OBS Business School

Estado de la Ciber-Inseguridad: realidades y percepciones

Ramón Miralles López
Profesor de OBS Business School

Septiembre, 2024

Partners Académicos:

Universitat de Barcelona

unie Universidad

OBSbusiness.school

Autor

Ramón Miralles López
Profesor de OBS Business School

Ramón Miralles es licenciado en Derecho por la Universidad de Barcelona, colegiado como ejerciente en el Ilustre Colegio de Abogados de Barcelona, con una experiencia profesional de más de 38 años en el sector de las TIC, dedicados fundamentalmente a dirigir proyectos de modernización digital en las administraciones públicas, primero en oficinas judiciales y después en la administración de la Generalitat de Catalunya y en el Ayuntamiento de Barcelona, asimismo destaca por su actividad en el ámbito empresarial, siendo actualmente Socio Director del Departament de Privacidad, Compliance y Ciberseguridad en ECIJA Abogados, en Barcelona.

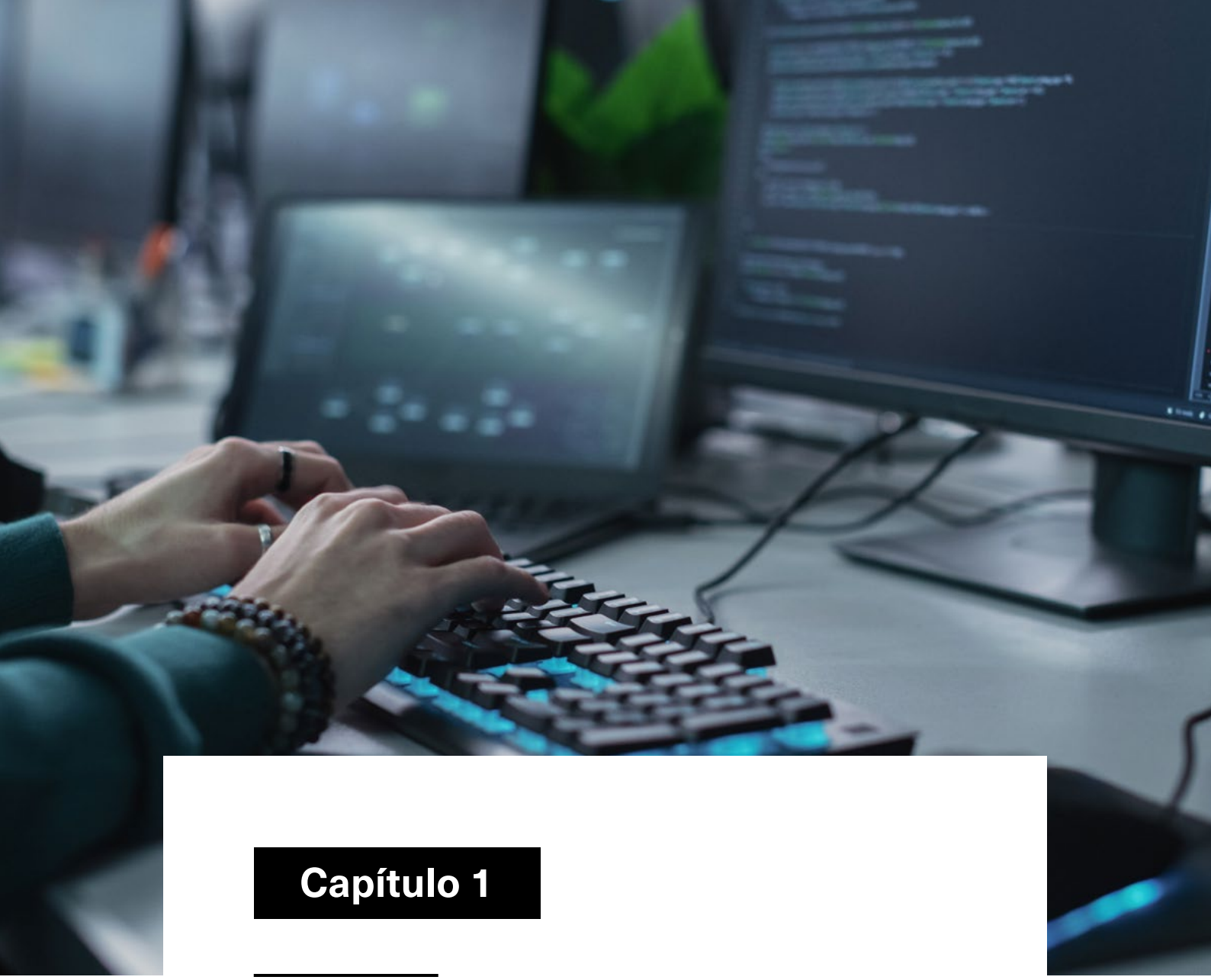
Experto en sistemas de gestión de la seguridad de la información, y gestión de riesgos legales y tecnológicos, ha ocupado posiciones de CISO (seguridad de la información), CIO (tecnologías de la información) y CAE (auditoria), certificado profesionalmente en ámbitos de seguridad de la información y privacidad, y miembro de las juntas directivas de diferentes asociaciones profesionales.

Profesor en diversos masters de formación permanente en OBS Business School: Ciberseguridad, Dirección de Sistemas y Tecnologías de la Información, Global Data Management, Machine Learning e Inteligencia Artificial y Tech MBA, así como en diversas Universidades y centros de estudios, en los que imparte materias relacionadas con los aspectos éticos y legales en el uso de las TIC.

Ha participado activamente en proyectos relacionados con las tecnologías y la acción social, entre otros, en la consultoría TIC para el desarrollo del eje tecnológico del plan estratégico de la Defensa Pública de Costa Rica, en el contexto del programa Eurosocial II de la Comisión Europea, y en el grupo impulsado por la Red Iberoamericana de protección de datos, dedicado a la adecuación al derecho a la protección de datos de carácter personal en la acción humanitaria internacional.

Ha recibido diferentes reconocimientos y premios: por el directorio internacional Best Lawyers, en sus ediciones 2022 y 2023, en el área de “Privacy & Data Protection Law”, y adicionalmente en la edición 2023 premiado como "Lawyer of the Year" por su trabajo en el área de Privacy & Data Protection Law en Barcelona; premio colectivo de la Agencia Vasca de Protección de Datos 2018 al *“Observatorio Iberoamericano de Protección de Datos”*; y premio 2018 al profesor mejor valorado por los alumnos del plan de formación de la Asociación Profesional Española de Privacidad (APEP).

Índice



Capítulo 1

Introducción y contexto

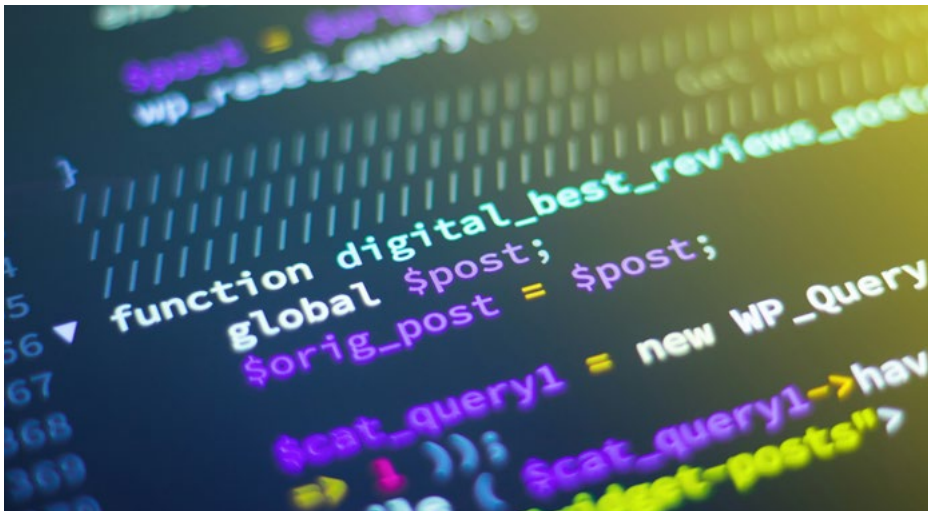
Desde el año 2006 el World Economic Forum[1] publica el "*Global Risks Report*", que nació con el propósito de dotar de conocimiento sobre los riesgos de todo tipo, a los responsables de la toma de decisiones en los ámbitos gubernamental y empresarial, con el objetivo de que pudieran abordar de manera preventiva las incertidumbres a las que potencialmente deberían enfrentarse durante el periodo de los 10 años siguientes a cada informe de riesgos globales; contextualizando el inicio de los citados informes, debe tenerse en cuenta que, en esos momentos, el mundo estaba próximo a una crisis financiera que posteriormente tuvo consecuencias, a nivel global y de largo alcance, para las economías y las sociedades.

1 El Foro Económico Mundial es una organización internacional creada en 1971 cuya actividad se orienta a la cooperación público-privada, ofreciendo una *"plataforma global, imparcial y sin fines de lucro para establecer vínculos significativos entre las partes interesadas con el fin de generar confianza y desarrollar iniciativas para la cooperación y el progreso"*. https://www.weforum.org/

Aunque la metodología de los informes se va actualizando de unos a otros informes, durante prácticamente 2 décadas estos se han basado en la denominada "*Encuesta de Percepción de Riesgos Globales*" (GRPS[2], por sus siglas en inglés), siendo esta la principal fuente de datos sobre riesgos globales del Foro Económico Mundial; las encuestas se dirigen a expertos del mundo académico, las empresas, el gobierno, la comunidad internacional y la sociedad civil[3].

Además, para complementar los datos de la GRPS, en él informe también se incluye[4] la "*Encuesta de Opinión Ejecutiva*" (EOS[5], por sus siglas en inglés), que tiene por objeto identificar los riesgos que representa la amenaza más grave para cada país en los dos siguientes años, para ello se cuenta con la opinión de más de 11.000 líderes empresariales en 113 economías, que proporcionan información sobre la percepción de los riesgos globales a nivel regional.

En el marco de los citados informes de riesgos globales, se entiende como riesgo global "*la posibilidad de que ocurra un evento o condición que, de ocurrir, afectaría negativamente a una proporción significativa del PIB, la población o los recursos naturales mundiales*"[6]; los riesgos globales se clasifican en 5 tipos, según su potencial impacto: económico, ambiental, geopolítico, social y tecnológico.



Por lo que respecta a los riesgos de carácter tecnológico[7], en la siguiente tabla se refleja la evolución de esa categoría durante el periodo 2021-2024, teniendo en cuenta exclusivamente las 10 primeras posiciones; por lo que respecta al presente informe, nos centraremos en los riesgos relacionados con la "ciber-inseguridad", entendiendo esta como la amenaza, y considerando que la ciberseguridad son las decisiones y soluciones que pretenden mitigar los riesgos derivados de tal amenaza.

2 Global Risks Perception Survey.
3 El informe del año 2024 se basa en las respuestas de 1.490 expertos, y se realizó del 4 de septiembre al 9 de octubre de 2023.
4 Esta encuesta se incluyó a partir del año 2022.
5 Executive Opinion Survey.
6 Ver apartado "Overview of Methodology" del "The Global Risks Report 2024" (p. 5), disponible en Global Risks Report 2024 | World Economic Forum | World Economic Forum (weforum.org)
7 Los ciberataques y la ciberseguridad se sitúan entre los riesgos de carácter tecnológico

Existen diferentes definiciones de los que debemos entender por "ciberseguridad"[8], pero no debemos quedarnos con la idea de que se trata de una cuestión que exclusivamente tiene que ver con los "ciberataques", es decir, con un origen malintencionado, ya que también las situaciones accidentales deben ser abordadas desde la perspectiva de la ciberseguridad.

Figura 01 → EVOLUCIÓN DE LOS RIESGOS DE CARÁCTER TECNOLÓGICO

Fuente: Elaboración propia

Año	Riesgo	Posición 0-2 años[9]	Posición 2-5 años[10]	Posición 5- 10 años[11]
2021	Cybersecurity failure	4	8	-[12]
2021	Digital inequality	5	-	-
2021	IT infrastructure breakdown	-	2	-
2021	Tech governance failure	-	9	-
2021	Adverse tech advances	-	-	4
2022	Cybersecurity failure	7	8	-
2022	Digital inequality	9	-	-
2022	Adverse tech advances	-	-	8
2023	Widespread cybercrime and cyber insecurity	8	n/a[13]	8
2024	Misinformation and disinformation	1	n/a	5
2024	Cyber insecurity	4	n/a	8
2024	Adverse outcomes of AI technologies	-	n/a	6

Con relación a la "ciber-inseguridad", de los anteriores datos se pueden desprender algunas conclusiones:

- En primer lugar, en los informes de los años 2021 y 2022, se considera la ciberseguridad como un riesgo a corto y medio plazo, pero no aparece como un riesgo para tener en cuenta a largo plazo; ello puede ser debido a que se consideraba que era un riesgo de posible mitigación, por el propio avance y mejora las tecnologías dedicadas a la ciberseguridad y que, por tanto, a largo plazo no iba a tener una relevancia significativa.
- En los informes de los años 2023 y 2024 se produce un cambio metodológico, y desaparece la percepción a medio plazo, analizándose exclusivamente los riesgos a corto (2 años) y largo plazo (10 años); en los informes no se indican los motivos de haber prescindido de los riesgos a medio plazo.

8 Tal vez una de las definiciones más precisas y comprensibles sea la de ISACA (Information Systems Audit and Control Association), para la que la ciberseguridad es la: *"Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".*

9 "Peligros claros y presentes. Riesgos a corto plazo". *Clear and present dangers Short-term risks (0 – 2 years)*

10 "Efectos colaterales. Riesgos a medio plazo". *Knock-on effects Medium-term risks (3 – 5 years)*

11 "Amenazas existenciales Riesgos a largo plazo". *Existential threats Long-term risks (5 – 10 years)*

12 El guion (-) indica que no aparece entre los 10 primeros riesgos

13 En los informes de 2023 y 2024 no se incluye la previsión a medio plazo (3-5 años)

- En el informe del 2023 la ciberseguridad se vincula a la ciberdelincuencia, si bien en el informe de 2024 se volvió a incluir de manera autónoma la inseguridad cibernética generalizada.
- Por último, cabe mencionar que, en el 2024, se incluyen como riesgos a largo plazo las consecuencias adversas de las tecnologías de inteligencia artificial (IA).

En todo caso, y sin perjuicio de los cambios metodológicos experimentados en los *"Global Risks Report"*, la ciberseguridad siempre se ha situado entre el "top 10" de los riesgos a corto plazo, por tanto, es una preocupación que se mantiene viva, y de hecho en el 2024 volvió a situarse en niveles del 2021, en cuanto a percepción del riesgo que podía suponer, situándose entre las 5 primeras posiciones del ranking.

La anterior conclusión obliga a considerar la "ciberseguridad" como una cuestión sobre la que debe hacerse un especial foco, dedicándole los recursos necesarios para que sea realmente efectiva, y cumpla con su función de mitigar la inseguridad que generan las ciberamenazas, a lo que debe añadirse que la percepción del 2021 y 2022, de que no era un riesgo que debiera tenerse en cuenta a largo plazo, se ha visto claramente modificada, ya que no solo se ha mantenido a corto plazo, si no que ha escalado posiciones y, si bien como consecuencia del cambio metodológico del 2023, aparece como un riesgo a largo plazo, es cierto que lo hace en posiciones más bajas, con lo que tal vez se mantiene un cierto optimismo de que, finalmente, las soluciones y decisiones relacionadas con la ciberseguridad harán que sea un riesgo menos significativo, aunque no sea esa la tendencia, como veremos a lo largo de este informe.

Capítulo 2

Las predicciones sobre ciberseguridad

El conocimiento del entorno y la madurez de los análisis de ciberseguridad provocan que las previsiones que suelen hacer cada año las empresas y organizaciones especializadas en esta materia, sean cada vez más precisas; hace algo más de una década, ese tipo de previsiones se sustentaban más en las percepciones de los expertos[14], y no tanto en un análisis basado en datos, aun así, el acierto se podía considerar aceptable; actualmente, en todas esas previsiones podemos detectar unanimidad en una serie de cuestiones que efectivamente acaban siendo una realidad.

14 Dejando de lado los intereses comerciales, que también pueden influir en las previsiones sobre tendencias.

Tal vez el uso de la inteligencia artificial, para hacer previsiones con relación a los riesgos de ciber-inseguridad y respecto de las medidas a adoptar para mitigar tales riesgos, influya en esa unanimidad, pero lo cierto es que el acierto es ahora más que aceptable y, para constatarlo, nada mejor que tener en cuenta las previsiones que se hicieron para el 2024 y verificar que es lo que ha sucedido, ahora que ya llevamos consumidas una buena parte del año.

El esquema mental que deben adoptar los responsables de ciberseguridad es que deben enfrentarse a riesgos de ciber-inseguridad, que pueden tener su origen tanto en las amenazas vinculadas a los ciberataques (malintencionados), como en los fallos de ciberseguridad (sean accidentales o derivados de errores propios), y que la mitigación de tales riesgos pasa por adoptar controles que reduzcan o mantengan ese riesgo de ciber-inseguridad en niveles que sean aceptables para la organización, por tanto, hay que ampliar el espectro de amenazas que deben ser tenidas en cuenta, ya que como analizaremos, los ciber-incidentes no siempre tienen su origen en ataques malintencionados que acaban teniendo éxito, aunque puedan ser los más habituales, ni tampoco las consecuencias de los ciberataques son siempre más gravosas que las de otro tipo de ciber-incidentes que puedan tener su origen en errores o accidentes de origen interno, a pesar de que estos se produzcan de manera más aislada o puntual.

Las previsiones relacionadas con la ciberseguridad suelen plantear tendencias, de las que se infieren los incidentes que presumiblemente afectarán la seguridad de los ciber-activos de información[15], lo que consecuentemente provoca la identificación de cuáles deberían ser las prioridades de protección para las organizaciones.

Un dato objetivo, aunque sea cualitativo, es que el número y la gravedad de los ciber-incidentes va aumentado y, en consecuencia, la presión es constante, esta circunstancia ha tenido como primera consecuencia que una parte importante de los presupuestos de las organizaciones se esté destinando a ciberseguridad, ya que estas son conscientes de los efectos negativos de los ciber-incidentes, puesto que no solo impactan en la propia actividad de la organización y provocan pérdidas económicas, también la reputación de la organización tanto de cara a clientes, como al mercado en el que desarrolla sus actividad, se ve dañada, así no es de extrañar que en las previsiones de gasto tecnológico que para el 2024 hizo Gartner, se estimaba que el 80% de los CIO estaban planificando aumentar el gasto en ciberseguridad.

No es objeto de este informe relatar de manera exhaustiva cuáles fueron las previsiones hechas para el 2024, pero siguiendo el esquema de las (i) tendencias en ciberseguridad, los (ii)ciber-incidentes con más incidencia y las (iii)prioridades de protección, vamos a identificar y describir brevemente 10 cuestiones para cada grupo de previsiones, que ya están teniendo un peso significativo durante el 2024 y que, con toda seguridad, tendrán incidencia durante el 2025.

15 El actual grado de desarrollo y despliegue del uso de las tecnologías de la información y la comunicación nos permite considerar que prácticamente todos los activos de información de las organizaciones están expuestos a la ciber-inseguridad.

2.1 Las tendencias en ciberseguridad

Las tendencias identificadas a continuación, no dejan de ser variables de entorno y circunstancias que, con carácter general, van a influir en el tipo de ciber-incidentes que potencialmente van a tener una mayor incidencia a nivel global, y en las prioridades en cuanto a medidas técnicas y organizativas para mitigar el riesgo de las ciber-amenazas que hay detrás de tales incidentes de seguridad.

1. A nivel global, la presión regulatoria derivada de obligaciones jurídicas y, por tanto, la necesidad de gestionar el cumplimiento normativo, tanto en materia de privacidad como de ciberseguridad, va a requerir importantes esfuerzos para mitigar los riesgos legales de incumplimiento; resulta especialmente relevante la actividad regulatoria en Latinoamérica en lo que se refiere de la protección de datos personales, entre otros cabe mencionar nuevas leyes o modificaciones de leyes previas, en Paraguay, Costa Rica, Chile y Argentina.

2. Como consecuencia de lo anterior y, por supuesto, del incremento de los ciberataques, los seguros de ciberseguridad van a aumentar su presencia en la estrategia de ciberseguridad de las organizaciones, y sus coberturas se van a extender específicamente a Directivos y mandos intermedios o responsable de departamentos, en particular, por los niveles de responsabilidad que van a tener que asumir desde la perspectiva normativa citada en el punto anterior.

3. Los 3 ámbitos a los que se van a dedicar más recursos económicos son: la lucha contra la desinformación, la seguridad de los servicios en la nube y, en general, la formación sobre ciberseguridad para los empleados.

4. Se va a hacer foco en la reducción de ciber-incidentes que tienen su origen en los empleados, lo que va a incluir, entre otras decisiones, un especial esfuerzo en la identificación de comportamientos sospechosos por parte de estos.

5. Desde el punto de vista estratégico, el enfoque Zero-Trust[16] va a predominar claramente en la toma de decisiones en materia de ciberseguridad.

6. El despliegue de la inteligencia artificial en las organizaciones va a ser un factor de riesgo que va a ir ganando peso, por tanto, las organizaciones van a tener que actualizar su mapa de riesgos para incluir las amenazas relacionadas con la IA.

7. Gana importancia la ciberseguridad aplicada a la cadena de suministro, con un claro enfoque a aumentar la ciber-resiliencia en las cadenas de suministro mundiales[17].

16 Según IBM en https://www.ibm.com/es-es/topics/zero-trust, el modelo *"Zero Trust es una infraestructura que parte de la premisa de que la seguridad de una red compleja está siempre en riesgo ante las amenazas externas e internas. Permite organizar y elaborar una estrategia para contrarrestar esas amenazas."*; básicamente se parte de la presunción de que todas las conexiones a los activos de información sean internas o externas, y de inicio a final, son una amenaza y, por tanto, deben tomarse decisiones para protegerse de esas amenazas.

17 Para más información ver Cómo reforzar la ciberresiliencia en la cadena de suministro de la manufactura avanzada | Foro Económico Mundial (weforum.org)

8. Las organizaciones van a hacer foco en la ciber-resiliencia[18], incluso la presión regulatoria va a ir en ese sentido[19].

9. La incidencia de los ciber-ataques va a requerir mejorar la capacidad de repuesta ante los ciber-incidentes, de ahí que las organizaciones se vayan a centrar en la mejora de los procesos destinados a gestionar las brechas de seguridad; en esta cuestión la presión regulatoria también obliga a ello, ya que muchas normas establecen obligaciones de notificación de los incidentes de seguridad a las autoridades competentes, e incluso la comunicación de estas a los clientes y usuarios que, de un modo u otro, se hayan podido ver afectados por tales incidentes.

10. El alto grado de especialización que requiere la toma de decisiones en materia de ciberseguridad, y la propia operativa de esta actividad, va a incidir en un claro aumento en la externalización de los servicios de ciberseguridad.

18 Según Akamai en ¿Qué es la ciberresiliencia? | Akamai *"La ciberresiliencia hace referencia a la capacidad de una organización para prevenir, detectar, dar respuesta y recuperarse rápidamente de las interrupciones de TI. Estas pueden ser incidentes de seguridad tales como ciberataques, así como el corte del suministro eléctrico, desastres naturales, fallos en el equipo, errores humanos y otras crisis y desafíos conocidos y desconocidos."*

19 Por ejemplo, la Ley de Ciberresiliencia de la UE, para más información QANDA_22_5375_EN.pdf (europa.eu)

2.2 Los ciber-incidentes

1. Los ataques tipo “ransomware” van a seguir muy presentes, y van a ser más avanzados, evolucionando hacía nuevas formas de interacción con los sistemas de información y redes, y con los usuarios, que darán como resultado un aumento de su tasa de éxito.

2. Lo mismo podemos decir de la evolución de los ataques de “phishing”, que van a ser más sofisticados y de una mayor dificultad de detección[20].

3. Se va a producir un aumento de ciberataques y de las potenciales amenazas a los perfiles ejecutivos de las organizaciones; la combinación de diferentes técnicas de ataque va a ser clave para provocar esa mayor incidencia sobre los ejecutivos y la alta dirección.

4. Los ciberataques impulsados por IA van a aumentar, tanto en número, como en la gravedad de sus consecuencias, ya que los ciber-atacantes van a aprovechar todas las posibilidades que les ofrece la IA, especialmente aquellas relacionadas con su función generativa.

5. El hecho de que vaya a seguir creciendo el número de dispositivos conectados a la red va a plantear desafíos de seguridad en el Internet de las cosas (IoT), de modo que todos los agentes implicados, desde fabricantes, desarrolladores, integradores, e incluso los usuarios, deberán tener muy presentes las amenazas que se derivan de esa amplia conectividad de todo tipo de dispositivos, y de su consecuente exposición a diversos tipos de ciber-amenazas.

6. El uso de la ingeniería social en la configuración de los ciberataques va a seguir presente, pero con mayores grados de sofisticación, en particular en lo que se refiere a suplantación de identidades[21] que, de manera instrumental, van a permitir generar nuevos tipos de ataques, con una alta probabilidad de que acaben siendo incidentes sobre los activos de información, persiguiendo como fin último causar importantes daños y perjuicios económicos.

7. Aunque anteriormente se ha hecho referencia al hecho de combinar diferentes técnicas de ataque, conviene tener presente que, con carácter general, y prácticamente por defecto, los ataques van a ser “multivectoriales”[22].

20 Se estima que en el año 2023 el 83% de las empresas estuvieron expuestas a ataques de phishing.
21 La inteligencia artificial va a tener una especial incidencia en esta cuestión.
22 Según Check Point en ¿Qué es un ataque multivectorial? - Software Check Point “*Un ataque multivectorial se define por el uso simultáneo de múltiples vectores de ataque o métodos de entrada al sistema de una organización. Por ejemplo, un atacante puede lanzar simultáneamente un ataque de phishing y un ataque DDoS o combinar el phishing con el relleno de credenciales.*”

8. Los propios sistemas de inteligencia artificial van a ser objeto de ciberataques, en particular de los denominados "ataques adversarios", que es un ciberataque que, mediante la introducción de datos engañosos en los modelos de IA, induce a estos a que proporcionen resultados distorsionados, se conoce también como "Adversarial ML"[23], que se está manifestando particularmente en usos de la IA para la clasificación de imágenes y para la detección de spam.

9. Los ciberataques relacionados con la geopolítica y la desinformación van a tener un lugar principal en el ranking de ciber-incidentes, especialmente como consecuencia de los conflictos internaciones (armados y comerciales) y las tensiones políticas internas de los países, en este sentido, las redes sociales van a seguir siendo el principal vehículo para la materialización de tales ciber-amenazas.

10. De forma paralela a lo mencionado anteriormente, la "guerra cibernética", que tienen su origen en los propios Estados, en tanto estos ya han asumido que se trata de un nuevo escenario de operaciones militares, supondrá una escalada en cuanto a la dimensión de los ciberataques, obviamente motivada por los conflictos bélicos o entre Estados, aunque estos no necesariamente sean conflictos armados.

23 Para más información al respecto se recomienda el documento del NIST (National Institute of Standards and Technology, de los Estados Unidos) sobre "Adversarial Machine Learning A Taxonomy and Terminology of Attacks and Mitigations", disponible en https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf

2.3 Las prioridades de protección

1. Una de las cuestiones que va a cambiar de una manera más evidente, puesto que va a impactar directamente en los usuarios de los sistemas de información, es la adopción de sistemas de autenticación que no van a usar la tradicional combinación de usuario y contraseña, de tal manera que los sistemas multifactor y biométricos van a ser las soluciones más adoptadas, aunque en este último caso, puede generar tensiones en relación con las normas de privacidad.

2. Otra de las prioridades para tener en cuenta va a ser la aplicación de medidas específicas de protección de datos y privacidad, en este sentido, tanto la regulación como los estándares internacionales recogen esta cuestión[24], por supuesto, en ambos casos desde un enfoque de gestión de los riesgos.

3. La inteligencia artificial también va a tener un papel relevante en la propia proteccion de los activos de información, particularmente aplicada a la detección de ciber-amenazas.

4. Los avances propiciados por la inteligencia artificial, y su convergencia con otras tecnologías, está provocando sustanciales avances en las técnicas aplicadas a los "deepfake"[25], por tanto, será imprescindible que, especialmente en entornos críticos, se desarrollen e implementen medidas de detección de los "deepfakes".

5. Las infraestructuras de telecomunicaciones y los móviles, si bien han ido mejorando en materia de ciberseguridad, el estado del arte de su protección aun no es el adecuado[26], por tanto, la seguridad móvil es una prioridad, que incluye abordar las vulnerabilidades de la red 5G; en esta cuestión, las operadoras de las redes de telecomunicaciones deberán tener muy en cuenta los servicios que puedan llegar a utilizar tales redes, y adoptar las medidas necesarias para protegerlos, especialmente en el caso se servicios que puedan ser considerados de misión crítica.

6. La apuesta por los servicios en la nube que han hecho las organizaciones es clara, y ya no hay debate respecto de lo adecuado de su uso, pero la tendencia de disponer de infraestructuras hibridas (combinación de soluciones "cloud" y "on-premise"[27]), obliga a considerar como prioritaria la adopción de medidas de protección que tengan en cuenta la convivencia e integración de ambos entornos[28].

---

24 Por ejemplo, la ISO/IEC 27001:2022 ya no solo hace referencia a la gestión de la seguridad de la información, en su más reciente versión se hace mención expresa tanto a la ciberseguridad como a la privacidad *(ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements)*

25 Un deepfake es un vídeo o un audio que, mediante la manipulación adecuada, falsifica la apariencia de una persona, pudiendo incluir además su voz, con el fin de generar un contenido falso dotado de un alto realismo, y que puede inducir a engaño a las personas.

26 Se estima que durante el 2023 se publicó cada 23 segundos una aplicación maliciosa para sistemas Android.

27 Cuando las organizaciones mantienen infraestructuras TIC propias (software y hardware), de manera que su gestión no se deja por completo en manos de terceros, como si sucede en el caso de los servicios en la nube, que implican una evidente disminución del control directo sobre las infraestructuras y los servicios TIC.

28 Por ejemplo, la implementación de "firewalls" híbridos de malla permiten proteger entornos distribuidos; para más información https://www.checkpoint.com/es/cyber-hub/network-security/what-is-firewall/what-is-a-hybrid-mesh-firewall/

7. Relacionado con la prioridad anterior, se van a desplegar con fuerza las llamadas plataformas de protección de aplicaciones nativa de la nube (CNAPP)[29] , lo que conlleva un necesario rediseño de la seguridad de las aplicaciones.

8. Las diversas ciber-amenazas a que están expuestos los activos de información, va a requerir hacer foco en la gestión de la exposición a tales amenazas, pero no será suficiente tener en cuenta solo las amenazas comunes, habrá que identificar y analizar las amenazas específicas a que está expuesta cada organización y entrar el detalle de estas a fin de gestionar los riesgos reales que estas entrañan.

9. Desde un punto de vista de gobernanza de la ciberseguridad, se deberá recurrir a marcos organizativos que, a alto nivel, den respuesta a las necesidades de ciberseguridad de cada organización, fortaleciendo particularmente la supervisión de la ciber inseguridad que debe asumir la alta dirección.

10. Y, finalmente, habrá que continuar trabajando en afianzar una cultura de ciberseguridad que alcance a toda la organización; la formación en ciber-resiliencia para los empleados va a ser clave para disminuir los ciberincidentes que tienen un origen interno, lo que conllevará poner a los empleados en el centro de la estrategia de ciberseguridad.

29 Para más información Plataforma de protección de aplicaciones nativas en la nube - Palo Alto Networks

Capitulo 3

Estado de la ciberseguridad a nivel mundial

El propio contexto en el que se desarrollan las actividades relacionadas con la ciberseguridad, tanto desde la perspectiva de defensa como de ataque, hace que se disponga de mucha información sobre la incidencia que, a nivel global y local, tienen los ciber-incidentes, pero salvo algunos indicadores globales sobre ciberseguridad que podemos valorar como objetivos[30], las fuentes de información son muy dispersas, lo que obliga a que, para hacer un análisis lo más riguroso posible, se deban consultar el mayor número de fuentes posibles, aunque la fiabilidad de las mismas no siempre sea uniforme, ya que o bien están sesgadas por intereses comerciales o de ciber-activistas, o por la propia opacidad de las organizaciones que sufren incidentes de seguridad.

En todo caso, el análisis conjunto de todas esas fuentes, aunque con algunas imperfecciones, sí que nos permite obtener una visión del estado de la ciber inseguridad bastante cercano a la realidad; desde el punto de vista metodológico, para elaborar este informe se han seleccionado una cuarentena de fuentes de información, después de haber valorado más de 450 referencias que han publicado, desde diferentes perspectivas, datos que dan idea sobre el estado de la ciber inseguridad en el periodo 2022-2024.

Respecto de la cuestión de la opacidad por parte de las organizaciones que han sufrido ciber-incidentes, podemos decir que es un fenómeno o actitud que se ha visto muy suavizado por la incidencia de las normas jurídicas[31], ya que obligan a que las organizaciones sean transparentes en relación a los incidentes de seguridad que sufran sus ciber-activos de información, ya sea porque tales incidentes deban ser notificados las autoridades competentes, o incluso porque deban ser puestos en conocimiento de las personas cuyos datos se hayan podido ver afectados por brechas en la seguridad de los datos, o por el hecho de ser usuarios de determinados servicios digitales que se han visto impactados por ciberataques; además, en particular, las obligaciones de cooperación y coordinación que prevén las normas que regulan la ciberseguridad también hacen que aumente el nivel de transparencia y, por tanto, de conocimiento común sobre los ciber-incidentes.

30 MAPA | Mapa en tiempo real de amenazas cibernéticas Kaspersky

31 Particularmente las normas jurídicas que regulan la protección de los datos personales, la ciberseguridad y la protección de las infraestructuras críticas.

3.1 Algunos datos globales de relevancia

Tomar decisiones de ciberseguridad ya forma parte de las actividades ordinarias de la mayoría de las organizaciones públicas y privadas, obviamente unas decisiones que deben adaptarse a las circunstancias y características de cada organización y, sería además deseable que tales decisiones se adoptaran conociendo y teniendo en cuenta el riesgo que realmente suponen las ciber-amenazas para cada organización.

La cuestión descrita en el párrafo anterior es consecuencia directa del alto grado de dependencia del uso de las tecnologías y de la red que tienen las actividades de negocio, de modo que la protección de los datos confidenciales, incluyendo los datos personales, la preservación de la confianza de los clientes en los servicios digitales y garantizar la el acceso a los servicios y la continuidad del negocio.

Ya no son cuestiones exclusivamente estratégicas, sino plenamente operativas, de manera que constituyen objetivos y resultados primarios y críticos para las organizaciones, para cuya consecución es necesario destinar recursos económicos y contar con perfiles cualificados.

Las estadísticas sobre la ciber-inseguridad tienen muy diversos orígenes, y los criterios para establecer cuándo se ha sufrido un ataque, y si ese ataque ha tenido éxito y, por tanto, se ha convertido en un ciber-incidente con consecuencias, no son homogéneos, ya que no existe procedimiento específico para identificar esas situaciones, ni tampoco se dispone de información completa y exhaustiva de todas las potenciales fuentes de información[32], por tanto, siempre debemos tener en cuenta que estamos hablando de ordenes de magnitud, que nos dan idea de qué tipo de ataques son los que generan un mayor nivel de ciber-inseguridad, o cuál es su origen, sus efectos, las mejores prácticas, etc.

Por citar algunos datos a nivel global que nos sirven para conocer el contexto de la ciber-inseguridad y los riesgos a los que debemos enfrentarnos en el ciberespacio, podemos mencionar que:

- Los intentos de “phishing” mediante el uso de correo electrónico es el ciberataque más habitual[33], con cifras de se sitúan alrededor de 3.400 millones de correos electrónicos diarios con contenido malicioso; en los Estados Unidos este tipo de ataques ocupa el primer lugar entre los delitos cometidos, con más de 300.000 denuncias anuales, superando las pérdidas económicas totales por esta causa la cifra de los 10.300 millones de dólares[34]; hay que tener en cuenta que a su vez el phishing causa el 90% de las violaciones de la seguridad de los datos, siendo el origen de una buena parte de los ciber-incidentes de “ransomware”.
- En el año 2022, se detectaron a nivel mundial 493,33 millones de ataques de “ransomware”[35]; en el año 2023 se estima que se produjeron

32 O al menos no se puede contar con toda la información realmente disponible.

33 Informes sobre la incidencia del phishing señalan que una tercera parte de los empleados fallan los test “phishing”, ya que abrieron correos electrónicos sospechosos o siguieron enlaces engañosos; los sectores de mayor riesgo son educación, salud y seguros

34 Datos referidos al año 2022

35 El “ransomware” tienen como consecuencia que los datos o sistemas afectados quedan secuestrados por los atacantes (usualmente mediante técnicas de cifrado), hasta que se paga un rescate por ellos.

1,7 millones de ataques de “ransomware” diarios, y que a nivel mundial el 71% de las organizaciones fueron el objetivo de ataques de “ransomware”, en el año 2018 esta cifra representaba el 55,1%; por otro lado, el 60% de las empresas que sufren este tipo de ataques pagan el rescate para recuperar los datos[36].

- El sector sanitario ha sido el que ha tenido que soportar unos mayores costes a causa de los ciber-incidentes, ocupando desde el año 2010 el primer lugar en cuanto a costes derivados de tales incidentes; al coste económico hay que añadir otro tipo de consecuencias, ya que según un estudio realizado por el Ponemon Institute[37], los ciber-incidentes en los hospitales tienen como consecuencia el aumento de las tasas de mortalidad de sus pacientes.

- Los ataque de denegación de servicio distribuido (DDoS) tiene por objetivo interrumpir o afectar a la capacidad de los recursos y la infraestructura TIC atacada, provocando la caída o interrupción del servicio y, según el tipo de servicio afectado, ello puede suponer importantes pérdidas financieras, aunque la motivación económica no siempre es la única, por ejemplo, en marzo de 2023, el sitio web de la Asamblea Nacional Francesa sufrió un ataque de este tipo, realizado por ciber-atacantes rusos, que justificaron el ataque por el apoyo del gobierno francés a Ucrania[38].
- En el año 2023, se ejecutaron diariamente 300.000 instancias de software malicioso, el 92% fue distribuido mediante correo electrónico, y se tardó un promedio de 49 días en detectarlo; se trata de un software que puede tener muy diversos usos, todos ellos maliciosos, entre otros, obtener acceso no autorizado a los sistemas informáticos, la sustracción de datos, interrumpir servicios, o causar daños a las infraestructuras de telecomunicaciones y redes informáticas; según diferentes fuentes, desde el año 2018 los ataques basados en software malicioso ha ido creciendo constantemente.

36 Según el informe de 2021 de “State of the Phish”, de Proofpoint, Inc. Proofpoint
37 Cyberattacks against U.S. hospitals mean higher mortality rates, study finds (nbcnews.com)
38 Hackers prorrusos bloquean la web de la Asamblea Nacional francesa (lavanguardia.com)

- También el IoT (Internet de las Cosas) es objetivo de los ciber-atacantes, en este caso el ataque se dirige a dispositivos que están conectados a Internet, como por ejemplo un televisor inteligente o un dispositivo médico conectado a la red; cuantos más dispositivos están conectados a la red más crecen los ciber-ataques que pueden afectarles, en el año 2022 estos aumentaron un 87% respecto del años 2021, contabilizándose 112,3 millones de casos; por citar algún caso "famoso", en el 2022, se reveló que se podía aprovechar un fallo en el "TeslaMate"[39] para llegar a controlar a más de 25 vehículos en 13 países diferentes, de modo que se podía tener acceso remoto a diversas funcionalidades e informaciones de los vehículos (entre otras, desbloquear puertas, abrir y cerrar ventanas, comprobar la ubicación del automóvil, etc.)[40.]
- Por lo que respecta a los costes derivados de los ciber-incidentes, aunque su cuantificación no está exenta de dificultades, en el año 2022[41] el coste medio global de una violación de datos experimentó un aumento de 4,24 millones de dólares en 2021 a 4,35 millones de dólares en 2022, y en 2024 ese coste medio pasó a ser de 4,88 millones de dólares, habiendo aumentado un 10% respecto del año 2023; un dato a tener en cuenta es que el coste de los ciber-incidentes para las organizaciones que ya disponían de un despliegue relevante en relación al uso de la IA con fines de ciberseguridad, fue 3,05 millones de dólares menor que en otras organizaciones que no contaban con ese despliegue; por otro lado, cabe tener presente que el 43% de las pequeñas empresas son víctimas de ciber-ataques.
- Para el 2026 se estima que a nivel mundial el coste de los ciber-delitos superará los 20 trillones[42] de dólares.
- En cuanto a los costes que supone la ciberseguridad para las empresas, es evidente que este puede variar considerablemente de unas empresas a otras, en este sentido, tienen una especial relevancia características como el tamaño y sector de actividad de la empresa, el impacto que pueden tener los ciber-incidentes en la continuidad del negocio, la cultura de ciberseguridad, el nivel de transformación digital implementado, etc., en todo caso, según la "Deloitte Insights", las organizaciones dedican a la ciberseguridad alrededor de un 10,9% de su presupuesto de TI y, desde otro punto de vista, se dedica aproximadamente un 0,48% de los ingresos de las empresas a la ciberseguridad, o en términos de coste por empleado, la media es de unos 2.700 dólares por empleado; como dato adicional a tener en cuenta, según datos de Check Point Research, en el primer trimestre de 2024, los ciberataques aumentaron a nivel mundial un 28%.

39 "TeslaMate" es el software que recoge datos de actividad de los vehículos del fabricante Tesla.
40 ¿Robar un Tesla desde casa? Un hacker accede a varios coches y logra activar la herramienta 'Conducción sin llave' (20minutos.es)
41 Según información elaborada por IBM Coste de una filtración de datos 2024 | IBM
42 Un trillón es un millón de billones.

3.2 Las geo-cifras de ciberseguridad

Otro tipo de análisis que resulta de interés es el territorial, puesto que puede proporcionarnos información sobre países o zonas geográficas que concentran el mayor número de ataques o permite conocer el nivel de ciber inseguridad; en este estudio, por razones de extensión e interés del propio informe, el análisis de la información va a ser algo más detallado para la región de Europa y para la de América Latina y el Caribe, aunque no hemos de olvidar que hablar de ciber inseguridad es hablar de un fenómeno global.

A continuación, los datos relacionados con la ciber inseguridad se presentan agrupados geográficamente, siguiendo parcialmente el "geoesquema" de la ONU[43] y el del índice global de ciberseguridad de la UIT[44], que prevé a efectos estadísticos una clasificación basada en 5 territorios que, a su vez, se dividen en subregiones (en este informe se utilizarán solo algunas de ellas), si bien debe tenerse en cuenta que los datos de ciertos países pueden no ser fiables o estar incompletos, o incluso que no se disponga de información.

43 En este informe se agrupan geográficamente los datos usando parcialmente el geoesquema de la ONU, que a efectos estadísticos prevé cinco grandes territorios: África, América, Asia, Europa y Oceanía, cada uno de ellos divididos en subregiones, tal y como señala la ONU: *"La asignación de países o zonas a agrupaciones específicas es por conveniencia estadística y no implica ninguna suposición con respecto a la afiliación política o de otra índole de países o territorios por parte de las Naciones Unidas"*. Para más información consultar https://unstats.un.org/unsd/methodology/m49/

44 Unión Internacional de Telecomunicaciones UIT: Comprometida para conectar el mundo (itu.int)

Para elaborar este informe metodológicamente se han tenido en cuenta las siguientes fuentes de información:

- El Índice Nacional de Ciberseguridad (NCSI)[45]; para elaborar este índice se dispone de información consolidada del periodo 2016-2023, referida a 176[46] países, y tiene la particularidad de que mantiene un índice en tiempo real, si bien respecto de este índice solo se dispone de información de 53 países, lo que significa que en algunos casos hay países para los cuales este no ha sido calculado; el NCSI se centra en cuestiones que sean medibles y relevantes para valorar de qué manera los gobiernos de los países abordan la ciberseguridad, concretamente: legislación vigente; unidades establecidas (organización dedicada a la ciberseguridad); formatos de cooperación; y resultados (por ejemplo, políticas, ejercicios, tecnologías, sitios web, etc.); el estado de la ciberseguridad en un país puede ser variable, de ahí el interés que tiene disponer de un índice que se actualiza constantemente.
- El Índice Global de Ciberseguridad (GCI)[47] de la UIT; los datos utilizados en este informe se refieren al GCI del 2020, que se corresponde con su cuarta edición; está previsto que se publique la quinta edición a mediados de septiembre de 2024, la información se refiere a 194 Estados Miembros de la UIT[48]; el cuestionario[49] utilizado incluye 82 preguntas agrupadas en cinco áreas: medidas jurídicas; medidas técnicas; medidas organizativas; medidas de desarrollo de capacidades; y medidas de cooperación.
- Cuando corresponda, se han usado informes sobre ciberseguridad a nivel territorial o global, en particular de las autoridades que actúan en el ámbito de los ciberdelitos, por ejemplo, la INTERPOL, el FBI o EUROPOL, o de otras entidades y organizaciones que han publicado informes relacionados con la ciberdelincuencia y la ciberseguridad.

45 El proyecto NCSI (National Cyber Security Index) es propiedad y está desarrollado por la e-Governance Academy Foundation de Estonia, para más información NCSI :: Ranking (ega.ee); en relación a la metodología se explica que: *"El Índice Nacional de Seguridad Cibernética es un índice global en vivo, que mide la preparación de los países para prevenir amenazas cibernéticas y gestionar incidentes cibernéticos"*; además del NCSI, también se calcula el nivel de desarrollo digital (DDL); para información detallada sobre la metodología utilizada se puede consultar el siguiente documento NCSI-3.0_Methodology.pdf (ega.ee)

46 Además, en paralelo añaden al territorio de Kosovo.

47 El Global Cybersecurity Index (GCI) se empezó elaborar en el año 2015 por la Unión Internacional de Telecomunicaciones (UIT), organismo especializado de las Naciones Unidas para las TIC, y sirve para medir mediante un cuestionario enviado a los miembros de la UIT, el compromiso de los estados con la ciberseguridad a nivel global, con el fin de ayudar a identificar áreas de mejora; los aspectos metodológicos de este índice se pueden consultar en Publicaciones de la UIT (itu.int)

48

49 En aquellos casos en que los países no respondieron al cuestionario, se llevó a cabo una "investigación documental", usando para ello información disponible en los sitios web oficiales y en otros recursos documentales, tal y como indica la UIT en su informe: *"Para esos países, los datos recopilados quizá no se correspondan con exactitud con la postura de ciberseguridad del país".*

3.2.1 África[50]

La información recogida continuación se refiere a todo el continente africano, y dado el nivel de desarrollo global de la zona, la fuente más fiable y reciente de información en cuanto a ciber-amenazas, la encontraremos vinculada a los ciberdelitos[51], junto con la información derivada de los citados índices de ciberseguridad.

Según el NCSI, actualmente el país de África con el mejor índice de ciberseguridad es Marruecos (posición 20), y le siguen Túnez (22) y Ghana (23); teniendo en cuenta los datos consolidades de este índice (2016-2023), los 3 países con mejor índice de ciberseguridad serían Marruecos, Benín y Egipto, y los 3 países con peor índice serían Sudán del Sur, Togo y la República Democrática del Congo.

Según el GCI los 3 países con un mejor nivel de ciberseguridad en África son Mauricio (a nivel mundial ocupa la posición 17), Tanzania y Ghana, mientras que las 3 últimas posiciones corresponden Guinea Ecuatorial (ocupa la posición 180 a nivel mundial), Eritrea y Burundi[52], si bien los 2 países que obtienen peores resultados (Guinea Ecuatorial y Eritrea) no contestaron al cuestionario que sirve de base al ICG (debe recordarse que el índice ICG utilizado es el de 2020, y que hay uno nuevo previsto para este 2024).

Figura 02 → RESÚMENES ÍNDICES ÁFRICA

Fuente: Elaboración propia

África (ONU)				
NCSI actual	NCSI 2016-2023		GCI (2020)	
	Mayor nivel	Menor nivel	Mayor nivel	Menor nivel
Marruecos (20)	Marruecos	Sudán del Sur	Mauricio	Guinea Ecuatorial
Túnez (22)	Benín	Togo	Tanzania	Eritrea
Ghana (23)	Egipto	Rep. Democrática del Congo	Ghana	Burundi

Según el informe de INTERPOL de 2024, que evalúa las ciber-amenazas en África, las que más crecieron durante el 2023 fueron: el "ransomware", la estafa a empresas por correo electrónico y otras estafas a través de Internet; en su informe, la INTERPOL destaca que *"se siguen dando importantes retos en materia de prevención, detección, investigación y desarticulación de la ciberdelincuencia en toda África".*

Tal y como concluye el Foro Económico Mundial (WEF) *"la ciberseguridad en el continente africano sigue siendo un desafío y muchas empresas no están preparadas para los ataques cibernéticos"*[53], y a la vez esa "escasa ciberseguridad" tiene como consecuencia que sea un objetivo sencillo para los ciberdelincuentes, considerándolo el *"punto débil de las redes empresariales mundiales".*

50 Los países incluidos en esta zona geográfica son los identificados en geo-esquema de la ONU
51 "Informe de INTERPOL de evaluación de las ciberamenazas en África – 2024" disponible en https://www.interpol.int/es/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_SP%20v3.pdf
52 Por orden de peor índice de ciberseguridad.
53 África necesita mejorar la ciberseguridad para impulsar la inversión | Foro Económico Mundial (weforum.org)

3.2.2 Región de la Comunidad de Estados Independientes (CEI)[54]

Según el NCSI, actualmente el país de esta zona geográfica con el mejor índice de ciberseguridad es Azerbaiyán (posición 18), y teniendo en cuenta los datos consolidades de este índice (2016-2023), los 3 países con mejor índice de ciberseguridad serían Federación de Rusia, Azerbaiyán y Bielorrusia, y por lo que respecta a los 3 países con peor índice, serían Turkmenistán, Tayikistán y Armenia.

Según el GCI, los 3 países con un mejor nivel de ciberseguridad en esta región son Federación de Rusia (a nivel mundial ocupa la posición 5), Kazajstán y Azerbaiyán, mientras que las 3 últimas posiciones corresponden a Turkmenistán (a nivel mundial ocupa la posición 144), Tayikistán y Kirguistán, si bien Turkmenistán y Tayikistán no contestaron al cuestionario que sirve de base al ICG.

Figura 03 → RESÚMEN ÍNDICES CEI

Fuente: Elaboración propia

CEI (UIT)				
NCSI actual	NCSI 2016-2023		GCI (2020)	
	Mayor nivel	Menor nivel	Mayor nivel	Menor nivel
Azerbaiyán (18)	Federación de Rusia	Turkmenistán	Federación de Rusia	Turkmenistán
n/a	Azerbaiyán	Tayikistán	Kazajstán	Tayikistán
n/a	Bielorrusia	Armenia	Azerbaiyán	Kirguistán

De esta región no se dispone de datos suficientemente rigurosos, ni completos sobre el tipo de amenazas a los que están expuestos los países que forman parte; además se da la circunstancia de que la incidencia de la guerra entre Rusia y Ucrania hace que la situación sea excepcional, ya que muchos ciber-incidentes están relacionados con el conflicto geopolítico de carácter bélico, actualmente activo entre esos 2 países.

En general, la información que se publica indica que la Federación de Rusia es uno de los países que sufre más ciber-incidentes, pero a la vez también forma parte de los principales países desde los que se generan más amenazas relacionadas con los ciber-delitos[55], al respecto resulta de interés la consulta del primer índice mundial de ciberdelincuencia, publicado en abril de 2024, que clasifica a los países según el nivel de amenaza de ciberdelincuencia que generan.

54 Los países incluidos en este grupo son los identificados por la UIT en esta agrupación, que son: la Federación de Rusia, Kazajstán, Azerbaiyán, Uzbekistán, Bielorrusia, Armenia, Kirguistán, Tayikistán y Turkmenistán.

55 Según el "Índice Mundial de Ciberdelincuencia" publicado en abril de 2024 por cinco investigadores de la Universidad de Oxford (Reino Unido), Rusia lidera la lista de los países que generan un mayor volumen de amenazas que tienen su origen en la ciber-delincuencia, seguida de Ucrania, China, Estados Unidos, Nigeria, Rumanía, Corea del Norte, Reino Unido, Brasil y la India; informe disponible en https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312

3.2.3 Región de los Estados Árabes[56]

Según el NCSI, actualmente el país de esta zona geográfica con el mejor índice de ciberseguridad es Marruecos[57] (posición 20), y a continuación Túnez (posición 22) y Arabia Saudí (29); y teniendo en cuenta los datos consolidades de este índice (2016-2023), los 3 países con mejor índice de ciberseguridad serían Arabia Saudí, Marruecos y Qatar, y por lo que respecta a los 3 países con peor índice, serían Irak, Yemen y Libia.

Según el GCI, los 3 países con un mejor nivel de ciberseguridad en esta región serían Arabia Saudí, Emiratos Árabes Unidos, y Omán; y por lo que respecta a los 3 países con peor índice serían Yemen (sin datos), Yibuti y Comores (sin contestación al cuestionario de la UIT).

Figura 04 → RESÚMEN ÍNDICES REGIÓN ESTADOS ÁRABES

Fuente: Elaboración propia

REGIÓN DE LOS ESTADOS ÁRABES (UIT)				
NCSI actual	NCSI 2016-2023		GCI (2020)	
	Mayor nivel	Menor nivel	Mayor nivel	Menor nivel
Marruecos (20)	Arabia Saudí	Irak	Arabia Saudí	Yemen
Túnez (22)	Marruecos	Yemen	Emiratos Árabes	Yibuti
Arabia Saudí (29)	Qatar	Libia	Omán	Comores

Esta agrupación de países se caracteriza por diferencias significativas en sus indicadores económicos, lo que se traduce en una mayor o menor preparación de cara a enfrentarse a ciber-incidentes, teniendo en cuenta lo antedicho, destacan como países mejor preparados para afrontar las ciber-amenazas los Emiratos Árabes, Arabia Saudí, Qatar, Omán y Marruecos, además este último país destaca en el conjunto del continente africano.

Un aspecto relevante que debe destacarse es que, según informaciones publicadas por el Parlamento Europeo en el año 2022, prácticamente el 60% de los ciberataques en Oriente Medio incluían una componente de ingeniería social[58], siendo las principales ciber-amenazas el "ransomware" y la fuga de datos.

56 Los países incluidos en este grupo son los identificados por la UIT en esta agrupación ("Región de los Estados Árabes")
57 Marruecos también ha sido analizado por su pertenencia geográfica a África (según geo-esquema de la ONU), pero por su parte la UIT lo incluye en lo que denomina región de los Estados Árabes, de ahí que aparezca en ambos grupos
58 https://www.europarl.europa.eu/topics/es/article/20220120STO21428/ciberseguridad-amenanzas-principales-y-emergentes

3.2.4 Región de Asia y Pacífico[59]

Según el NCSI, actualmente el país de esta zona geográfica con el mejor índice de ciberseguridad es Australia (posición 4), seguida de China (28) y Nueva Zelanda (34), y teniendo en cuenta los datos consolidades de este índice (2016-2023), los 3 países con mejor índice de ciberseguridad serían Malasia, Singapur y la República de Corea; y por lo que respecta a los 3 países con peor índice, serían Palau, Estados Federales de Micronesia e Islas Marshall.

Según el GCI, en la región de Asia y el Pacífico, los 3 países con un mejor nivel de ciberseguridad en esta zona son la República de Corea (a nivel mundial ocupa la posición 4), Singapur y Malasia[60], mientras que las 3 últimas posiciones corresponden a la República Popular Demócrata de Corea (ocupa la posición 181 a nivel mundial), Maldivas y Timor-Leste, si bien estos 3 países no contestaron al cuestionario que sirve de base al ICG.

Figura 05 → RESÚMEN ÍNDICES REGIÓN DE ASIA Y PACÍFICO

Fuente: Elaboración propia

REGIÓN DE ASIA Y PACÍFICO (UIT)				
NCSI actual	NCSI 2016-2023		GCI (2020)	
	Mayor nivel	Menor nivel	Mayor nivel	Menor nivel
Australia (4)	Malasia	Palau	República de Corea	Rep. Popular Demócrata de Corea
China (28)	Singapur	Estados Federales de Micronesia	Singapur	Maldivas
Nueva Zelanda (34)	República de Corea	Islas Mashall	Malasia	Timor-Leste

En el año 2022 la región de Asia-Pacífico fue la región más atacada a nivel global, sufriendo el 31% de los ataques a nivel mundial; según diferentes informes la fuga de datos es una de las principales amenazas en esta zona, ya que cerca del 50% de los ciber-incidentes tuvieron como consecuencia el robo de información confidencial, considerado como tal los datos personales y la información confidencial de las empresas y gobiernos, por lo que podemos afirmar que el ciber-espionaje tienen una incidencia relevante en esta región.

El siguiente tipo de ciber-incidente de importancia fueron los que perseguían afectar a la disponibilidad en el acceso a infraestructura y datos, interrumpiendo las operaciones principales de las organizaciones; y en tercer lugar se situaría el "ransomware", en este caso, las principales víctimas son las empresas industriales, seguidas de las entidades del sector salud y del sector financiero.

En esta zona del mundo, la tendencia en el año 2023 fue de aumento de los ciberdelitos, incluso algunos analistas hacen referencia a que es la nueva "zona cero"[61] de los incidentes relacionados con la ciberdelincuencia.

59 Los países incluidos en este grupo son los identificados por la UIT en esta agrupación (Región de Asia-Pacífico)
60 Aunque en diferente orden, ambos índices del 2020 coinciden en situar a estos 3 países en las primeras posiciones del ranking de la región de Asia y el Pacífico de la UIT
61 https://www.weforum.org/agenda/2023/06/asia-pacific-region-the-new-ground-zero-cybercrime/

3.2.5 Estados Unidos de América y Canadá

Según el NCSI actualmente los Estados Unidos ocupa la posición 7, y Canadá la 9, y teniendo en cuenta los datos acumulados del NCSI, Canadá ocupa la posición 33, y los Estados Unidos la 46; en este caso, se da la circunstancia de que en el índice más reciente Estados Unidos está por encima de Canadá, no así en el acumulado de 2016 a 2023, que sería a la inversa.

A nivel mundial, según el GCI los Estados Unidos ocupa la posición 1 y Canadá la 13, ahora bien, ninguno de los 2 países contestó al cuestionario que sirve de base a este índice.

Según el informe elaborado por el "Internet Crime Complaint Center" (IC3)[62] del FBI[63], correspondiente al año 2023, los 3 principales ciberdelitos denunciados en los Estados Unidos, fueron: el "Phishing/Spoofing" (298.878 denuncias), los ciber-incidentes seguridad que afectaron a datos personales (55.851 denuncias) y la falta de pago o de entrega en compras en línea (50.523 denuncias); según el citado informe del IC3, los 3 estados con mayor número de denuncias presentadas fueron California (77.271), Texas (47.305) y Florida (41.061).

Según un informe de KPMG, de marzo de 2024[64] el "ransomware" y los ataques que comprometen los correos corporativos empresariales[65] fueron en el año 2023 las dos principales ciber-amenazas que afectaron a las empresas y organizaciones en Canadá.

62 2023_IC3Report.pdf
63 Internet Crime Complaint Center(IC3) | Home Page
64 Cyber incidents and intelligence: 2023 (kpmg.com)
65 "Business Email Compromise" (BEC)

3.2.6 América Latina y el Caribe[66]

Según el NCSI, actualmente el país de esta zona geográfica con el mejor índice de ciberseguridad es la República Dominicana (posición 21), seguida de Chile (25) y Uruguay (27), y teniendo en cuenta los datos consolidades de este índice (2016-2023), los 3 países con mejor índice de ciberseguridad serían República Dominicana, Paraguay y Argentina; y por lo que respecta a los 3 países con peor índice, serían Dominica, San Vicente y la Granadina y Haití.

Según el GCI, los 3 países con un mejor nivel de ciberseguridad en esta zona son Brasil (ocupa la posición 18 a nivel mundial), México y Uruguay, mientras que las 3 últimas posiciones corresponden a Honduras (ocupa la posición 178 a nivel mundial), Dominica y Haití, si bien Honduras no contestó al cuestionario que sirve de base al ICG.

Figura 05 → RESÚMEN ÍNDICES AMÉRICA LATINA Y EL CARIBE

Fuente: Elaboración propia

AMÉRICA LATINA Y EL CARIBE (ONU)				
NCSI actual	NCSI 2016-2023		GCI (2020)	
	Mayor nivel	Menor nivel	Mayor nivel	Menor nivel
Rep. Dominicana (21)	Rep. Dominicana	Dominica	Brasil	Honduras
Chile (25)	Paraguay	San Vicente y la Granadina	México	Dominica
Uruguay (27)	Argentina	Haití	Uruguay	Haití

La Organización de los Estados Americanos (OEA) ha estado haciendo foco sobre la ciberseguridad, en particular en relación con la ciberdelincuencia, paralelamente los países de esta zona han prestado especial atención a disponer de legislación relacionada con las ciber-amenazas, por ejemplo, Argentina, Costa Rica y Chile se han adherido a la Convención de Budapest sobre cibercrimen del Consejo de Europa[67], al igual que otros países, como México, Colombia y Paraguay.

Lo mismo puede decirse de la regulación en materia de protección de datos personales, que su desarrollo en la región ha tenido muy presente el Reglamento General de Protección de Datos de la Unión Europea (RGPD), asimismo también han servido de guía las directivas de ciberseguridad de la Unión Europa, conocidas como directivas NIS[68].

66 Los países incluidos en esta zona geográfica son los identificados en el geo-esquema de la ONU

67 Este Convenio tiene por objeto contribuir a la lucha contra los delitos cometidos usando tecnologías, así como los delitos en los que se ha utilizado la tecnología para facilitar o reforzar los efectos perjudiciales de otros delitos; el Convenio orienta a los países en el desarrollo de su legislación nacional sobre ciberdelincuencia https://eur-lex.europa.eu/ES/legal-content/summary/convention-on-cybercrime.html y

68 Directivas europeas NIS-1 y NIS-2, la segunda sustituye a la primera: Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión 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, por la que se modifican el Reglamento (UE) n. 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

En general, en América Latina y Caribe, las capacidades de los Estados para disponer de políticas de ciberseguridad eficaces todavía están en fase de construcción, dándose la circunstancia de que el nivel de madurez en desigual entre los diferentes países de la región, al respecto resulta de interés el análisis realizado en un artículo[69] del Real Instituto Elcano.

Según datos globales analizados por Kaspersky, entre junio de 2021 y julio de 2023, los ciberdelincuentes han mantenido en esta zona un nivel de actividad estable, si bien los ataques usando programas maliciosos ("malware") contra ordenadores y dispositivos móviles han experimentado un extraordinario aumento, concretamente un 617% para el caso de los ataques de "phishing" y un 50% de ataques de troyanos dirigidos a aplicaciones bancarias.

Los países más afectados por el "phishing" son, por este orden, Brasil, México, Perú, Colombia, Ecuador, Chile y Argentina; y por lo que respecta a los troyanos dirigidos a aplicaciones del sector bancario, Brasil y México se sitúan también en las 2 primeras posiciones, seguidos de Colombia, Perú, Ecuador, Argentina y Chile; como podemos apreciar las primeras 7 posiciones las ocupan los mismos países, si bien con algunas variaciones en cuanto a las posiciones que ocupan en relación a uno u otro tipo de ataque.

Por lo que respecta a ciber-incidentes que han afectado de manera importante a plataformas tecnológicas de servicios, los gobiernos de Panamá y Costa Rica fueron las principales víctimas entre el 2021 y 2022[70].

Otro indicador que resulta relevante para valorar el nivel de ciber-inseguridad, aunque esté vinculado no solo a datos objetivos, sino también a percepciones, es saber hasta que punto las personas, sean consumidores, usuarios o ciudadanos, perciben si se se sienten seguros cuando utilizan la redes, especialmente en relación con los potenciales fraudes en línea, sean relacionados con las transacciones bancarias en línea, o con las compras en internet.

Según un estudio[71], basado en una encuesta de Mastercard, dirigida a consumidores de varios países de la región, se puso en evidencia que un alto porcentaje de esas personas habían sufrido algún ciber-fraude: México (82%), Perú (81%), Argentina (76%), Chile (74%), Colombia (72%), República Dominicana (71%) y Costa Rica (70%).

Y, en lo que se refiere a percepciones, en el mismo estudio[72] se detectó que la confianza en relación con la ciberseguridad en el comercio en línea era en general baja o muy baja: Costa Rica (16%), Argentina (23%), República Dominicana (25%), Colombia (26%), Chile (27%), Perú (28%), México (36%) y Brasil (59%).

69 "El sector de ciberseguridad en América Latina: apuntes para leer un mapa del Estado en construcción" de Jorge M. Vega, doctor en Seguridad Internacional. Docente e investigador en Derecho y Seguridad Internacional en la Universidad del Salvador (USAL), disponible en https://www.realinstitutoelcano.org/analisis/el-sector-de-ciberseguridad-en-america-latina-apuntes-para-leer-un-mapa-del-estado-en-construccion/

70 https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content

71 https://www.mastercard.com/news/media/xpuetfcn/security-barometer-report_if_report-visual.pdf

72 Se preguntaba: ¿Hasta qué punto confía en que los comerciantes en línea mantienen sus datos personales seguros en sus sistemas?

3.2.7 Región de Europa[73]

Según el NCSI, actualmente el país de esta zona geográfica con el mejor índice de ciberseguridad es la República Checa (posición 1), seguida de Polonia (2) y Bélgica (3), y teniendo en cuenta los datos consolidades de este índice (2016-2023), los 3 países con mejor índice de ciberseguridad serían Bélgica, Lituania y Estonia; y por lo que respecta a los 3 países con peor índice, serían Ciudad Vaticano, San Marino y Bosnia y Herzegovina.

Según el GCI, los 3 países con un mejor nivel de ciberseguridad en esta zona son Reino Unido (ocupa posición 2 a nivel mundial), Estonia y España, mientras que las 3 últimas posiciones corresponden a San Marino (ocupa la posición 146 a nivel mundial), Andorra y Bosnia y Herzegovina, si bien Andorra no contestó al cuestionario que sirve de base al ICG.

Figura 06 → RESÚMEN ÍNDICES REGIÓN DE EUROPA

Fuente: Elaboración propia

REGIÓN DE EUROPA (UIT)				
NCSI actual	NCSI 2016-2023		GCI (2020)	
	Mayor nivel	Menor nivel	Mayor nivel	Menor nivel
República Checa (1)	Bélgica	Ciudad Vaticano	Reino Unido	San Marino
Polonia (2)	Lituania	San Marino	Estonia	Andorra
Bélgica (3)	Estonia	Bosnia y Herzegovina	España	Bosnia y Herzegovina

En Europa, las instituciones de la Unión Europea hacen un especial foco sobre la ciber-inseguridad a la que están expuestos los ciudadanos y las empresas europeas, se parte de la base de que existen ciertos sectores que son críticos, concretamente el transporte, la energía, la sanidad y las finanzas, tienen una alta dependencia de las TIC para desplegar sus actividades.

Además, las instituciones europeas disponen de indicadores que ponen en evidencia que los ciberataques y la ciberdelincuencia van en aumento y son más sofisticados, y que esta situación se agravará por la previsión de que 41.000 millones de dispositivos en todo el mundo estarán conectados a la red (Internet de las cosas) en el 2025.

La creación hace ya dos décadas[74] de ENISA[75], con el fin de "velar por un alto nivel común de ciberseguridad en toda Europa", fue una decisión que ponía en evidencia la importancia que a la ciberseguridad se daba en Europa, y es una pieza clave en el desarrollo de las políticas europeas en esta materia.

73 Los países incluidos en este grupo son los identificados por la UIT en esta agrupación (Región de Europa)

74 ENISA se creó en el año 2004 como Agencia de Seguridad de las Redes y de la Información de la Unión Europea, posteriormente se reforzaron sus funciones, y paso a denominarse Agencia de la Unión Europea para la Ciberseguridad, en el año 2019, mediante el Reglamento sobre la Ciberseguridad de la Unión Europea, disponible https://eur-lex.europa.eu/ES/legal-content/summary/the-eu-cybersecurity-act.html. La agencia mantiene el acrónimo de cuando fue creada en el año 2004.

75 https://www.enisa.europa.eu/about-enisa/about/es

ENISA coopera con los Estados miembros y con los organismos de la UE, en la gestión de las ciber-amenazas, mediante “el intercambio de conocimientos, la creación de capacidades y la sensibilización”, persiguiendo como objetivos, reforzar la confianza en la economía digital, impulsar la resiliencia de las infraestructuras y proteger a la sociedad y a la ciudadanía europea de la ciber-inseguridad.

Uno de los aspectos claves en el modo en que se aborda la ciberseguridad es que cada estado miembro de la Unión Europea cuenta una “estrategia nacional de ciberseguridad”, en la que se establecen “los objetivos estratégicos, los recursos necesarios para alcanzar esos objetivos y las medidas políticas y normativas adecuadas con objeto de alcanzar y mantener un elevado nivel de ciberseguridad”, para hacernos una idea de su alcance, se hace referencia[76] de manera específica, por ejemplo, a que los Estados miembros deberán desarrollar, formando parte de su estrategia nacional de ciberseguridad, una política que aborde el despliegue de tecnología en las ciudades inteligentes y sus posibles efectos en la sociedad, o que deberá tenerse en cuenta en la citada estrategia, la ciberseguridad de los cables de comunicaciones submarinos.

76 En 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, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

En Europa, la regulación sobre la ciberseguridad es un pilar básico, a partir del cual se articula un elevado nivel común de ciberseguridad en toda la Unión Europea.

El planteamiento de la Unión Europea en materia de ciberseguridad además obedece también al convencimiento de que las "tensiones geopolíticas aumentan los riesgos cibernéticos, mientras que los ciberataques exacerban la dinámica geopolítica", tal y como ha expresado el World Economic Forum (WEF)[77].

Según datos proporcionados por Google[78], a los que hace referencia el WEF, en el año 2023 habían aumentado los ciberataques en que los Estados participaban activamente, cifrando ese aumento de ataques a usuarios de países de la OTAN en un 300%[79], respecto del año 2020, de ahí la necesidad de que, en un contexto geopolítico inestable, sea prioritario reforzar la ciber-resiliencia de las infraestructuras y de las cadenas de suministros.

77 https://es.weforum.org/agenda/2023/03/ciberseguridad-en-la-era-de-la-policrisis/
78 https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
79 Según el WEF: *"En febrero de 2022, el proveedor de comunicaciones por satélite Viasat fue atacado, provocando cortes en toda Europa horas antes de que Rusia lanzara su invasión. Aunque el objetivo principal era el ejército ucraniano, el ataque también afectó a los servicios de Internet de decenas de miles de personas en toda Europa y desconectó el acceso remoto a unas 5800 turbinas eólicas en toda Alemania."*

Capítulo 4

Conclusiones

Aunque a lo largo de este informe ya se hace referencia a algunas conclusiones y recomendaciones, conviene centrar algunas cuestiones que se derivan de los datos e informaciones utilizados en el análisis realizado en este documento, y que se resumen en los siguientes 10 puntos:

La ciber-inseguridad es una realidad y hay que afrontarla, ya que va unida al desarrollo y uso de los medios digitales tanto a nivel empresarial como particular.

Las predicciones en materia de ciber-inseguridad son cada vez más acertadas, por tanto, deberán ser tenidas muy en cuenta por los directivos de ciberseguridad, que van a tener que asumir responsabilidades complejas, que aunaran aspectos y criterios técnicos, organizativos y jurídicos.

Los ciber-ataques van a seguir aumentado, tanto en número como en la gravedad de sus consecuencias, por tanto, hay que adoptar medidas técnicas y organizativas para enfrentarse a ellos, siendo el enfoque a riesgos el más efectivo.

El uso de marcos de ciberseguridad y los estándares que proponen las mejores prácticas en ciberseguridad, van a ser el campamento base para definir las estrategias de defensa para la contención de los ciber-atacantes.

Las normas jurídicas que obligan a tomar decisiones en materia de ciberseguridad no deben ser considerada barreras, hay que usarlas como aliadas, ya que no pretenden otra cosa que reforzar la ciber-resiliencia de las organizaciones.

El ciberespacio forma parte de la realidad, los conflictos entre personas y entre estados se desarrollan simultáneamente en escenarios virtuales y presenciales, que están conectados como nunca, eso incluye la necesidad de proteger las infraestructuras digitales y la protección de las cadenas de suministro mundiales.

La ciber-inseguridad es un fenómeno global, pero las capacidades de ciberseguridad mundial son desiguales, hay grandes diferencias entre países, y los eslabones más débiles de la cadena se detectan con facilidad por parte de los ciber atacantes que se centran donde es más probable que los ciberataques tengan éxito.

Cualquier organización, de cualquier sector y de cualquier tamaño o volumen de negocio, está expuesta a las mismas ciber-amenazas, pero no todas disponen de los mismos medios para defenderse, esta es una brecha que debe ser abordada desde las instancias públicas.

Extender la cultura de ciberseguridad es esencial para evitar los ciberataques en los que una parte del ataque depende precisamente del conocimiento de las personas, de ahí que estas deban disponer de recursos formativos adecuados en esta materia, de ellos depende una buena parte del éxito de las decisiones en materia de ciberseguridad.

Y, finalmente, la inteligencia artificial realmente no va a suponer ningún cambio en el actual equilibrio de fuerzas, formará parte de las herramientas de los ciber-atacantes y de los ciber-defensores, pero no generará un desequilibrio sustancial hacía uno u otro lado.

Referencias bibliográficas

1. Akamai. (2024). *¿Qué es la ciberresiliencia?* | Akamai. → IR A ENLACE

2. Check Point. (2024). *¿Qué es un ataque multivectorial?* - Software Check Point. → IR A ENLACE

3. IBM. (2024). *Coste de una filtración de datos 2024.* → IR A ENLACE

4. INTERPOL. (2024). *Informe de evaluación de las ciberamenazas en África – 2024.* → IR A ENLACE

5. National Institute of Standards and Technology (NIST). (2023). *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations.* → IR A ENLACE

6. Universidad de Oxford. (2024). *Índice Mundial de Ciberdelincuencia.* → IR A ENLACE

7. Vega, J. M. (2024). *El sector de ciberseguridad en América Latina: apuntes para leer un mapa del Estado en construcción.* Real Instituto Elcano. → IR A ENLACE

8. World Economic Forum. (2024). *The Global Risks Report 2024* (p. 5). → IR A ENLACE

9. Unión Europea. (2022). *Ley de Ciberresiliencia de la UE.* → IR A ENLACE

Anexo

Actualización con datos de la 5ª edición del "Global Cybersecurity Index"

Nota del autor: en el informe se han utilizado datos de la cuarta edición del Global Cybersecurity Index (2020); tal y como se indica en el propio informe, estaba prevista la publicación de la 5ª edición para mediados de septiembre de 2024, concretamente este se publicó el pasado 12 de septiembre de 2024, una vez el informe ya estaba preparado para su publicación, de modo que este anexo tiene como finalidad completar el informe los datos más relevantes que aporta la última edición del GCI.

El informe en el que se establece el índice global de ciberseguridad es elaborado por la UIT (Unión Internacional de Telecomunicaciones), organismo especializado de Naciones Unidades para las tecnologías de la información y la comunicación, que está integrado por 194 Estados y más de 1000 empresas, universidades y organizaciones internacionales y regionales, tienen su sede central en Ginebra (Suiza) y cuenta con oficinas regionales en todos los continentes.

El objetivo del informe, que se centra en establecer lo que se conoce como "Global Cybersecurity Index" (GCI)[1], es evaluar el estado y el progreso a nivel mundial de la ciberseguridad; la UIT en su nota de prensa[2] de presentación del informe, señala como principal conclusión del mismo, que los países están reforzándose en materia de ciberseguridad, y han mejorado respecto del anterior GCI, pero resalta que hay que seguir intensificando y mejorando las medidas adoptadas por los Estados.

Hay ciertas amenazas que mantienen su presión, como los ataques de ransomware, especialmente los que afectan a los gobiernos, pero también los ciberataques a las infraestructuras industriales, a lo que se unen altos costes derivados de las interrupciones de los sistemas y, por supuesto, se mantiene un alto nivel de incidencia de las brechas de la seguridad de datos personales y de las informaciones de las organizaciones.

En el informe de 2024, se ha mantenido como metodología de análisis la evaluación de los esfuerzos que hacen los países en los cinco pilares ya evaluados en anteriores informes: jurídico, técnico, organizativo, desarrollo de capacidades y cooperación, pero se ha modificado el modo en que se ha clasificado a los países, pasándose a ubicar a estos entre 5 niveles (Tier 1 a 5).

1 Disponible en https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

2 https://www.itu.int/en/mediacentre/Pages/PR-2024-09-10-Global-Cybersecurity-Index.aspx

Se trata de un informe en el que se lleva a cabo una evaluación de las acciones que los países han llevado a cabo para mejorar su ciberseguridad y hay que subrayar que, los marcos jurídicos o medidas legales se evidencian como el pilar más sólido de la ciberseguridad, ya que 177 países del total de los que han sido objeto de análisis, tienen al menos una regulación sobre la protección de datos personales o la protección de la privacidad; asimismo, la existencia de Equipos de Respuesta a Incidentes Informáticos (CIRT, por sus siglas en inglés) sería el segundo aspecto en el que más países han tomado la decisión de crearlos, en total 139 tienen al menos un CIRT activo.

En el nivel 1, el informe sitúa a los países que se consideran que son "modelos a seguir", es decir, los que han alcanzado un desarrollo más avanzado en ciberseguridad (teniendo en cuenta el análisis de los pilares ya citados); en total hay 46 países en este nivel.

NIVEL 1 - MODELOS A SEGUIR (PUNTACIONES DE 95 A 100)			
Australia	Ghana	Morocco	Slovenia
Bahrain	Greece	Netherlands (Kingdom of the)	Spain
Bangladesh	Iceland	Norway	Sweden
Belgium	India	Oman	Tanzania
Brazil	Indonesia	Pakistan	Türkiye
Cyprus	Italy	Portugal	United Arab Emirates
Denmark	Japan	Qatar	United Kingdom
Egypt	Jordan	Korea (Republic of)	United States
Estonia	Kenya	Rwanda	Viet Nam
Finland	Luxembourg	Saudi Arabia	
France	Malaysia	Serbia	
Germany	Mauritius	Singapore	

Fuente: Global Cybersecurity Index 2024 de la International Telecommunication Union (ITU)

En el nivel 2, hay 29 países que se consideran que están “avanzando” en materia de ciberseguridad.

NIVEL 2 - AVANZANDO (PUNTACIONES DE 85 A 95)			
Albania	Ecuador	Mexico	Switzerland
Austria	Georgia	Philippines	Togo
Azerbaijan	Hungary	Poland	Uruguay
Benin	Ireland	Romania	Uzbekistan
Canada	Israel	Russian Federation	Zambia
China	Kazakhstan	Slovakia	
Croatia	Lithuania	South Africa	
Czech Republic	Malta	Sri Lanka	

Fuente: Global Cybersecurity Index 2024 de la International Telecommunication Union (ITU)

En el nivel 3, hay 49 países que están “estableciendo” sus pilares de ciberseguridad, sería equivalente a un nivel medio de ciberseguridad.

NIVEL 3 - ESTABLECIENDO (PUNTACIONES DE 55 A 85)			
Algeria	Cuba	Libya	Papua New Guinea
Andorra	Dem. Rep. of the Congo	Malawi	Paraguay
Belarus	Dominican Rep.	Moldova	Peru
Bhutan	Eswatini	Monaco	Senegal
Botswana	Ethiopia	Mongolia	Sierra Leone
Brunei Darussalam	Gambia	Montenegro	Trinidad and Tobago
Bulgaria	Guinea	Mozambique	Tunisia
Burkina Faso	Iran (Islamic Republic of)	Myanmar	Uganda
Cameroon	Jamaica	Nepal (Republic of)	Ukraine
Chile	Kiribati	New Zealand	Vanuatu
Colombia	Kuwait	Nigeria	
Costa Rica	Kyrgyzstan	North Macedonia	
Côte d'Ivoire	Latvia	Panama	

Fuente: Global Cybersecurity Index 2024 de la International Telecommunication Union (ITU)

En el nivel 4, hay 56 países “en evolución”, se entiende que existe ya una base mínima a partir de la se pueden a ir mejorando las capacidades de ciberseguridad.

NIVEL 4 - EN EVOLUCIÓN (PUNTACIONES DE 20 A 55)			
Angola	El Salvador	Madagascar	South Sudan
Argentina	Equatorial Guinea	Mali	State of Palestine
Armenia	Fiji	Mauritania	Sudan
Bahamas	Gabon	Namibia	Suriname
Barbados	Grenada	Nauru	Syrian Arab Republic
Belize	Guatemala	Nicaragua	Tajikistan
Bolivia (Plurinational State of)	Guyana	Niger	Tonga
Bosnia and Herzegovina	Haiti	Saint Kitts and Nevis	Turkmenistan
Cabo Verde	Honduras	Saint Lucia	Tuvalu
Cambodia	Iraq	Saint Vincent and the Grenadines	Venezuela
Chad	Lao P.D.R.	Samoa	Zimbabwe
Comoros	Lebanon	San Marino	
Congo (Rep. of the)	Lesotho	Sao Tome and Principe	
Djibouti	Liberia	Seychelles	
Dominica	Liechtenstein	Somalia	

Fuente: Global Cybersecurity Index 2024 de la International Telecommunication Union (ITU)

Y finalmente, en el nivel 5, hay 14 países que todavía están “construyendo” sus instrumentos de ciberseguridad.

NIVEL 5 - CONSTRUYENDO (PUNTACIONES DE 0 A 20)			
Afghanistan	Dem. People's Rep. of Korea	Marshall Islands	Vatican
Antigua and Barbuda	Eritrea	Micronesia	Yemen
Burundi	Guinea-Bissau	Solomon Islands	
Central African Rep.	Maldives	Timor-Leste	

Fuente: Global Cybersecurity Index 2024 de la International Telecommunication Union (ITU)

El GCI 2024 pone en evidencia que la región de África es la que más ha mejorado desde el anterior índice, si bien se ha detectado que todas las regiones del mundo han experimentado mejoras en materia de ciberseguridad desde el 2020.

En la región de Sudamérica, se ha avanzado significativamente en la implementación de marcos legales y técnicos, pero aún debe mejorar en lo que respecta al desarrollo de capacidades en materia de ciberseguridad y en la cooperación, siendo este un elemento clave para afrontar las ciber-amenazas globales; según el informe, Brasil y Chile destacan por su progreso en medidas organizativas y su participación en iniciativas de cooperación internacional.

El análisis de las “desarrollo de capacidades” se sustenta en la existencia de programas de investigación y desarrollo, educación y capacitación en materia de ciberseguridad, y de entidades del sector público que los fomenten; mientras que la “cooperación” se refiere a la existencia en el país de asociaciones, marcos de cooperación y redes de intercambio de información, tanto de carácter local como internacional

Por lo que respecta a España, obtiene la puntuación máxima en 4 de los 5 pilares analizados, ubicándose en el nivel 1, con una valoración de su GCI que está por encima de la media de los países de la Unión Europea.

OBS Business School

School of **Business Administration & Leadership**

School of **Innovation & Technology Management**

Planeta Formación y Universidades