Se han igualado los tres métodos más difundidos: cuestionarios, evaluación documental y auditorías / certificaciones de terceros.

Figura 14. Responsabilidad en materia de gestión de riesgos de terceros

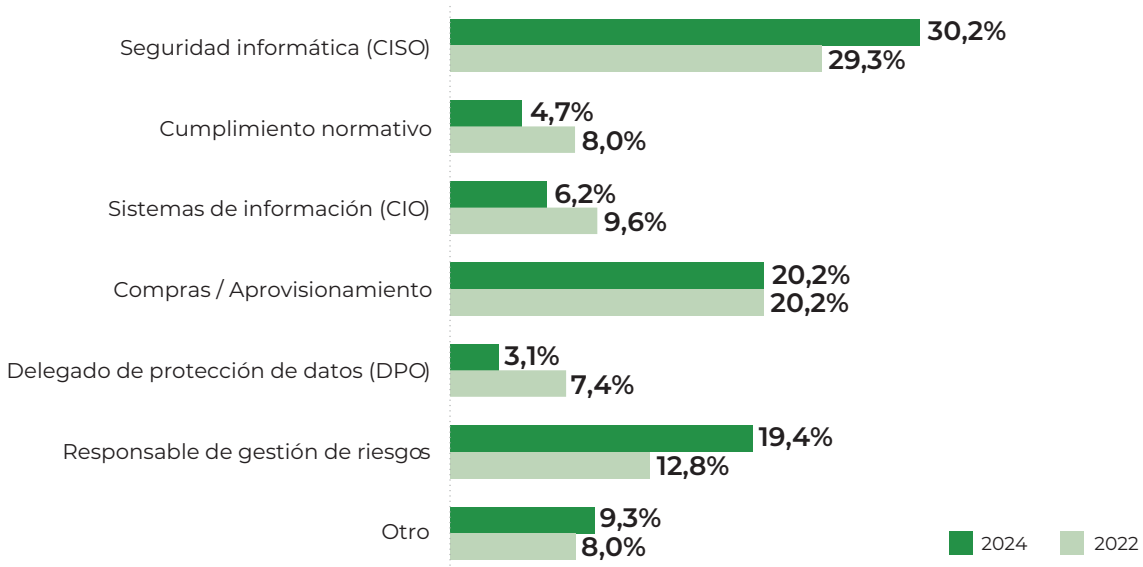
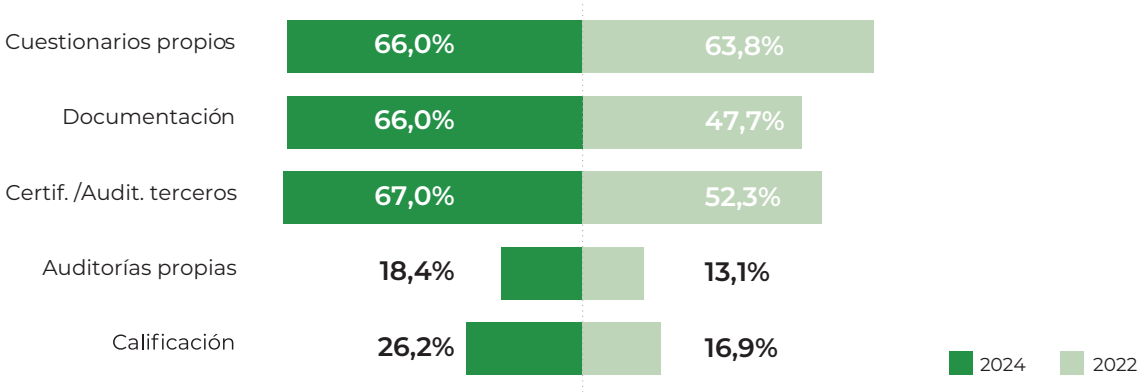


Figura 15. Métodos de evaluación de proveedores de gestión de riesgos de terceros



- **La calificación es el mecanismo que más crece** (un 55%) pasando de un 16,9% a un 26,2%. Es decir, **1 de cada 4 organizaciones está utilizando calificaciones para evaluar a sus proveedores.**

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.

ditorías" y los segundos porque se transforman en receptores de auditorías en las que siempre muestran lo mismo a diferentes auditores.

Por otro lado, esta forma de actuar no se produce en ningún otro sector económico (un restaurante, al comprar producto, no tiene que hacer pruebas sobre el género antes de usarlo, o un concesionario no tiene que hacer pruebas de seguridad de los vehículos antes de venderlos al público) dónde se han establecido otros mecanismos más eficientes basados en la responsabilidad y en la transparencia (más al estilo de cómo se

Y si volvemos por un momento al aspecto de la periodicidad, vemos que hay un 37,7% 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.

Llama la atención, debido a la cantidad de recursos que consume, el incremento significativo (un poco más del 40%) en el uso de auditorías propias (hasta el 18,4%), aunque sigue siendo el mecanismo menos utilizado. Una de las posibles causas de este aumento puede ser el papel de los supervisores (de las mencionadas normas europeas) que están poniendo énfasis en la necesidad de auditar a los proveedores críticos. Esta situación, a nuestro juicio, no es sostenible en el tiempo por la dedicación de recursos que implica por todas las partes (tanto clientes – auditores, como proveedores – auditados): Los primeros porque les supone convertirse en "firmas de auestá planteando en la inminente directiva europea sobre ciber resiliencia). Este es el principio que ha puesto en valor el sector financiero español con el lanzamiento del servicio **Pinakes**® para la 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 (57%) y la demostración de cumplimiento (32%), aunque lo que más ha crecido ha sido el uso de la misma como herramienta de *reporting* interno (31%). En los últimos meses se ha percibido que la calificación supone un mecanismo objetivo de evaluación de la postura de ciberseguridad en una organización que permite (normalmente) al CISO informar a la Dirección sobre el estado de protección de una manera comprensible, comparable a lo largo del tiempo y con otras organizaciones (*benchmarking*) y con la confianza de estar libre de sesgo. **Estas características**

de objetividad y transparencia son muy valoradas por los órganos de Dirección para cumplir con las exigencias definidas, tanto en la Directiva NIS2 como en el Reglamento DORA.

Finalmente, para poner en relación la calificación con el resto de mecanismos, preguntamos a los usuarios de estos servicios qué mecanismos le 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, aunque la tendencia es claramente descendente (28,7% de los casos). Vemos que, finalmente, se ha reconocido que **la certificación de un sistema de gestión 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.

En este aspecto, el mecanismo más detallado, que podrían ser las auditorías independientes son el segundo elemento mejor valorado (un 23,5%) – aunque desciende a los niveles de 2020, seguido del Esquema Nacional de Seguridad (que asciende hasta un 20,6%).

En cuanto a las calificaciones de seguridad, bajan su porcentaje, aunque la calificación de LEET Security sigue siendo considerada más fiable que los ratings automáticos. Como ya se puso de manifiesto en la edición anterior, este resultado es indicador de la labor de concienciación que aún queda por hacer en esta materia.

Figura 16. Usos de la calificación en las organizaciones

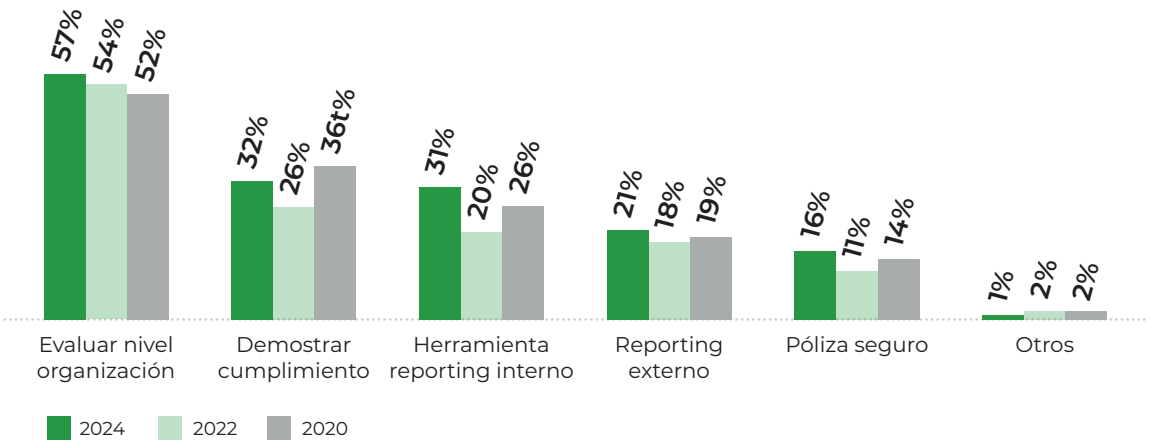
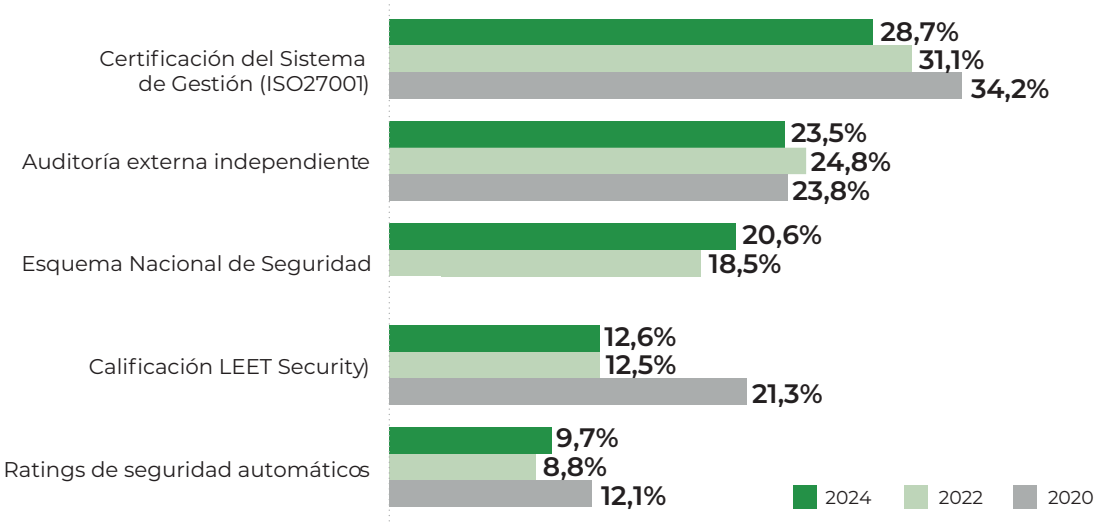


Figura 17. Confianza en las garantías de seguridad aportadas



Ciberseguridad de las infraestructuras digitales

Como novedad en esta edición y a raíz de nuestra incorporación a Uptime Institute en febrero de 2023, hemos incluido algunas cuestiones relativas a la ciberseguridad de las infraestructuras digitales. En paralelo, el servicio de Estudios de Uptime Institute también ha puesto en marcha una encuesta global sobre la seguridad para operadores y propietarios de CPD (Centros de Proceso de Datos).

El objetivo es entender mejor qué papel juega la ciberseguridad en la resiliencia de las infraestructuras digitales que soportan nuestros servicios desde ambos puntos de vista.

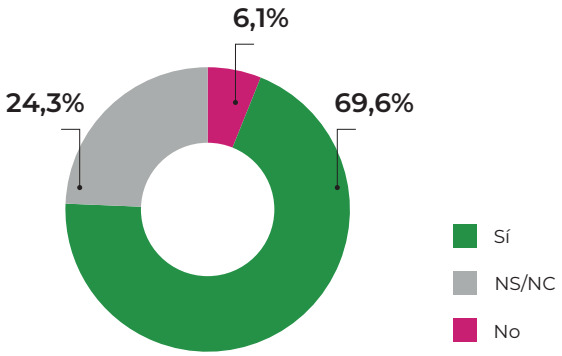
Para ello, lo primero sea, quizás, entender si este tipo de infraestructuras son objeto de ataques (es decir, no si los sistemas alojados en el ***white space*** son objeto de ataque, que seguro que lo son, sino si los propios sistemas que gestionan el CPD son atacados). Y la respuesta nos ha parecido muy interesante, ya que:

- Sólo el 6,1% reconoce la existencia de ataques específicos al CPD, lo que podríamos considerar como un porcentaje bajo;
- Sin embargo, **un 24,3% de las organizaciones desconoce si sus infraestructuras digitales han sido atacadas,** lo que pone de manifiesto que se trata de un ámbito de ciberseguridad que requiere de una mayor atención en estos momentos.

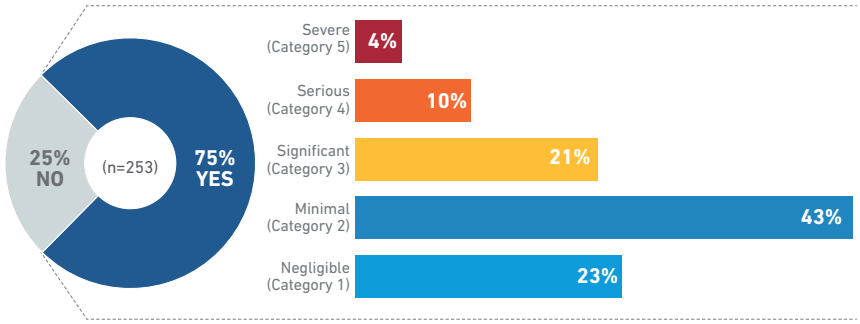
En la encuesta a propietarios y operadores de infraestructuras, esta misma pregunta referida a los últimos 3 años (en lugar de sólo uno) arroja datos muy distintos, ya que básicamente los datos se dan la vuelta. De hecho, el 75% de las organizaciones declaran haber tenido un incidente, de los cuales, más de un tercio han tenido un impacto considerable (valoración mayor de 100 mil dólares).

En nuestra encuesta, la primera pregunta ha sido sobre la realización de

Figura 18. Ciber ataques dirigidos a las infraestructuras digitales

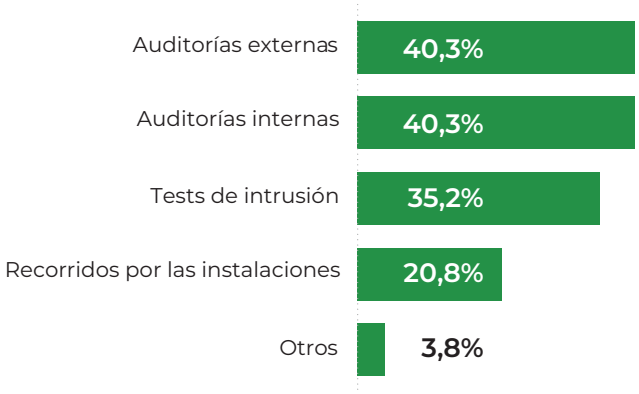


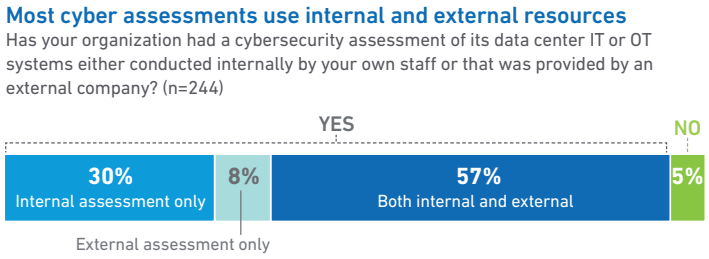
Did your organization experience an impactful cyber incident in the past three years? On a scale of 1 (negligible) to 5 (severe) how would you classify your data center's most impactful cybersecurity incident in the past three years?



revisiones de ciberseguridad en los CPD y nos hemos encontrado con que una gran mayoría de las organizaciones encuestadas, 4 de cada 5, sí realizan este tipo de revisiones, concretamente un 80,6%.

Figura 19. Tipo de revisiones de ciberseguridad



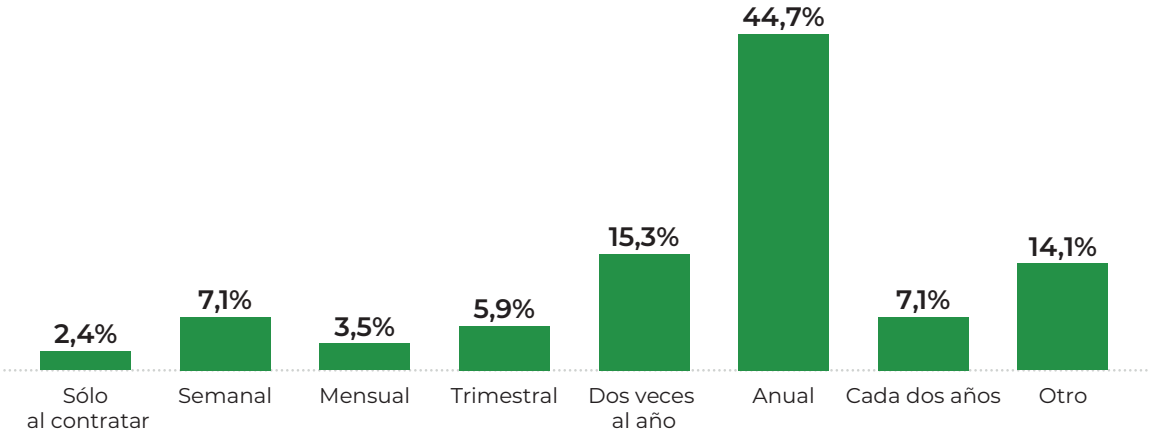


De estas organizaciones que realizan revisiones, vemos que el mismo porcentaje de ellas (un 40,3%) utiliza tanto auditorías externas como internas, mientras que un solo un 35,2% declara realizar pruebas de intrusión. Esta percepción es compartida con la encuesta de Uptime Institute en el que ambos tipos de auditorías subían hasta el 57% de las respuestas.

Y en cuanto a la periodicidad de realización, en la mayoría de las ocasiones se realizan de manera anual (en un 44,7% de los casos), mientras que sólo un 2,4% de las organizaciones revisan únicamente durante el período de contratación. Estos datos contrastan con la encuesta de Uptime Institute, en la que la mayoría de las revisiones se realizan con periodicidad trimestral o aún menor (56%) y las anuales sólo suponen el 25% de las respuestas.

Un aspecto que nos interesaba también entender era el contenido de las revisiones de ciberseguridad de los CPD, entendiendo que este tipo de infraestructuras tienen características específicas a tener en cuenta (la utilización de OT – *Operational Technologies*, las limitaciones para no impactar la disponibilidad

Figura 20. Periodicidad de las revisiones de ciberseguridad en infraestructuras



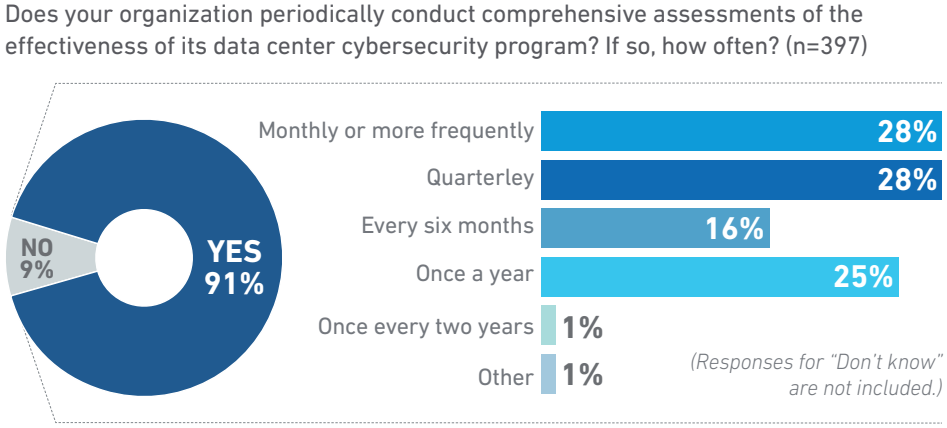
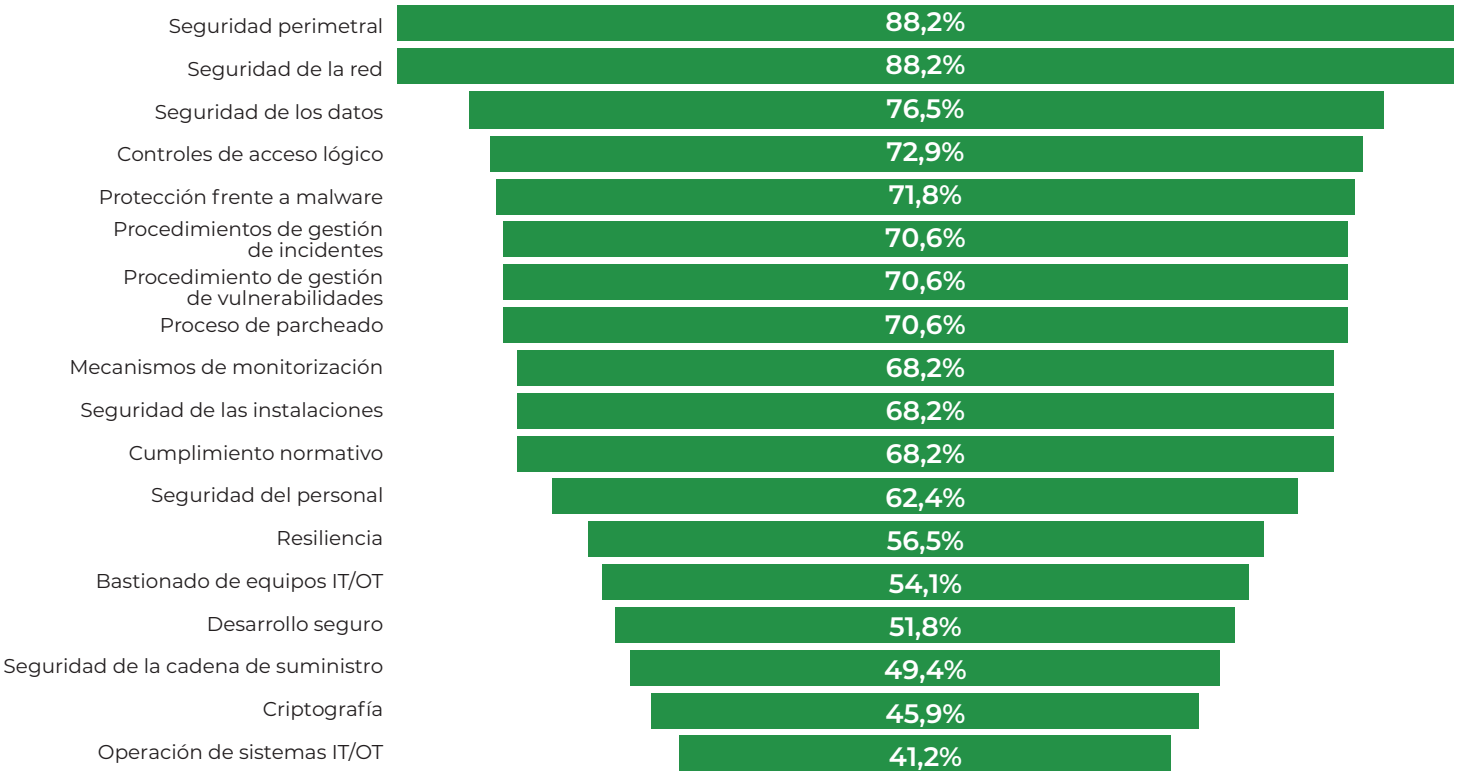


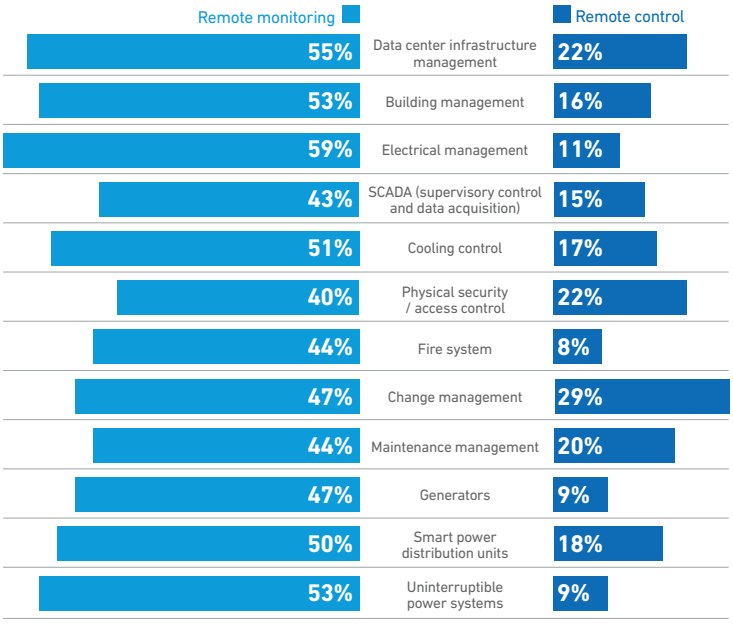
Figura 21. Confianza en las garantías de seguridad aportadas



del servicio o la convivencia de múltiples redes para asegurar conectividad externa con redes internas de servicio propias de la instalación). Desde nuestro punto de vista, la evaluación de un CPD se parece más a la revisión de un Sistema de Control Industrial que a un sistema TI; es como si el CPD fuera una fábrica de capacidad de procesamiento y conectividad que utilizamos desde TI para ofrecer un servicio a nuestros clientes. En la **figura 21** se resumen los aspectos que las personas encuestadas nos han señalado como parte de sus evaluaciones de ciberseguridad de los CPD:

Figura 22. Conectividad de sistemas OT

Which of the IT and operational technology systems used to operate your data center(s) provide remote (offsite) capabilities? (n=242)



(Responses for "Don't know" are not included.)
("Lighting control", "Ticketing", "Billing" response categories are not shown.)

UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2023

uptime INTELLIGENCE

- La **seguridad de red se aborda en la práctica totalidad de los casos** (tanto la seguridad perimetral, como la propia red, se incluyen en un 88,2% de las respuestas).
- Alrededor de 3 de cada 4 también han mencionado los controles de acceso lógico, la protección frente al *malware* y la gestión de incidentes y vulnerabilidades.
- Es destacable que aproximadamente la mitad de las evaluaciones ha incluido en sus respuestas:
  - La resiliencia de los sistemas de operación de la infraestructura;
  - La configuración segura o la operación adecuada de los sistemas OT;
  - O la seguridad en la cadena de suministro

Cabría pensar que la cadena de suministro no es muy relevante, pero sabemos por la encuesta realizada por Uptime Institute a los propietarios y operadores de infraestructuras digitales, que alrededor del 50% de los sistemas están conectados al exterior para ser monitorizados (de los cuales, aproximadamente el 20% también pueden ser operados desde fuera del CPD).

Para completar el entendimiento de este escenario de evaluación hemos preguntado por la utilización de estándares o marcos de referencia para ayudar a definir estos procesos y, las respuestas indican que el estándar más ampliamente utilizado es la ISO/IEC 27001 (respuesta de un 78% de las organizaciones encuestadas), seguida de lejos por el propio estándar de diseño y construcción de CPD de Uptime Institute (los conocidos *Tiers*). Nos llama la atención que, dado el peso que tiene la OT en la operación de los CPD, la norma IEC 62443 sólo haya sido mencionada por el 5% de las personas encuestadas cuando, en nuestra opinión, es una referencia muy válida si consideramos estos entornos como sistemas de control industrial.

Finalmente hemos preguntado por los roles con responsabilidad en materia de ciberseguridad en este ámbito obteniendo respuestas muy interesantes:

- En el 30% de los casos, **la responsabilidad recae sobre TI, por delante de los equipos de ciberseguridad** (20% de las respuestas).
- La propia área de operaciones del CPD es indicada como responsable en el 10% de las organizaciones lo cual significa que dicho personal debe contar con preparación en materia de ciberseguridad, haciendo su formación y preparación más compleja.
- **Llama la atención que se delegue la responsabilidad en los propios proveedores del equipamiento en más del 12% de los casos**, puesto que parecería más indicado que esta función la realizara alguien de la organización o, al menos, estuviera controlada por una persona interna.
- Finalmente, más de un 17% de los encuestados indica no saber quién se encarga lo que, de nuevo, parece indicar que la ciberseguridad del propio CPD queda en tierra de nadie.

Figura 23. Estándares utilizados en infraestructuras digitales

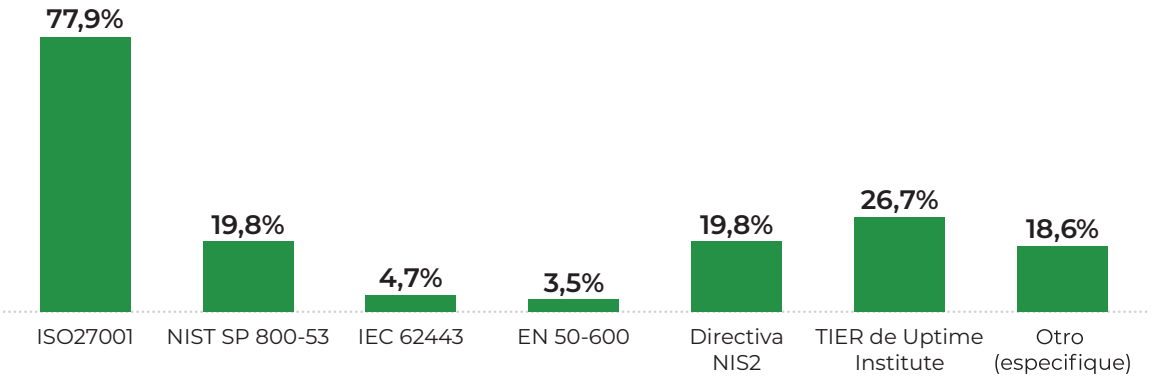
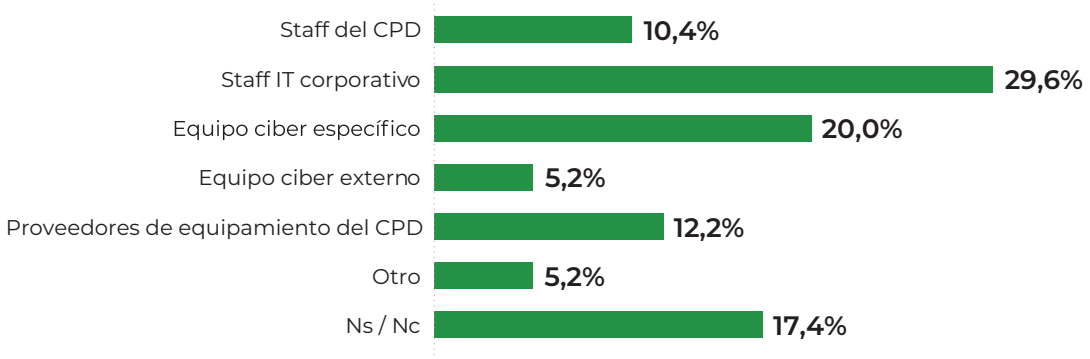


Figura 24. Responsabilidad sobre la ciberseguridad de las infraestructuras digitales



ANÁLISIS ESTADÍSTICOS DE CALIFICACIONES EMITIDAS

Continuando con la sección que iniciamos en el estudio publicado en 2020, incorporamos aquí nuevamente un análisis de nivel de los resultados obtenidos en 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 y, en términos globales, la evolución de los resultados obtenidos por las organizaciones que cuentan con servicios calificados se refleja en la siguiente tabla:

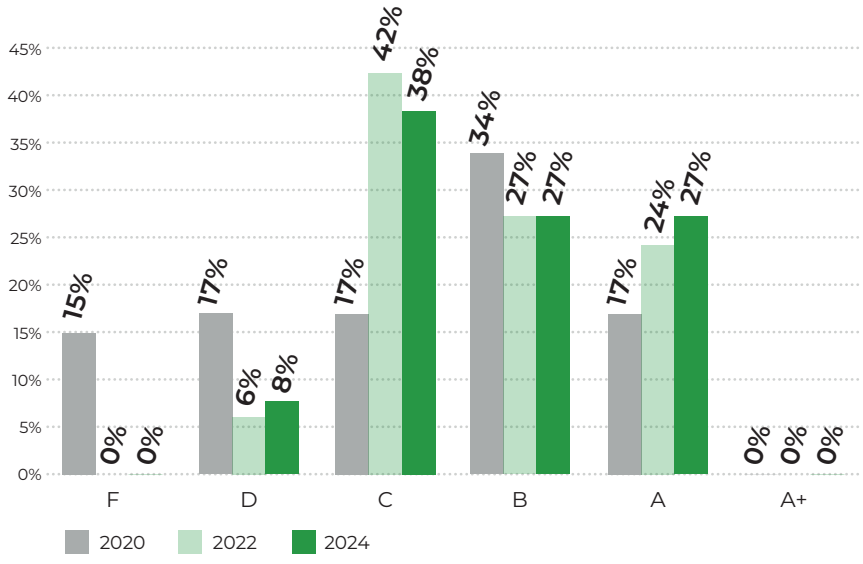


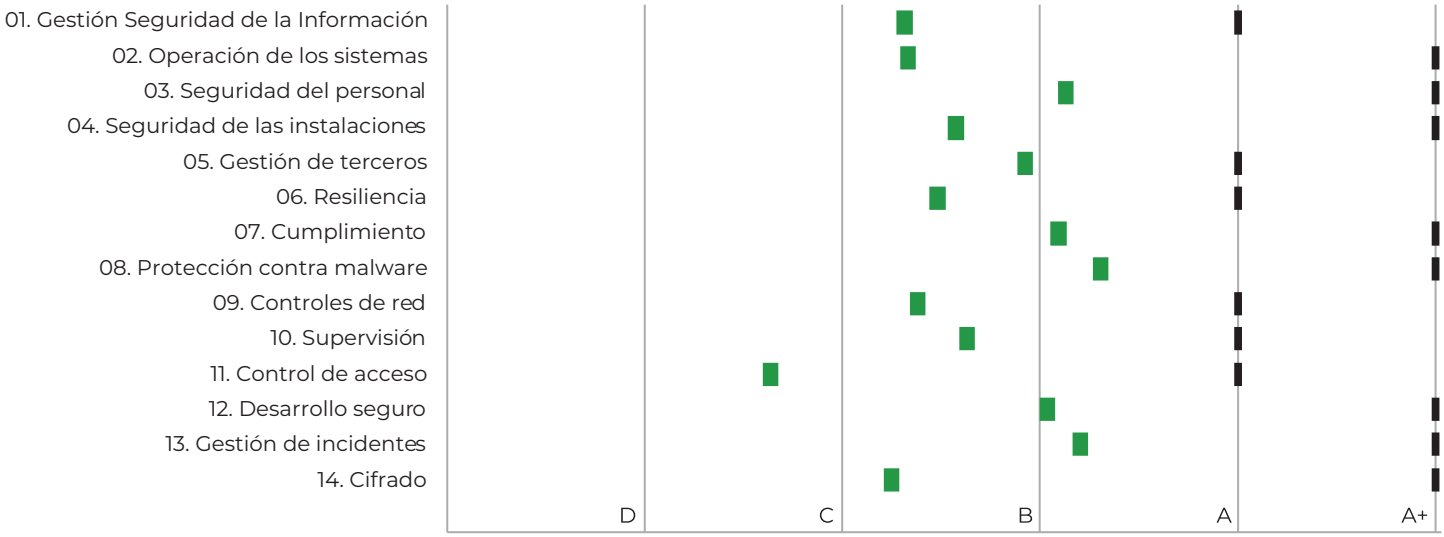
Figura 25. Calificaciones de los servicios calificados

Año tras año, la calificación es renovada en más del 90% de los casos, con lo que **la evolución pone de manifiesto una mejora de los niveles obtenidos**, que ha ido desplazándose en mayores porcentajes desde los más básicos hacia los más elevados. La moda (nivel más frecuente) sigue estando en el C - supone un nivel más que aceptable para una inmensa mayoría de servicios no críticos - pero son un número creciente de casos los que ya se sitúan en un excelente nivel A.

Esta tendencia se viene observando desde los comienzos de nuestra actividad. Los clientes que han optado por la calificación disponen, no solo de un completo sistema de métricas acerca de su posicionamiento en ciberseguridad, sino también de una herramienta que les señala dónde están aquellos aspectos que le permiten mejorarlo, haciendo buena la frase de Lord Kelvin: "Lo que no está definido no se puede medir. Lo que no se mide, no se puede mejorar. Y lo que no se mejora, siempre se degrada".

Además de los niveles de calificación, en 2021 pusimos en marcha el denominado **calificador cuantitativo de resiliencia**: un indicador entre 0 y 1000 que muestra de forma global y ponderada (dando más peso a las secciones con mayor impacto en una detección y prevención temprana de amenazas, aprendizaje y capacidad de recuperación), **cuya valoración también ha mejorado, pasando del 604 en el anterior estudio, al 619 en el actual**.

La calificación también aporta un resultado muy detallado. La siguiente tabla muestra las valoraciones ponderadas medias (en verde), así como las máximas (en negro) que se han obtenido, para los 14 dominios que constituyen el marco de controles de LEET Security:



Al analizar estos resultados, aparte de la consiguiente mejora que se refleja en la calificación global, encontramos un perfil muy parecido a los ejercicios anteriores.

El mejor comportamiento sigue estando en la protección frente a código malicioso, quizás porque es el concepto que primero viene a la mente de todo el mundo y la implantación de sistemas antivirus está tremendamente generalizada desde hace años. **Acompañan** en la parte alta **la seguridad del personal y la gestión de incidentes**.

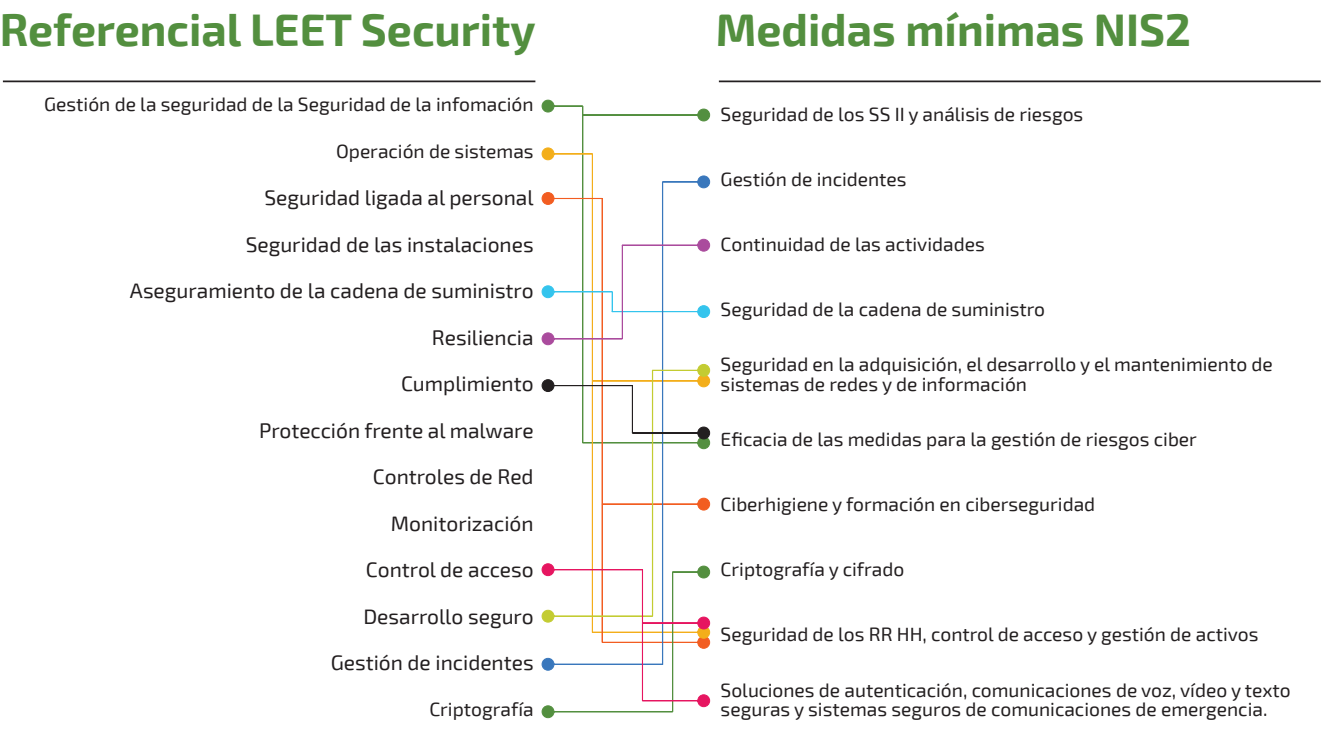
Cabe destacar el dominio relacionado con el personal, ya que las organizaciones están incrementando los esfuerzos en formación y concienciación en ciberseguridad, debido a la importancia que estas tienen como factores preventivos.

Sin embargo, **Control de Acceso sigue estando a la cola**. Este dominio cuenta con unos requisitos altamente demandantes en cuanto a la fortaleza y garantías de los sistemas de autenticación y ciertamente son pocas las organizaciones que cumplen con todos ellos. En todo caso, este resultado refleja la filosofía de mínimos que rige la metodología, ya que, aunque una media aritmética sobre todos los componentes conduce a un resultado notablemente superior, la valoración para el dominio -en cada evaluación realizada- es el mínimo de los resultados en cada una de las secciones que lo componen, con la finalidad de poner de manifiesto el eslabón más débil de la cadena.

La metodología de evaluación y calificación aporta gran utilidad a las organizaciones que se ven obligadas por regulaciones como la directiva NIS 2. El artículo 21 de la misma declara que los órganos de dirección son responsables de garantizar la implantación de medidas técnicas, operativas y de organización, incluyendo una relación de contenidos que están completamente recogidos en el marco de control desarrollado por LEET Security.

Esto otorga a la calificación una función de utilidad adicional: además de disponer de una herramienta que ha demostrado su contribución a la mejora de las capacidades de ciberseguridad, los órganos directivos de las organizaciones obligadas por la directiva cuentan con una herramienta que facilita ejercer sus obligaciones y responsabilidad personal de control para asegurar un adecuado posicionamiento de ciberseguridad en sus compañías.

En cuanto a la gestión de riesgos de ciberseguridad, la Directiva NIS2 recoge un listado mínimo de medidas técnicas, operativas y de organización para gestionar los riesgos de seguridad de los sistemas y redes de información, así como el entorno físico de dichos sistemas. Estas medidas deben ser utilizadas tanto por las entidades esenciales como importantes en sus operaciones o en la prestación de sus servicios para prevenir o minimizar las repercusiones de los incidentes en los destinatarios de sus servicios. Las medidas indicadas como mínimas son las que se incluyen a continuación y se exigirán siempre de forma proporcional a los riesgos y vulnerabilidades específicas y al tamaño de las entidades:



De tal forma que las 10 medidas de obligado cumplimiento establecidas por la NIS2, que incluyen medidas técnicas, operativas y de organización para gestionar los riesgos de seguridad de los sistemas y redes de información, así como el entorno físico de dichos sistemas, están cubiertas por los 14 dominios de la metodología.

OPINIÓN

Cadena de suministro. La importancia de agilizar el control de la seguridad

*[Por **Javier Palacios**, Director Operaciones Servicios Gestionados de Avvale]*

Ya nadie duda de la importancia del control de la cadena de suministro, pero no lo hacemos bien.

Todos tenemos claro que nuestros proveedores son parte de nuestro entorno de seguridad. De su nivel de seguridad depende, en parte, nuestro propio nivel de seguridad.

Por eso, y por "imperativo legal" (porque nos lo imponen todos nuestros procesos de auditoría, incluidas las financieras, y las nuevas regulaciones legales que van surgiendo en todos los ámbitos), todos nos hemos lanzado a controlar a nuestros proveedores, en la mayoría de las ocasiones con cuestionarios que cada vez hacemos más complejos, extensos y en los que exigimos todo tipo de evidencias sin tener en cuenta que muchas de esas evidencias las estamos pidiendo sin tener ningún NDA acordado, ni ningún contrato de servicio firmado (porque suele ser en el proceso previo de la adjudicación), y pidiendo detalles de información que, de por sí, pone en riesgo la seguridad el compartirla abiertamente.

Yo veo dos problemas, dos errores que estamos cometiendo y que nos están desbordando a todos, u obligándonos a invertir una enorme cantidad de recursos (económicos y humanos) en este control.

El primero es que únicamente miramos a quien nos provee de servicios, sin mirar a quien se los proveemos, que también deberíamos hacerlo, a los que también deberíamos evaluar, ya que también forman parte de nuestro entorno de seguridad. Ya sé que esto, lo primero que nos hace pensar es, ¿cómo vamos a explicar desde el punto de vista de negocio que no escogemos un determinado cliente porque supone un riesgo de ciberseguridad? (algo que si hacemos con los proveedores). Lo segundo que nos hace pensar es: "¡todavía más recursos para controlar!", más coste, más tiempo, más esfuerzo.

Parte del problema es que hay certificaciones de seguridad que sólo indican tener un nivel decente de seguridad o, por lo menos, del control de la seguridad, que, aunque en sus versiones actualizadas si entran un poco más en medidas concretas aplicadas, pero se siguen centrando mucho más en la pura gestión. No indican, una vez alcanzado el nivel de seguridad requerido, cómo de avanzada es la implementación de seguridad, hasta qué punto se han implementado medidas adicionales de seguridad que mejoren el nivel respecto al mínimo requerido.

Esto nos lleva a la desconfianza. O por lo menos a la falta de certeza sobre cómo de avanzada es la implementación de medidas adicionales. Y nos devuelve al punto de partida. A tener que auditar y ser auditado por cada tercera parte con la que interactuamos.

De seguir así, todos necesitaremos más recursos de auditoría, más recursos

para realizar seguimientos, más procesos y más complejos para la homologación...

¿Cómo lo resolvemos entonces? Yo veo varios caminos y seguro hay más:

- El primero, mediante la homologación real de terceras partes. Es decir, hacer una primera homologación más completa y que a partir de ahí únicamente sea necesario mostrar un cierto avance. Sin tener que estar continuamente completando los mismos cuestionarios y contestando las mismas preguntas. Esto puede ser aplicable con terceras partes con las que tengamos un trato estable y prolongado en el tiempo.
- El segundo camino es utilizar plataformas de homologación que pongan en contacto a proveedores y clientes, de forma que una única homologación, basada en rigurosos y detallados niveles de cumplimiento de seguridad, sea útil para múltiples clientes, a la vez que un cliente puede seleccionar entre múltiples proveedores, filtrando por los niveles de seguridad requeridos para cada servicio. Ya existen plataformas así, como Pinakes®, aunque muy centrada en un único sector (banca/finanzas).
- El tercer camino es confiar en certificaciones que nos indiquen niveles de cumplimiento, de forma que, en base a una calificación, obtenida mediante la aplicación de métricas conocidas, permita asegurar el nivel real de medidas implementadas y de control de la seguridad, haciendo posible la selección de distintos niveles requeridos en función de la criticidad de la necesidad. Esto sí permite confiar en un certificado. Aquí no estamos aceptando un nivel de base que nos obligue a tener que indagar el nivel adicional de seguridad, estamos teniendo ya esa información, sin esfuerzos (recursos) adicionales requeridos.

Cualquiera de estos caminos nos ayudaría a todos a reducir la sobrecarga en el control de las terceras partes, que se está convirtiendo en una espiral creciente, que, de seguir así, va a requerir una cantidad cada vez mayor de recursos en un crecimiento exponencial.

No sólo reduciríamos la sobrecarga, si no que realmente tendríamos un mejor control, mucho más preciso y, lo más importante, de manera mucho más rápida, algo que en el mundo de la protección es clave.

Tener que esperar semanas (a veces incluso meses) para tener una correcta revisión de terceras partes, es un riesgo en sí mismo. Tener la capacidad de beneficiarnos de las calificaciones correctas, realizadas por terceros realmente independientes y rigurosos, nos permite conocer de manera inmediata la idoneidad para la colaboración o no con una tercera parte.

Esto nos permitiría no sólo mirar hacia “abajo”, hacia los proveedores, si no mirar también hacia “arriba” hacia las terceras partes a las que proveo servicios.

Ese tiene que ser el objetivo de todos, poder asegurar de forma rápida los correctos niveles de seguridad de nuestras terceras partes. Sin demora, sin bloqueos, sin recursos adicionales, sin bloquear el negocio y minimizando los riesgos.

Encadenados, enganchados a la seguridad de nuestros proveedores

*[Por **Mª Elisa Vivancos**, Responsable de ciberseguridad para los Sectores Estratégicos de Cadena de suministro, Pymes y Despachos Profesionales en INCIBE-CERT]*

Es una suerte vivir estos tiempos en los que confluyen una conectividad casi sin límites, una velocidad de proceso acelerada y una gran capacidad de almacenamiento. La innovación en automatización y digitalización está brotando en un entorno fértil para las tecnologías disruptivas, no sin su parte oscura de conflictos éticos, coste medioambiental o de aumento de la superficie de ataque. Y es que, los nuevos modelos de negocio que en ellas se sustentan, tan atractivos y rentables, nos hacen cada vez más dependientes de terceros y por ende de sus riesgos. Estamos enganchados, para lo bueno y lo malo, a nuestras cadenas de suministro. Y, en un entorno hiperconectado y globalizado, los ciberincidentes pueden tener importantes repercusiones económicas y sociales que se han demostrado transfronterizas y globales.

No en vano, la Unión Europea, consciente de esta dualidad, productividad y ciberseguridad, libra una batalla normativa en todos los frentes para mejorar, entre otros, el funcionamiento del mercado interior; la resiliencia de los servicios esenciales para el mantenimiento de funciones sociales o actividades económicas vitales; la resiliencia operativa del sector financiero; la inteligencia artificial; la ciberseguridad en redes 5G; o la de los productos con elementos digitales, como muestra.

En la Directiva NIS2 se aborda la dependencia de la ciberseguridad de las entidades importantes y esenciales de la de sus proveedores de servicios de almacenamiento y tratamiento de datos, de servicios gestionados y de los desarrollos de *software*. Obliga a las empresas a tener en cuenta, en las medidas técnicas operativas y de organización que se adopten, el análisis de los riesgos procedentes de sus relaciones con proveedores y prestadores directos. NIS2 prevé además la posibilidad de llevar a cabo evaluaciones coordinadas de riesgos de seguridad de las cadenas de suministro de servicios, sistemas o productos TIC críticos específicos. El resultado de estas evaluaciones tendrá su peso en las medidas adoptadas por las entidades importantes y esenciales. Por último, a determinadas categorías de entidades, si se detectan niveles insuficientes de ciberseguridad, se les podrá exigir que utilicen productos, servicios o procesos TIC certificados en virtud de un esquema europeo de certificación de ciberseguridad.

Enfocada en la resiliencia de entidades críticas, en la Directiva CER una de las medidas que han de adoptar las entidades en su ámbito consiste en identificar cadenas de suministro alternativas para recuperarse de los eventuales incidentes, y otra, comprobar los antecedentes del personal de servicios externos que ejerza funciones esenciales. Por otra parte, para la identificación de las entidades críticas se tiene en cuenta la dependencia que, a su vez, se genera en otros sectores de estos servicios esenciales, lo que los convierte en cadenas de suministro de terceros.

Un caso particular, es el detallado tratamiento de la gestión del riesgo TIC derivado de terceros de entidades financieras en el Reglamento DORA. El capítulo V comprende una sección con los principios fundamentales para una buena gestión del riesgo TIC derivado de terceros, incluyendo las cláusulas mínimas de los acuerdos contractuales, y otra sección

el marco de supervisión de proveedores terceros esenciales de servicios TIC.

Ya en el **Reglamento CSA** se otorgaba a ENISA capacidades para reforzar las cadenas de suministro dentro de la Unión, por ejemplo, celebrando acuerdos de reconocimiento mutuo relativos a certificados europeos de ciberseguridad que están dando lugar a esquemas europeos de certificación de productos TIC basados en Common Critera, como EUCC.

En este sentido, el recientemente aprobado Reglamento CRA aborda los requisitos obligatorios de seguridad para productos con elementos digitales. Estos productos contienen y dependen de componentes software que pueden ser desarrollos de terceros. Entre los requisitos: que se comercialicen sin vulnerabilidades, con una configuración segura por defecto y que se tenga en cuenta la ciberseguridad en todo su ciclo de vida. Por otra parte, obliga a los fabricantes a ofrecer un soporte durante al menos cinco años, gestionar las vulnerabilidades y lanzar las actualizaciones que las corrijan. Clasifica los productos en varios niveles, productos importantes (clase I y II) y productos críticos con elementos digitales. Estos últimos se consideran dependencias críticas de las entidades esenciales de la Directiva NIS2 y para ellos la CE estudia que sean sometidos a certificaciones cuando exista un esquema europeo de certificación pertinente y en su caso se haya realizado la evaluación de su impacto en el mercado.

Por todo esto, los años siguientes se aventuran al menos emocionantes a la espera de que entre en vigor alguna de estas normas, se traspongan otras a la legislación nacional, terminen los periodos de la carencia o se publiquen las normas derivadas que en ellos se especifican. Esperemos que todo este despliegue normativo redunde en un enganche sólido y seguro de las entidades afectadas y sus cadenas de suministro que permita servicios esenciales y mercados digitales más ciber resilientes.

La ciberseguridad en la Gestión 5.0 del futuro: Claves para una estrategia empresarial integral

*(Por **Ignacio Babé**, Director General - CEO del Club Excelencia en Gestión)*

La creciente digitalización y la transformación empresarial han traído consigo innumerables oportunidades, pero también han generado nuevos riesgos y vulnerabilidades, sobre todo en lo que respecta a la ciberseguridad. En este contexto, los líderes empresariales deben abordar el tema de forma estructurada e integral. Los estudios sobre ciberseguridad, como los realizados por LEET Security en colaboración con el Club Excelencia en Gestión, demuestran que la mayoría de las organizaciones han incrementado su preocupación por las amenazas cibernéticas, aunque aún queda mucho por hacer para gestionar estos riesgos de manera efectiva. La integración de la ciberseguridad dentro de los modelos de gestión, conce-

bidos como sistemas, tal y como hace el Modelo EFQM, puede ofrecer soluciones clave para un enfoque empresarial sostenible y orientado hacia el futuro.

Los sucesivos estudios realizados reflejan la magnitud de las amenazas actuales, donde, de manera creciente, (casi 3 de cada 5 en la actualidad) de las empresas considera que los riesgos de ciberataques son mayores que en el pasado, lo que ha llevado a casi el 70% de las organizaciones a aumentar sus inversiones en esta área. Y creciendo. Sin embargo, a pesar de este incremento en la inversión, sigue habiendo carencias importantes en la gestión de riesgos asociados a terceros. De hecho, el estudio revela un preocupante porcentaje de empresas que no realiza ningún tipo de evaluación de sus proveedores de servicios, lo que pone en peligro no solo la seguridad de sus datos, sino también la continuidad de sus operaciones.

El papel crítico de los proveedores y la cadena de suministro en la seguridad de las empresas es otro dato que ha destacado en cada uno de los estudios. Con un 63,6% de las empresas permitiendo que proveedores externos se conecten a sus sistemas, el riesgo de ciberataques a través de terceros es elevado. Estos datos subrayan la necesidad de un enfoque proactivo que vaya más allá de las medidas técnicas tradicionales, y que incluya la gestión de la relación con proveedores y la evaluación continua de sus capacidades de seguridad.

En este escenario, el Modelo EFQM se presenta como una herramienta muy útil para integrar la ciberseguridad en la estrategia y gestión empresarial. El Modelo EFQM es un modelo referencial de gestión que fomenta la excelencia y la mejora continua a través de una estructura flexible que se adapta a las necesidades cambiantes del mercado. Este enfoque, que promueve una visión integral de la gestión empresarial, concebida como un sistema, es esencial para afrontar los desafíos actuales de la ciberseguridad. Recordemos que los sucesivos estudios realizados muestran que las organizaciones que aplican este tipo de enfoques estructurados tienden a tener una mayor conciencia sobre los riesgos cibernéticos y una inversión más significativa en medidas de protección.

Uno de los aspectos clave del Modelo EFQM es su capacidad para integrar diferentes áreas de la organización en torno a un objetivo común de mejora continua y sostenibilidad. En el ámbito de la ciberseguridad, esto implica que las organizaciones no solo deben invertir en tecnologías de seguridad, sino también en procesos de gestión de riesgos que involucren a toda la empresa, desde la alta dirección hasta los departamentos operativos. De hecho,en cada uno de los estudios se ha hecho patente la importancia de que la ciberseguridad sea vista como una responsabilidad compartida por toda la organización, y no solo como un asunto técnico gestionado por el área de TI.

La gestión (el management) del futuro requiere un enfoque holístico, donde la resiliencia cibernética se considere un pilar fundamental de la estrategia empresarial. El Modelo EFQM permite a las organizaciones adoptar este enfoque, integrando la ciberseguridad dentro de su sistema de gestión global, y garantizando que los riesgos relacionados con terceros sean debidamente evaluados y gestionados.

El futuro de la gestión de las organizaciones está estrechamente vinculado a su capacidad para integrar la ciberseguridad en sus procesos y estrategias de gestión. El Modelo EFQM, con su enfoque en la excelencia, la innovación, la sostenibilidad y la mejora continua, ofrece el marco ideal para que las empresas puedan gestionar de manera efectiva los riesgos cibernéticos y garantizar la protección de su cadena de valor. En un entorno empresarial cada vez más digital y conectado, aquellos que logren integrar estos aspectos en su gestión estarán mejor preparados para enfrentar los desafíos del futuro y prosperar en un mercado cada vez más competitivo y exigente.

La gestión del riesgo de terceros y la cadena de valor

*(**Daniel Gil** - Miembro de la Junta Directiva de CCI y Director de Compras de Unicaja)*

Cada vez operamos en mercados más complejos e interconectados. Esta circunstancia, unida a la evolución continua y la velocidad en el cambio que el mercado demanda, hace que sea indispensable apoyarnos en empresas externas, terceros especialistas en ámbitos que no son nuestro negocio core y que nos permiten ampliar nuestras capacidades.

El principal problema que encontramos en este ecosistema es la dificultad para conocer con pleno detalle y garantizar el grado de protección, seguridad y gestión de riesgos de todos nuestros proveedores. Esto, unido a que el eslabón más débil de la cadena es donde siempre se concentra el mayor riesgo y el que tiene más probabilidades de provocar un fallo o incidente, hace que, aunque tengamos una protección adecuada en nuestros sistemas e infraestructuras tecnológicas, nuestro riesgo se sitúe en el nivel del elemento de mayor debilidad.

Este hecho no ha sido pasado por alto por la normativa europea, tanto en el ámbito de la Resiliencia Operativa Digital, con la normativa DORA, que será de obligado cumplimiento para empresas de servicios financieros y asegurador a partir de enero de 2025, como en el ámbito de la Sostenibilidad y la Responsabilidad Social Corporativa, con la nueva Directiva de Diligencia Debida, que ha sido aprobada recientemente.

En ambos casos, la normativa intenta controlar la cadena de valor en toda su amplitud, haciendo responsable a las empresas obligadas del control transversal de la cadena de valor o suministro, y asumiendo el control total no sólo de su actividad sino de la de sus proveedores en los productos que suministran o servicios que prestan, o los efectos que puede causar el producto y servicio desde su consumo hasta su reciclaje o destrucción.

En este nuevo ecosistema normativo cobra especial importancia realizar un análisis de riesgos de nuestros proveedores, mucho más exhaustivo, de forma continua y desde un momento preliminar, contemplando dos perspectivas:

1. Servicio. Se debe analizar el riesgo inherente del servicio que se recibe, tanto desde un punto de vista del impacto que puede producir una discontinuidad o incidencia en el mismo, como de la probabilidad de su ocurrencia. Esto nos permitirá catalogar ese servicio con un nivel de riesgo determinado, que marcará las bases para el tipo de proveedor que puede prestarlo. Los elementos de riesgo que debe considerarse, en función de la tipología, incluyen desde el ciberriesgo, hasta la protección de datos, continuidad de negocio o impacto medioambiental, entre otros.
2. Proveedor. Una vez definidos los riesgos y catalogado el servicio en función del análisis realizado, debemos garantizar que nuestros proveedores están capacitados para la prestación del mismo, de acuerdo con los procesos de control o elementos mitigadores del riesgo que hayamos asignado. Para ello es necesario rediseñar y robustecer el sistema de homologación de nuestros proveedores, asegurando no sólo la capacidad del proveedor para prestar el servicio, sino garantizando que dispone de un grado de madurez acorde con nuestras políticas y que realiza una gestión interna adecuada en cuestiones de responsabilidad social corporativa y respeto a los derechos humanos, no sólo en su ámbito sino extendido a los proveedores que subcontraten para la realización de la actividad.

El servicio Pinakes, desarrollado de forma colaborativa entre el Centro de Cooperación Interbancaria (CCI) y LEET Security, es un claro ejemplo de iniciativa que tiene como objetivo la mitigación del riesgo de nuestros proveedores. A través de una calificación focalizada en la confidencialidad, integridad y disponibilidad de la información, a través de más de 1.000 controles verificados anualmente por un auditor externo se garantizan las medidas de protección y control que el proveedor tiene implantadas, así como la robustez de sus procesos internos. Este tipo de soluciones nos facilitan dar respuesta y cumplimiento de una forma adecuada y colaborativa a los requerimientos normativos y a nuestras propias políticas internas.

Cybersecurity and digital infrastructure: A data center paradox

*(**Andy Lawrence**, Executive Director of Research de Uptime Institute)*

Uptime Institute's research suggests cybersecurity threats are a growing threat to data centers. Managers are doing more, but many are aware it is not enough.

For many years, experts have been issuing a warning to operators of data centers and other related critical infrastructure: the threat of a malicious cyber-attack does not just apply to the IT that is hosted in your facilities, but also to the operational technology itself. Systems that manage power, cooling, water are just as critical to continued and safe operation as the processing, storing and networking of data.

This warning is underlined with some examples of some serious attacks that have affected operational technology. A very small number of these examples include data centers. Despite this, cybersecurity, which comes near the top of IT management concerns and merits a heavy investment, are rarely mentioned – or heavily invested in – by data center or facilities managers. In enterprises, responsibility is assumed to be the domain of the IT security team, which has little direct involvement in the data center and its exotic equipment for managing power, cooling, and environmental conditions.

This, then, is the paradox: Data center managers are acutely aware of the costs of outages and invest very heavily, in time and money, to prevent them. But they pay insufficient attention to cybersecurity concerns, relying on IT departments, occasional and sometimes inadequate certification by third parties, and on an assumption that air gapping of operational equipment, and the low profile and proprietary nature of the facilities systems, will protect them. (There are, of course, some standout exceptions to this).

Awareness rising

If this is changing, it is only happening slowly. Threats to data center cybersecurity continued to rise in 2024, with three in four operators saying they have experienced a cyber incident in the past three years, according to the Uptime Institute Data Center Security Survey 2024. But only about one in ten operators say

they have had a serious or severe incident in that time, perhaps partially explaining why the level of concern in the industry is still relatively low.

A low level of concern does not mean inaction. Uptime Institute regularly encounters operators who conduct exceptional due diligence on all equipment and software, and who are constantly vigilant, embedding security in operational practices. And, in fact, survey data suggests that a wide range of cybersecurity procedures and assessments are conducted (see figure one below).

But there is another oddity, if not a paradox. Despite the low level of incidents, and of the many assessments that are carried out, only half (51%) of 218 operators said they believe their company's cyber assessments are effective (44% said "somewhat effective"). Operators and managers, it seems, are themselves uneasy about their own levels of protection.

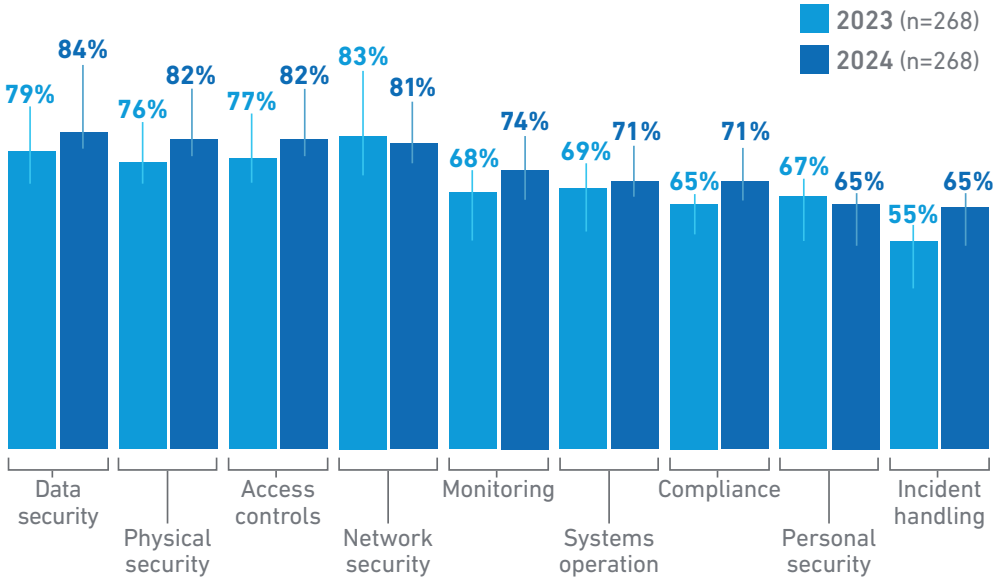
Uptime Institute's research also pointed to an overlooked cybersecurity problem: cybersecurity systems can prevent a rapid and ordered recovery of critical systems after an outage – and outages also get management attention. This is because, after power and cooling systems are stabilized, servers running the authentication directory (AD) need to be recovered so that legitimate users and systems can be granted secure access to resources within the network. However, if recovery of these servers is mismanaged or encounters issues, security systems may block access to operating platforms. In a recent Uptime study, a surprising 10% of respondents said their most impactful cyber security incident was caused by a power outage – and such outages are themselves rare events.

The recovery and reconfiguration of security systems often not included in data center emergency operating procedures (EOPs). But this is not surprising: data center managers are insufficiently trained in cyber security issues – and cyber and IT specialists tend not to know enough about, or pay enough attention to, the operational technology in the data center.

*References: A series of reports by Michael O'Neill and Antonio Ramos on cyber security policies for data centers is available at info@leetsecurity.com. Some of the findings from Uptime Intelligences 2024 Cyber security survey can be found here (***https://intelligence.uptimeinstitute.com/resource/operators-boost-cyber-security-efforts-more-work-needed***).*

Cybersecurity assessments are becoming more robust

Which of the following areas are reviewed by your organization when conducting data center cybersecurity assessments? Choose all that apply.



UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2024

uptime INTELLIGENCE

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

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

www.leetsecurity.com

LEET SECURITY

CyberSecurity
Rating Agency