OBS Business School

Transformación Digital y Ciberseguridad: binomio inseparable

Ramón Miralles López

Profesor de OBS Business School

Noviembre, 2023

Partners Académicos:

Universitat de Barcelona

unie Universidad

OBSbusiness.school

Autor

Ramón Miralles López
*Colaborador 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 35 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, actualmente es socio director en una consultora jurídica especializada en derecho digital.

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).

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 especialmente 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, concretamente 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 **5**

Capítulo 2 Transformación digital: de dónde venimos, donde estamos y hacía donde vamos **7**

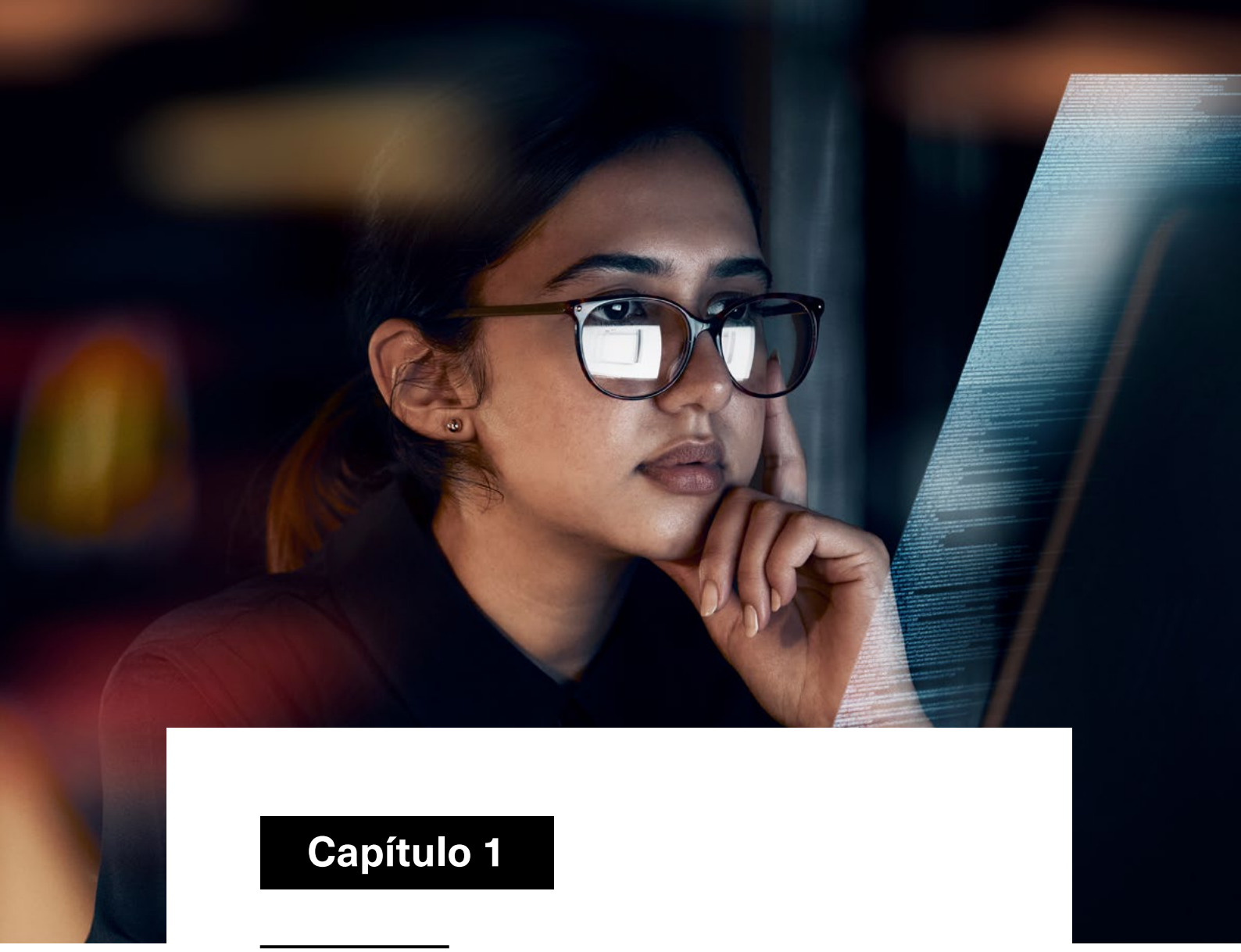
Capítulo 3 Contextualizando la Ciberseguridad y su vínculo inseparable con la transformación digital **13**

Capítulo 4 Las exigencias jurídicas: innovación y regulación **21**

Capítulo 5 Estado de la regulación de la ciberseguridad a nivel mundial **27**

Capítulo 6 Conclusiones y recomendaciones **30**

Referencias bibliográficas **33**



Capítulo 1

Introducción

Con prácticamente una cuarta parte del siglo XXI consumida, explicar el significado e implicaciones de la irrupción de las tecnologías de la información y la comunicación (TIC) en el ámbito empresarial y personal resulta más complejo de lo que lo fue hasta finales de los 90.

La transformación digital trasciende el simple uso de las TIC. Tampoco se centra exclusivamente en nuevos perfiles profesionales, cambios en procesos y métodos de trabajo por las TIC o en su impacto en los negocios y las relaciones con clientes. Es todo eso y mucho más. Podríamos decir que la transformación digital es, en esencia, una actitud y aptitud de las organizaciones y sus integrantes para adaptarse a la rápida evolución tecnológica.

En este informe vamos a centrarnos en las organizaciones, más concretamente en las empresas[1]. La actitud tiene que ver con cómo afrontan la evolución tecnológica y las decisiones para aprovechar al máximo las tecnologías digitales. La aptitud es la capacidad para tomar tales decisiones intelectualmente y en cuanto a recursos, teniendo en cuenta que la transformación digital es disruptiva y busca cambios radicales.

De nada sirve tener una buena actitud frente a un reto, si no se acompaña de una adecuada aptitud para afrontarlo o llevarlo a cabo, porque hoy por hoy, la transformación digital, también es un reto, y no aceptarlo puede significar a medio plazo, o incluso a corto, que una organización deje de ser competitiva, viéndose superada por los "acontecimientos" tecnológicos.

Un claro ejemplo es la explosiva irrupción de la inteligencia artificial, con grandes posibilidades pero también extraordinarios riesgos internos y externos, sobre la que hay que tomar decisiones para su incorporación en las organizaciones.

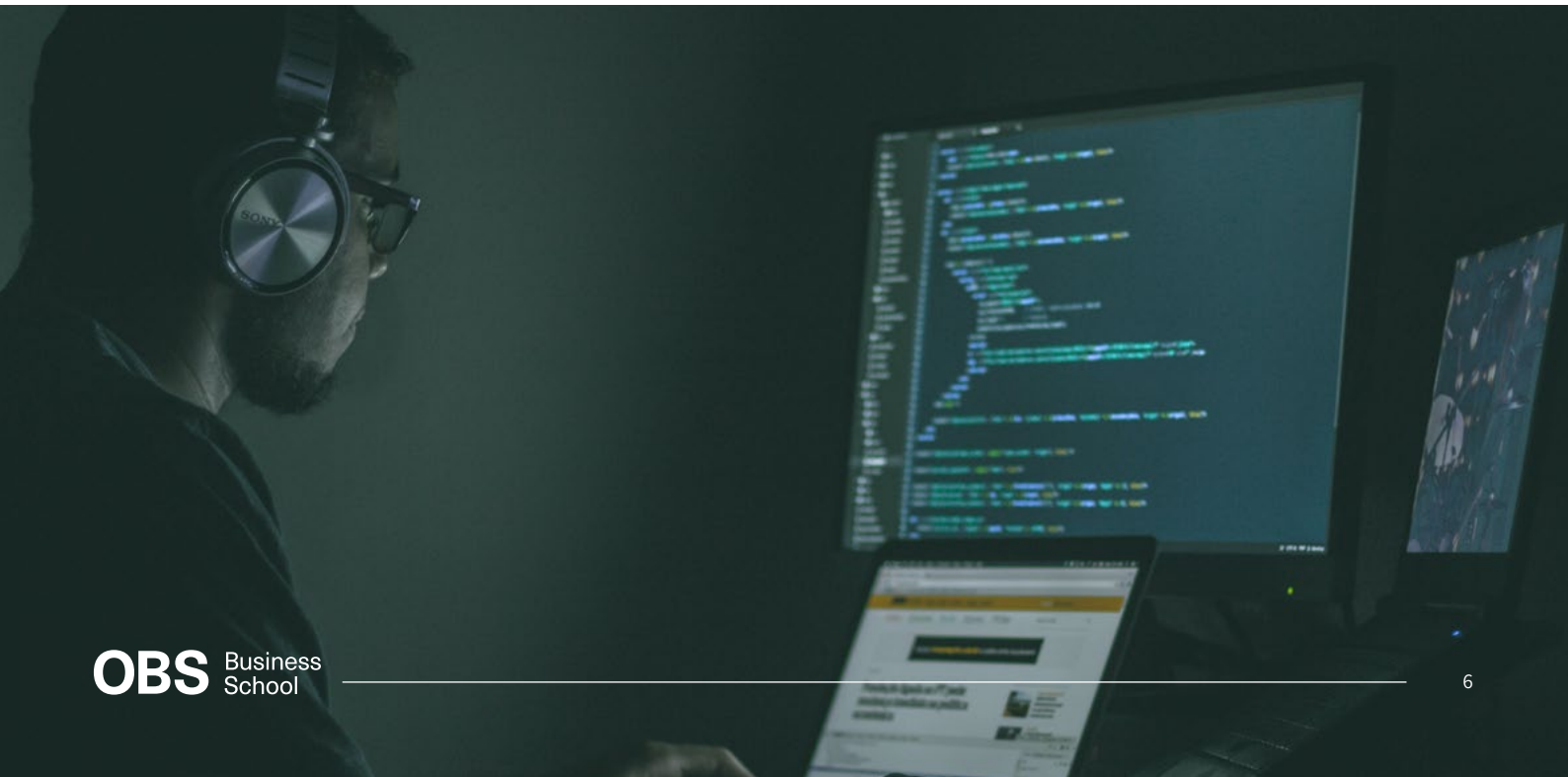
Este informe plantea la necesidad de escenarios de transformación digital seguros, afrontando eficazmente sus riesgos tecnológicos. No podemos lograr la transformación digital sin priorizar que información, procesos y personas cumplan sus funciones en un entorno seguro, en particular respecto a la ciberseguridad, sin olvidar la presión legal al respecto.

El proceso de transformación digital que no vaya acompañado de decisiones en materia de ciberseguridad estará abocado al fracaso, ya que el uso extensivo e intensivo de tecnologías que implica, genera amenazas ante las que podemos ser vulnerables si no estamos preparados. De ahí la inseparabilidad entre transformación digital y ciberseguridad.[2]

---

[1] Para profundizar el proceso de transformación digital de las administraciones públicas en España, es de interés el documento de trabajo "La digitalización en las administraciones públicas en España", de Lorenzo Cotino, Catedrático de Derecho Constitucional de la Universidad de Valencia, publicado por la Fundación Alternativas https://fundacionalternativas.org/wp-content/uploads/2023/10/DIGITALIZACION_ADMIN_PUBLICAS.pdf

[2] Como ejemplo la reciente consulta (septiembre 2023) planteada el Gobierno español para impulsar la transformación digital y ciberseguridad de los medios de comunicación https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/asuntos-economicos/Paginas/2023/130923-transformacion-digital.aspx



Capítulo 2

Transformación digital: de dónde venimos, donde estamos y hacía donde vamos

El concepto de transformación digital está unido al de "Industria 4.0". Podemos hablar de una relación causa-efecto: la "Industria 4.0" explica por qué ahora hablamos de transformación digital.

El concepto de "Industria 4.0" se generalizó a partir de la obra[3] "La Cuarta Revolución Industrial"[4] (2016) del economista Klaus Schwab, fundador del Foro Económico Mundial[5], donde afirma que: *"La Cuarta Revolución Industrial genera un mundo en el que los sistemas de fabricación virtuales y físicos cooperan entre sí de una manera flexible a nivel global. Sin embargo, no consiste solo en sistemas inteligentes y conectados. Su alcance es más amplio y va desde la secuenciación genética hasta la nanotecnología, y de las energías renovables a la computación cuántica. Es la fusión de estas tecnologías y su interacción a través de los dominios físicos, digitales y biológicos lo que hace que la Cuarta Revolución Industrial sea diferente a las anteriores"*.

Hablar de transformación digital es hablar de progreso, que es *"avanzar, mejorar, hacer adelantos en determinada materia"*, y por tanto, cabe preguntarse si realmente hemos progresado como sociedad en las últimas décadas apoyándonos en las tecnologías digitales.

Obviamente la respuesta varía según el contexto geo-político o país analizado, variará si nos enfocamos en las personas y la brecha digital, o si lo analizamos desde la perspectiva de los servicios públicos, de los negocios y servicios digitales, o si lo que queremos tener en cuenta es la perspectiva económica. Las perspectivas son múltiples e inabarcables para este estudio[6], que analiza transformación digital y ciberseguridad como binomio inseparable

Pero conviene disponer de contexto para evidenciar los avances más significativos en lo que llevamos de siglo XXI, algunos iniciados en la década de 1990.

Un elemento clave es la conectividad. Así, en España a principios del siglo XXI, concretamente en el año 2003, existía conexión a internet en algo más del 25% de los domicilios[7], mientras que la media en Europa en el mismo año, ese porcentaje superaba el 40%; en el 2022 en España ese porcentaje pasó a ser del 96,1%, un porcentaje algo superior a la media europea.

En América Latina y el Caribe (LAC), en el 2022, dos terceras partes de los domicilios tenían conexiones fijas a internet, es decir, por debajo del 70%, aunque debe tenerse en cuenta que existen desviaciones importantes entre países de la zona; en todo caso, antes de la pandemia ese porcentaje era casi del 50%[8], por lo que se detecta un avance significativo de este indicador.

---

[3] "La cuarta revolución industrial" Schwab, Klaus; ISBN: 9788499926940, Editorial Debate, fecha y lugar de edición: 2016 en Barcelona. España

[4] Se hace referencia a una "cuarta revolución industrial" teniendo como antecedentes la existencia de 3 revoluciones industriales previas: la primera, que se sitúa a finales del siglo XVIII, caracterizada por la aplicación del vapor a la producción mecánica; la segunda revolución industrial, un siglo después de la primera, que se centra en la producción masiva de bienes, sustentada en la energía eléctrica; y la tercera, que se inicia a finales de los años sesenta del siglo pasado, con la informática, que permitió una progresiva automatización de todo tipo de procesos y se empieza a hablar de "sociedad de la información".

[5] Fundada en 1971 como organización sin fines de lucro, centrada en la cooperación mundial, que aglutina a nivel mundial a empresas, intelectuales y políticos https://es.weforum.org/

[6] Para profundizar en esta cuestión en lo que se refiere a España recomiendo la lectura del informe "Impacto de la transformación digital en España: 1998-2023", publicado por la Fundación Orange en junio de 2023, disponible en https://fundacionorange.es/25a/informe/Informe-25a.pdf

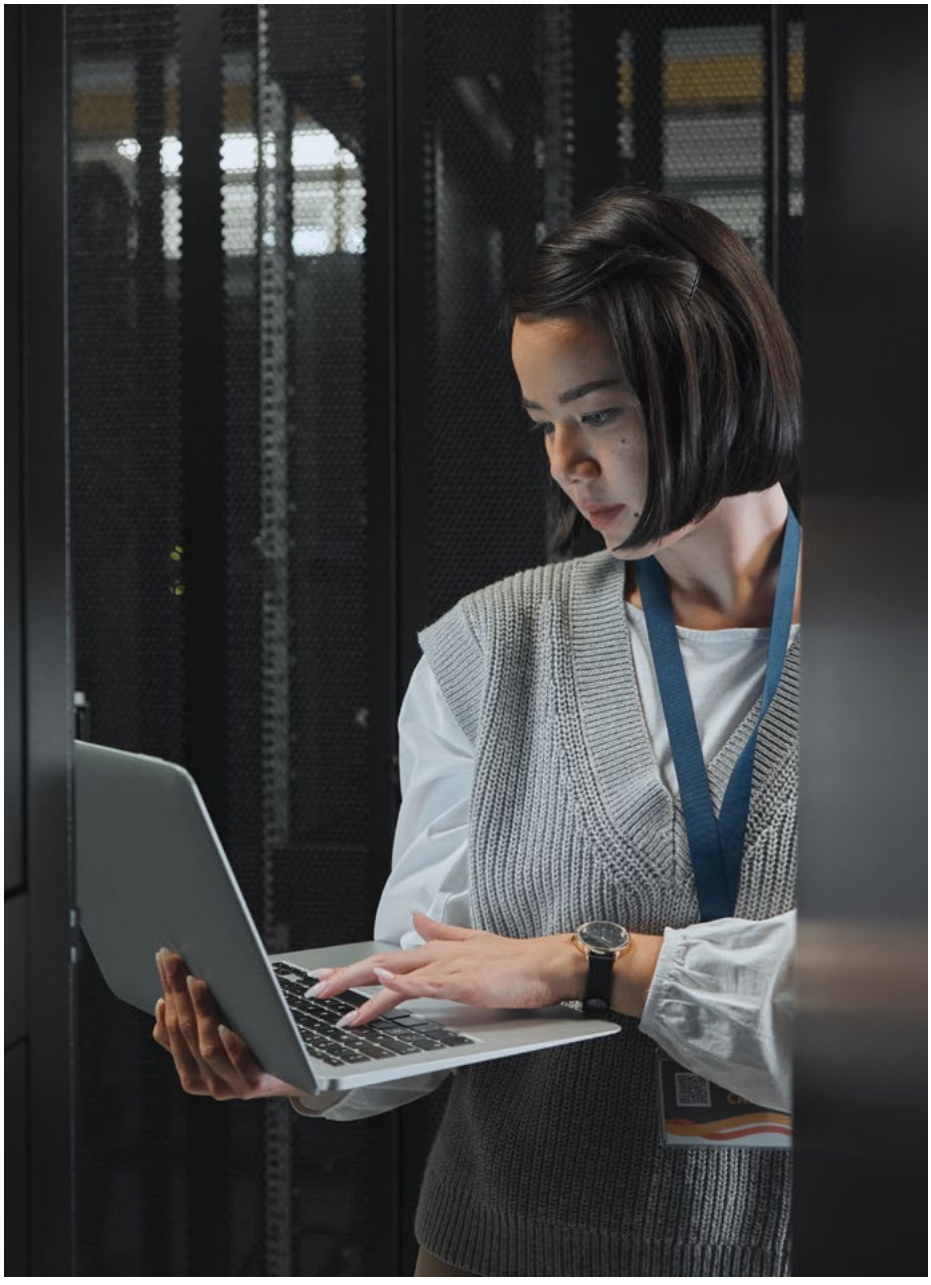
[7] Hay que tener en cuenta que puede haber diferencias entre entornos rurales y urbanos

[8] Se puede encontrar más información en el documento "Acceso y uso de internet en América Latina y el Caribe. Resultados de las encuestas telefónicas de alta frecuencia de ALC 2021*", de septiembre de 2022, publicado por el Programa de las Naciones Unidas para el Desarrollo https://www.undp.org/es disponible en https://www.undp.org/sites/g/files/zskgke326/files/2022-09/undp-brlac-Digital-ES.pdf

Por encima del 70% se encuentran pequeños países como Santa Lucía o Dominica, junto con países de mucho mayor extensión, como Brasil y Chile, y por debajo del 40% se encuentran Guatemala, Nicaragua y Haití.

La conectividad a internet es clave para que las empresas desarrollen estrategias de transformación digital, ya que permite acceder a nuevos clientes o implementar el teletrabajo. Conocer el volumen y tipos de acceso disponibles es esencial para tomar decisiones al respecto.

El concepto de transformación digital no es nuevo, pero tal vez se ha hablado mucho y actuado poco, por lo que aún se utiliza con frecuencia. Algunas iniciativas y cifras ayudan a comprender que, aunque se han dado pasos, queda camino por recorrer, debido a la rápida evolución tecnológica ya que no todas las empresas pueden ir al mismo ritmo.



En Europa, la Comisión Europea ha publicado un informe[9] sobre el estado de la Década Digital en Europa, un programa político con objetivos a alcanzar en 2030 a fin de conseguir la transformación digital de Europa que se desarrolla alrededor de cuatro ejes[10]:

- **Habilidades**: disponer de 20 millones de especialistas en TIC (9,5 millones en 2023) con perspectiva de género, y al menos 80% de la población con capacidades digitales básicas (68% en 2023).
- **Transformación digital de las empresas**: que más del 90 % de PYMEs alcancen un nivel básico de uso de las tecnologías digitales (77% en 2023), y que un 75% de las empresas de la Unión Europea utilicen servicios en la nube, inteligencia artificial o soluciones de "big data".[11]
- **Infraestructuras digitales seguras y sostenibles**: conectividad Gigabit universal[12]; creación de 10.000 "edge nodes"[13] de alta seguridad, climáticamente neutros; y disponibilidad de hasta 3 ordenadores con aceleración cuántica.[14]
- **Digitalización de los servicios públicos**[15]: para ciudadanos y empresas, particularmente los servicios públicos clave como, disponer del 100% de acceso a la historia de salud digital, o la identidad digital, de manera que el 100 % de los ciudadanos tengan acceso a una identificación digital en el 2030.

Iniciativas como la Década Digital europea evidencian que incluso regiones avanzadas en tecnología digital deben seguir esforzándose para obtener el máximo provecho.

En América Latina y el Caribe, el informe de 2022 "Datos y hechos sobre la transformación digital"[16], sobre la "Agenda Digital para América Latina y el Caribe" que analiza los principales indicadores de adopción de tecnologías digitales, constata que casi el 67% de la población eran usuarios de internet pero con menor penetración de banda ancha que Norteamérica y Europa.

[9] En septiembre de 2023 se ha publicado el primer informe sobre el estado de la Década Digital en Europa https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade

[10] Para una descripción ampliada de esta iniciativa de la Unión Europea es útil consultar el siguiente enlace https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_es?etrans=es

[11] Según el informe de la Comisión Europea los porcentajes actuales serían: servicios en la nube (45%), inteligencia artificial (11%) o soluciones de "big data" (19%)

[12] En el informe de la Comisión Europea, el despliegue de la banda de frecuencias de 3,4-3,8 GHz de 5G se encuentra en el 41%

[13] La tecnología Edge Computing es una propuesta tecnológica que permite que los datos no deban procesarse totalmente centralizados, pudiendo procesarse en ordenadores distribuidos llamados "Edge Nodes".

[14] En el informe de la Comisión Europea se pone en evidencia que todavía no existen resultados en estas 2 cuestiones: creación de "Edge nodes" y disponibilidad de ordenadores cuánticos

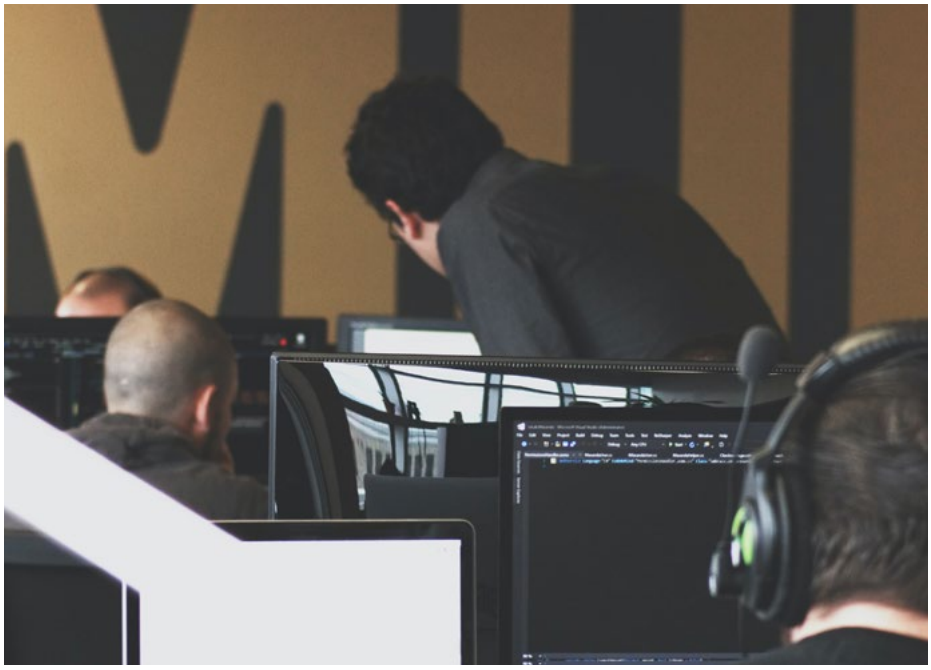
[15] La mayoría de los indicadores que maneja el informe de la Comisión Europea están muy cerca del 80%, y los servicios públicos para empresas están en el 84%, mientras que el acceso a las historias de salud digitales se sitúa en el 72%

[16] El informe hace referencia al periodo 2005-2019, ya que en el año 2020 la Agenda Digital para América Latina y el Caribe cumplía 15 años. https://www.cepal.org/sites/default/files/publication/files/46766/S2000991_es.pdf

El barómetro sobre transformación digital en España y Latinoamérica de 2021[17] publicado por Three Points[18] concluye que la mayoría de empresas iberoamericanas no la han iniciado formalmente (58% en general y 78% en Latinoamérica), aunque un 71% tenía intención de hacerlo en 2022. España (44%) y México (58%) son los países que tienen un mayor número empresas que han iniciado su transformación digital.

Los principales motivos son la falta de inversiones (54%) y de habilidades digitales (51%) y, precisamente, conseguir una mayor rentabilidad de las actividades de negocio se identificó como la principal motivación para iniciar el proceso de transformación digital (67%), a lo que debe añadirse que el 70% de las empresas que habían iniciado su transformación digital valoraron que el éxito del proceso había sido medio o alto.

Por tanto, ahora más que nunca debe estar en la agenda de los directivos. No es una carrera para velocistas, sino para fondistas, que deben planearlo todo para alcanzar el éxito, que no es necesariamente llegar primero, sino en condiciones.



¿Qué debemos tener en cuenta para abordar un proceso de transformación digital?

Junto con el contexto para definir la estrategia de transformación digital y diseñar un plan en torno a procesos, tecnología y personas, debemos asumir premisas inspiradoras del proceso, que es principalmente tecnológico. La ciberseguridad tendrá un peso significativo en tecnología, pero también en organización y personas.

[17] El "Think Digital Report 2021" analiza la situación respecto de la transformación digital en España y en países de Latinoamérica: México, Colombia, Perú, Ecuador y Argentina http://crm.threepoints.com/comunicacion/prensa/ThreePoints_Think_Digital_Report_2021_ResumenEjecutivo.pdf

[18] Three Points The School for Digital Business https://www.planeta.es/ca/three-points-school-digital-business

La transformación digital, por naturaleza, no acaba nunca. Es parte del progreso y mejora continuos. No sirve un gran esfuerzo si luego no usamos las tecnologías adecuadas. Debemos estar alerta a nuevas soluciones y valorar adoptarlas o no, un dilema permanente.

Hay cuatro premisas básicas que deberemos tener en cuenta para afrontar el reto que supone la transformación digital:

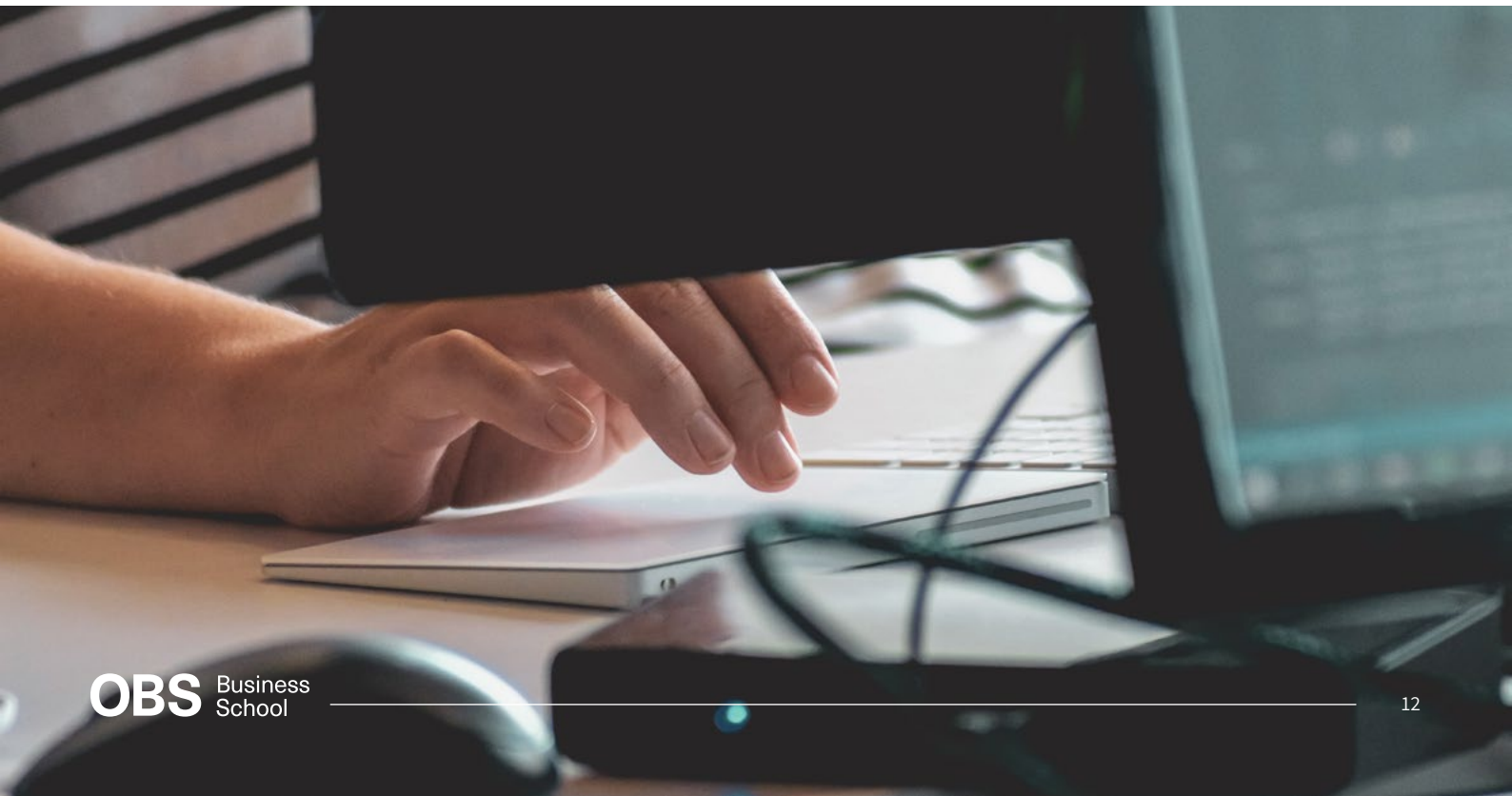
1. **El liderazgo del proceso:** la transformación digital se despliega de arriba abajo. La dirección debe tener un papel esencial en todo el proceso, aportando recursos e implicándose al máximo en todas las etapas.

2. **La planificación:** la transformación digital requiere un plan. Los cambios pueden ser tan disruptivos que no cabe la improvisación, especialmente en la selección y seguridad de las tecnologías.

3. **La especialización:** se requieren recursos internos y externos realmente especializados, tanto en el negocio como en las tecnologías elegidas y en la seguridad de la información. Deben incorporarse nuevos perfiles o capacitar a los existentes para que la falta de conocimiento no sea una barrera.

4. **La implicación:** toda la organización debe alinearse con los cambios, estando informada, concienciada y formada en el momento y con los contenidos adecuados.

La realidad es que aún estamos en una etapa incipiente de los procesos de transformación digital, sin poder detectar nuevas tendencias que modifiquen el escenario a medio plazo. Un indicador son las agendas políticas de transformación digital con horizontes en 2030. Elucubrar más allá se aproximaría a la ciencia ficción, y lo cierto es que aún queda mucho por consolidar.



Capítulo 3

Contextualizando la Ciberseguridad y su vínculo inseparable con la transformación digital

El concepto de ciberseguridad está vinculado al de seguridad de las TIC, siendo prácticamente equivalentes en la mayoría de definiciones.[19]. El motivo de que nos centremos ahora en la ciberseguridad no es otro que la propia evolución del uso de las TIC, que no se concibe fuera de las redes públicas de comunicaciones, es decir, de Internet, , de ahí que habar de seguridad de sistemas de información es referirse a la ciberseguridad, es decir, la protección de activos de información accesibles desde o hacia Internet.

[19] A principios de los ochenta se fundamentan las bases de la seguridad de la información tal y como la conocemos actualmente, como principal referencia tenemos el documento de James P. Anderson, de 1980, *"Computer Security Threat Monitoring and Surveillance"*.

Una definición formal de ciberseguridad nos la propone ISACA (Asociación de Auditoría y Control de Sistemas de Información)[20]; la ciberseguridad es la:

> *"Protección de activos de información – conocimientos y datos con valor para la organización - 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".*

De esa definición podemos extraer los cuatro elementos que forman parte esencial de la ciberseguridad:

- El objetivo de proteger los activos de información de los que dependen las actividades de las organizaciones, en lo que respecta a su tratamiento, almacenamiento y comunicación.
- La necesidad de gestionar los riesgos, con el fin de adoptar controles que permitan mitigarlos (reducirlos) hasta niveles aceptables por la organización.
- Los activos de información a proteger están interconectados, es decir, su uso está vinculado al hecho de estar conectados a redes públicas de comunicaciones.
- Y como consecuencia de esa interconexión, serán objeto de protección activos de información digitales.

Una característica esencial de la ciberseguridad es abordarla como un proceso, no solo como implementación de tecnología. Ésta deberá ser gestionada en base a procesos, ya que no basta con implementar soluciones de seguridad[21], se requiere acompañarlas de procesos, procedimientos, organización y políticas con directrices de seguridad desde la alta dirección a toda la organización, cuya implicación es esencial para una adecuada gestión de la ciberseguridad.

---

[20] ISACA es una organización cuyos miembros son profesionales relacionados con los sistemas y las tecnologías de la información, y para los cuales ISACA dedica esfuerzos con el objeto de que estos aumenten sus habilidades y conocimientos en auditoría, ciberseguridad y tecnologías emergentes; con más de 50 años de existencia y con 170.000 miembros y presencia en 188 países https://www.isaca.org/

[21] Aplicaciones de seguridad y dispositivos cuya función es proteger los activos de información, como por ejemplo: los antivirus, los firewalls, los sistemas de backup, los IDS -Intrusion Detection System- o los sistemas de detección de intrusiones, entre otros muchos tipos de soluciones de seguridad.

Por supuesto, las decisiones en materia de ciberseguridad deben adaptarse a las características y circunstancias de cada organización, pero eso no es obstáculo para que todas las empresas tomen decisiones para proteger sus activos de información, ya que la realidad es que están expuestos a ser objeto de ataques con consecuencias muy graves.

De hecho, muchos de los esfuerzos destinados a que los activos de información estén convenientemente protegidos se dirigen precisamente a pequeñas y medianas empresas, ya que las grandes empresas ya cuentan con recursos suficientes para afrontar las amenazas a que están expuestos sus servicios y plataformas digitales, así como la información que manejan, amenazas que no difieren demasiado de aquellas a las que están expuestas las citadas pequeñas y medianas empresas[22].

Existe una clara conexión entre el desarrollo de la sociedad de la información (y de los procesos de transformación digital), con la necesidad de proteger la información; la seguridad de la información tiene como principal función generar confianza, ya que implica que los usuarios y los propietarios de los sistemas de información deben confiar en que:

- La información estará disponible cuando y donde se la necesita, es decir, estará garantizada su disponibilidad.
- La información no será modificada sin control, es decir, se garantizará su integridad, es decir, podremos confiar en que la información es correcta para su uso en las actividades de negocio, y no ha sido manipulada o alterada accidental o malintencionadamente.
- La información se mantendrá accesible solo para aquellos que deben conocerla, por tanto, garantizando su confidencialidad.

Las tecnologías de la información y la comunicación (TIC) son esenciales para las organizaciones, mejorando la eficiencia y expandiendo oportunidades de negocio, especialmente en “social media”. Estas tecnologías, fundamentales, enfrentan diversas amenazas, necesitando estrategias proactivas para disminuir riesgos e impactos.

La información forma parte de esos activos a proteger, pero desgraciadamente no siempre la seguridad de la información se tiene suficientemente en cuenta, al menos de manera preventiva, y resulta habitual que solo se eche en falta cuando se produce algún incidente que causa daños, en ocasiones irreparables, tanto de tipo material como de reputación, que al final se traducen en pérdidas económicas o de credibilidad.

A medida que las organizaciones reconocen su alta dependencia de las TIC para sus operaciones, comprenden que no pueden permitirse fallos en sus sistemas. Esta conciencia eleva la demanda de seguridad, especialmente porque muchas actividades empresariales dependen completamente de las tecnologías de la información. Así, cualquier brecha de seguridad puede inutilizar el negocio o degradar severamente su rendimiento.

---

[22] Resulta de interés consultar los recursos que el INCIBE (Instituto Nacional de Ciberseguridad español) https://www.incibe.es/ pone al alcance de pequeñas y medianas empresas; en https://www.incibe.es/empresas/herramientas/politicas se publican documentos que van a permitir a este tipo de empresas asegurar sus activos de información, sin que el coste tenga que suponer una dificultad insalvable.

Precisamente, llevar a sus últimas consecuencias un proceso de transformación digital pone a las empresas en esa situación de vulnerabilidad, por la alta dependencia que tiene el negocio de las tecnologías, lo que genera un riesgo inherente solo por el mero hecho de utilizarlas.

Las medidas de seguridad deben adecuarse a los riesgos únicos de cada empresa. Esto implica identificar claramente los activos de información vulnerables a ciberincidentes, para posteriormente analizar y evaluar los riesgos a que están expuestos tales activos y tener la capacidad de decidir de qué modo mitigarlos, es decir, qué medidas de seguridad deberán implementarse, teniendo en cuenta su eficacia y un uso eficiente de los recursos disponibles.

La necesidad de que los procesos de transformación digital vayan acompañados de decisiones en materia de ciberseguridad es indiscutible, a mayor dependencia de las tecnologías, mayores son los riesgos, y más autoexigentes deben ser las empresas con las medidas de ciberseguridad. De otro modo, no solo los activos de información estarán amenazados, el propio negocio estará en riesgo.

La ciberseguridad precisa ser abordada de forma ordenada. Como el proceso de transformación digital, el proceso de ciberseguridad deberá planificarse, de modo que tampoco cabe improvisar en este asunto. Básicamente las fases típicas son:

- **Planificación de la seguridad:** Diseñar la gestión de la ciberseguridad considerando los riesgos identificados. En entidades mayores, incluye establecer la estructura organizativa y políticas de ciberseguridad.
- **Implementación de procedimientos:** Definir la operativa de las medidas de seguridad seleccionadas.
- **Gestión de la seguridad:** Asegurar que las prácticas de seguridad se apliquen y funcionen según lo planeado.
- **Control y verificación:** Revisar constantemente la seguridad de los sistemas de información, adaptándose a las evoluciones tecnológicas y de ciberataques para mantener los riesgos en niveles aceptables.

Y la estrategia principal para llevar a cabo todas las acciones relacionadas con implementar la ciberseguridad, es plantearla con un enfoque de "ciberseguridad desde el diseño", es decir, desde el mismo momento en que estamos valorando adoptar una cierta tecnología, uno de los elementos a evaluar, junto con sus capacidades, funcionalidades, escalabilidad, costes, etc., será su seguridad intrínseca (propia) y su encaje en nuestro modelo de ciberseguridad.

La citada estrategia debe completarse con otra estrategia de seguridad de carácter operativo, denominada "Zero Trust", que se basa en considerar que ninguna persona o dispositivo, tanto si se ubica dentro o fuera de la red de una organización, debe tener acceso a los sistemas de información, hasta que se considere explícitamente necesario y ello se verifique; en definitiva, "cero confianza" por defecto.

Por tanto, hay que considerar la ciberseguridad como un proceso estratégico, que debe formar parte del sistema de gestión integral de la organización, alineándose con los objetivos de negocio; una empresa que cuida de sus sistemas de información no solo va a desarrollar con mayor eficacia sus procesos de negocio, también va a generar mayor confianza en sus clientes y empleados y, en general, en todas aquellas partes interesadas en su actividad, e incluso le puede generar un valor competitivo en el mercado, especialmente si sus competidores sufren algún incidente que comprometa la ciberseguridad de sus sistemas de información.

La información que manejan las empresas y, en general sus sistemas de información, sufren exposición a acciones de carácter delictivo directa o indirectamente relacionadas con las tecnologías, de hecho casi a diario podemos leer noticias en prensa al respecto, se puede decir que ninguna compañía está a salvo, , ya que los objetivos de los delincuentes no se centran exclusivamente en las grandes compañías, o en empresas con datos valiosos (por ejemplo, bancos o grandes comercios electrónicos), también son objetivo las pequeñas y medianas empresas, e incluso los particulares.

Que exista esa delincuencia organizada, que actúa utilizando también los avances tecnológicos, no debe hacernos perder de vista que también podemos tener incidentes internos, es decir, que, ya sea de manera accidental o malintencionada, miembros de la propia organización actúan de manera incorrecta, y ello acabe provocando un incidente de graves consecuencias para los sistemas de información[23].

Por supuesto, el origen y características de los ciberataques ha ido evolucionando, pasando de una situación inicial de individuos que en solitario, o en muy reducidos grupos, perpetraban ese tipo de acciones que, por distintos motivos (no siempre de carácter lucrativo) perjudicaban a las empresas, a la situación actual, en la que los cuerpos y fuerzas de seguridad que investigan ese tipo de actividad delictiva se enfrentan a verdaderas organizaciones criminales, con equipos de expertos altamente cualificados y altas posibilidades de alcanzar sus objetivos ya que disponen de muchos recursos para desarrollar sus actividades delictivas, que cada día son más lucrativas y con menor riesgo; y, por supuesto, tampoco hay que dejar de lado los ataques cuyo origen son activistas de todo tipo.

En ese escenario, cualquier empresa puede padecer un ataque que inutilice sus sistemas, o le impida disponer de su información de negocio; actualmente el ataque más típico, y usualmente más devastador, es aquel que, una vez se toma el control de los sistemas de la empresa atacada, se procede al cifrado de la información, produciéndose un verdadero *"secuestro de la información"*, ya que se solicita un rescate, en base a una cantidad en dinero a cambio de entregar las claves de descifrado (si consultamos en "Google" por "ransomware cryptolocker"[24] encontraremos multitud de casos e información al respecto).

Además, esa delincuencia no solo está muy preparada y dispone de muchos y sofisticados recursos, se encuentra muy bien organizada desde la perspectiva de la especialización que tienen los diferentes grupos de delincuentes, ya que, por ejemplo, algunos tan solo se dedican a obtener el control de redes empresariales, para vender ese control, y que otros delincuentes lo exploten, otros se dedican al robo de información confidencial, otros se dedican a las estafas, otros al blanqueo de dinero, etc.

Todo ello ha supuesto un considerable aumento de ese tipo de delitos en todo el mundo, es un fenómeno global, lo que ha obligado a los cuerpos y fuerzas de seguridad, ha adaptarse a esas nuevas formas de delincuencia, creando grupos especializados, dedicados a investigar y perseguir ese tipo de delitos, y en paralelo las normas penales también se han adaptado a ese escenario para poder juzgar y sancionar esas conductas.

Los ciberataques están en constante aumento y además son más sofisticados, en España en el 2022[25] los ciberataques aumentaron un 28% con respecto a 2021, una tendencia al alza que se ha mantenido durante lo que llevamos el 2023, por tanto, evitar un ciberataque o defenderse de este, es cada vez más complejo.

---

[23] Pensemos en las situaciones de teletrabajo, que implican acceder a sistemas de información de la empresa desde ubicaciones fuera de esta, a través de redes de comunicaciones públicas y de dispositivos que, en muchos casos, son propiedad de los empleados y que, por tanto, utilizan también para fines propios.

[24] Ya en el año 2016 Europol en su informe "Internet Organised Crime Threat Assessment", identificó el "ransomware" como una de las principales ciberamenazas https://www.europol.europa.eu/cms/sites/default/files/documents/europol_iocta_web_2016.pdf

[25] Para información detallada se puede consultar el "Informe sobre la cibercriminalidad en España", del Ministerio del Interior del Gobierno de España, disponible en https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2021_126200212.pdf

En un documento del Parlamento Europeo, del pasado 21 de marzo de 2023[26], se afirmaba que las amenazas a la ciberseguridad crecen como consecuencia de la transformación digital, y hace referencia al informe "Threat Landscape 2022" de ENISA[27], señalando que los sectores que sufrieron más ataques entre junio de 2021 y junio de 2022 fueron: la administración del Estado (24%), los servicios digitales (13%), la ciudadanía (12,4%), los servicios (11,8 %), el sector financiero (8,6%) y el sector sanitario (7,2%).

A su vez, en el documento "Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe"[28], de la Comisión Económica para América Latina y el Caribe (CEPAL), se pone el énfasis en los ataques que durante el periodo 2020-2022 afectaron a infraestructuras críticas[29], enmarcándolos en lo que denomina *"acelerado proceso de digitalización de los últimos años"*, e indicando que si bien se han producido importantes avances en los marcos normativos durante el año 2022, y en las estrategias de ciberseguridad en la zona, "aún falta mucho por hacer".

El informe también hace referencia a que los 27 millones de pequeñas y medianas empresas que existen América Latina y el Caribe, conforman un sector económico que tiene un gran impacto social y económico, y según Kaspersky, esas empresas pueden tener pérdidas de hasta 155 mil USD al sufrir un ciberataque, además de tener que hacer frente a multas de las autoridades o indemnizaciones a clientes, el abandono de socios de negocio, o daños a su imagen o reputación.

Diferentes estudios y expertos señalan que los ciberataques, particularmente los de «ransomware», continuarán predominando entre los incidentes cibernéticos. Estos ataques han experimentado un aumento significativo desde 2020, impactando sobre todo a pequeñas y medianas empresas, con un incremento aproximado del 75%.

Las tendencias de ciberataques para 2023 reflejan una sofisticación creciente, en gran parte impulsada por el uso de inteligencia artificial. La IA se está empleando para desarrollar ataques más efectivos, sin embargo, también es una línea de defensa, utilizándose para contrarrestar estas amenazas avanzadas:

- **Malware avanzado**: Este software malicioso se está perfeccionando para eludir la detección de antivirus, cambiando constantemente su "apariencia".
- **Ransomware**: Se está volviendo más sofisticado y dañino, con rescates más elevados. Destaca el "ataque de triple extorsión", que implica cifrado de datos, venta de información robada y amenazas de ataques adicionales.

---

[26] Se identifican las principales amenazas a la ciberseguridad en el 2022 y los sectores más afectados, así como el impacto de la guerra en Ucrania, se afirma que las amenazas a la ciberseguridad crecen como consecuencia de la transformación digital, poniendo en evidencia que durante la pandemia de Covid-19, las empresas tuvieron que hacer rápidas adaptaciones al modelo de teletrabajo, lo que tuvo como consecuencia un aumento de los ciberataques. https://www.europarl.europa.eu/pdfs/news/expert/2022/1/story/20220120STO21428/20220120STO21428_es.pdf

[27] La Agencia de la Unión Europea para la Ciberseguridad https://www.enisa.europa.eu/ (ENISA), fue creada en el año 2004 y reforzada por el Reglamento sobre la Ciberseguridad de la UE del 2019 https://www.boe.es/buscar/doc.php?id=DOUE-L-2019-80998 , entre sus funciones destaca la de contribuir a la política de ciberseguridad de la Unión Europea.

[28] El objetivo del documento es identificar las políticas dirigidas a analizar los incidentes de ciberseguridad ocurridos entre 2020 y 2022, en diez países seleccionados de América Latina, incluyendo información obtenida por los equipos de respuesta a incidentes de ciberseguridad, así como informes publicados por instituciones especializadas en la materia https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content

[29] En total 82 ataques relevantes, repartidos en los 10 países que forman parte del estudio realizado:

- **Phishing y Smishing**: Los ataques de phishing se están refinando, eliminando los errores que denotaban su falsedad. El smishing, similar al phishing pero a través de SMS, explota la menor protección de los teléfonos móviles.
- **Seguridad en la nube**: Aunque los servicios en la nube han sido relativamente resistentes, su creciente uso por empresas requiere una atención mayor en la ciberseguridad, ya que los ataques se están desplazando hacia estos sistemas.
- **Ataques a redes domésticas**: Con el auge del teletrabajo, las redes domésticas, generalmente menos seguras, se han convertido en objetivos, aprovechando sus vulnerabilidades.

En el ya citado informe "Threat Landscape 2022" de ENISA, se identifican las 8 amenazas a la ciberseguridad más frecuentes: "ransomware", "malware", ingeniería social[30], amenazas contra los datos[31], amenazas contra la disponibilidad y denegación de servicio[32], amenazas contra la disponibilidad de internet, desinformación/mal uso de la información o difusión de información engañosa[33] y ataques a la cadena de suministro[34].

En cuanto a las tendencias de defensa antes los ciberataques, la adopción de la autenticación multifactor, que ya se ha empezado a usar, en el 2023 va a seguir creciendo, ya que añade una capa de seguridad adicional a los inicios de sesión en los sistemas, y según diversos estudios con esta medida se pueden detener prácticamente la totalidad de los ataques de "phishing" general, y un alto porcentaje, superior al 70%, de los ataques dirigidos.

Y por supuesto, la gran tendencia va a ser el uso de la inteligencia artificial en las diferentes soluciones de ciberseguridad, lo que va a provocar que estás den un salto cualitativo y cuantitativo en lo que respecta a su eficacia frente a los ciberataques, que irá acompañada de los denominados modelos de seguridad como servicio[35], permitiendo a un buen número de organizaciones definir una estrategia o modelo de seguridad de sus activos de información con el que pueden conseguir un entorno razonablemente seguro para desarrollar sus actividades de negocio en un contexto digital, y además acometer el proceso de transformación digital, mitigando los riesgos específicos en materia de ciberseguridad.

[30] *"Casi el 60% de los ataques en Europa, Oriente Medio y África incluyen un componente de ingeniería social, según una investigación citada por ENISA"*

[31] Con el fin de para obtener acceso no autorizado y/o divulgar la información

[32] Se materializan en ataques que impiden a los usuarios acceder a datos o servicios

[33] Se hace referencia expresa a la tecnología "deepfake", que permite generar audio, vídeo o imágenes falsos que pueden pasar por reales.

[34] Suelen combinar dos ataques, contra el proveedor y contra el cliente, se afirma que "las organizaciones son cada vez más vulnerables a este tipo de ataques, debido a la creciente complejidad de los sistemas y a la multitud de proveedores, que son más difíciles de supervisar"; la transformación digital también puede favorecer que este tipo de amenazas acaben siendo incidentes de seguridad, que frecuentemente van a tener consecuencias en forma de pérdidas económicas

[35] La seguridad como servicio (SECaaS) es un modelo de prestación de servicios de seguridad en el que se ofrece a las organizaciones un acceso a soluciones y servicios de ciberseguridad en la nube, lo que puede incluir sistemas de gestión de accesos e identidades, los firewalls, las redes privadas virtuales (VPN) o la monitorización continua de los sistemas.

Capítulo 4

Las exigencias jurídicas: innovación y regulación

La historia humana está marcada por avances tecnológicos que, si bien impulsan el desarrollo y bienestar, también introducen o intensifican riesgos. Ejemplos claros incluyen la energía nuclear, la industria automovilística, farmacéutica, y la aviación comercial, donde la paradoja de "beneficio-riesgo" resulta evidente.

En estos contextos, la regulación busca equilibrar intereses contrapuestos y mitigar riesgos, imponiendo marcos legales con principios y obligaciones que fomenten una coexistencia armoniosa. Sin embargo, la legislación a menudo se rezaga, especialmente en sectores de rápido avance como las TICs, dificultando la creación de leyes duraderas y adaptativas ante desafíos emergentes.

Esos marcos jurídicos abordan muchas cuestiones, pero cuando se trata del uso de las tecnologías de la información y la comunicación, hay un claro denominador común: la seguridad de la información.

Aunque idealmente, las medidas de seguridad deberían integrarse en una cultura de autoprotección, evitando depender excesivamente de la regulación, la realidad demuestra que esto es necesario. Factores como el desconocimiento, la falta de concienciación, restricciones presupuestarias, desalineación con objetivos empresariales, u otras prioridades, han impedido históricamente que la protección de sistemas de información sea impulsada adecuadamente por las empresas, quienes deberían ser las más interesadas en asegurar sus sistemas y tecnologías.

El legislador se ha visto obligado, con el fin de favorecer unas condiciones adecuadas en el uso de las TIC, a elaborar normas que promueven la cultura de la seguridad de la información, llegando a recurrir a la sanción económica ante el incumplimiento de obligaciones relacionadas con la protección de la información[36].

Las buenas prácticas en seguridad de la información pueden ser asumidas bien como un ejercicio autónomo de gestión responsable de los medios tecnológicos utilizados, o bien porque el entorno en el que la organización desarrolla sus actividades ejerce una cierta presión para posicionarse adecuadamente respecto de la seguridad de la información, ya sea por influencia de la competencia, del mercado, de los clientes, de los accionistas, de los proveedores, o de cualquier otro agente interesado directa o indirectamente en la actividad de la organización (stakeholders).

Hay un segundo escenario, en el que la motivación tiene un carácter más "externo", la acción del legislador, cuando decide que hay actividades, que necesariamente deben incorporar medidas de seguridad de la información para ser llevadas a cabo dentro de la legalidad.

Así, cuestiones como la protección de los datos personales, o la regulación de la seguridad en el contexto de la administración electrónica, el "compliance", la regulación de la historia clínica, la prevención del fraude, la ciberseguridad, etc., obligan a que se tomen medidas de seguridad.

[36] Particularmente en el caso del derecho a la protección de los datos de carácter personal.

Un ejemplo destacado de regulación en seguridad de la información es el Reglamento General de Protección de Datos (RGPD) de Europa, aprobado en 2016. Esta normativa, que aplica a toda la UE, considera esencial proteger la seguridad de los datos personales, exigiendo a las organizaciones evaluar los riesgos asociados a cualquier operación de tratamiento de datos personales. El RGPD trasciende las fronteras europeas, aplicándose a empresas fuera de Europa si estas ofrecen bienes o servicios a individuos en la UE y manejan sus datos personales. Esta amplia cobertura ha hecho del RGPD un referente regulatorio en diversas regiones del mundo.

La seguridad de la información, desde la perspectiva de protección de datos personales, implica concretar qué controles o medidas de seguridad hay que implementar en los tratamientos de datos personales a fin de preservar la disponibilidad, integridad y confidencialidad de la información de carácter personal.

El principio de seguridad en el contexto de la protección de datos de carácter personal se concreta en el deber jurídico que tienes las empresas que tratan datos personales, de llevar a cabo las acciones necesarias para proteger los datos de carácter personal; la regulación europea no incorpora un catálogo de medidas de seguridad, solo hace referencia a:

- La aplicación de la “seudonimización” o el cifrado de datos personales.
- La capacidad de garantizar la confidencialidad, integridad y disponibilidad, así como la resiliencia, de los datos y de los sistemas de información.
- Se refiere a los planes de contingencia y de continuidad para el caso de incidentes técnicos o físicos.
- Alude a la implementación de procesos de verificación periódica de la eficacia de las medidas técnicas y organizativas implementadas.

En materia de seguridad de los datos se añade además la obligación de notificar los incidentes de seguridad ("data breach") a las autoridades de protección de datos, de manera ordinaria en un plazo máximo de 72 horas; incluso se prevé la comunicación del incidente a las personas afectadas, cuando este pueda suponer un alto riesgo para las personas.

Finalmente, hay que hacer una breve referencia al régimen sancionador, especialmente por lo que respecta a la cuantía de las sanciones económicas, cuando se produzca una situación de ausencia de medidas de seguridad, o incluso si estas no han sido eficaces a causa de cómo se han implementado y/o gestionado, la sanción podrá ser de hasta 10 millones de euros, o un 2% de la facturación a nivel mundial.

En el proceso de transformación digital de las empresas se van a ver involucrados datos personales, de ahí la importancia de tener en cuenta regulaciones que establecen unas obligaciones jurídicas tan específicas.

Y, en este punto, conviene hacer una referencia al equilibrio entre la innovación y la regulación, ya que al fin y al cabo, acometer un proceso de transformación digital es innovación, que se verá limitada por lo dispuesto en la regulación.

La OCDE hace una definición formal de que debemos entender por innovación, desde un prisma eminentemente económico: "La innovación es un proceso iterativo activado por la percepción de una oportunidad proporcionada por un nuevo mercado y/o nuevo servicio y/o avance tecnológico que se puede entregar a través de actividades de definición, diseño, producción, marketing y éxito comercial del invento".

La innovación tiene como principal objetivo generar valor, la vía para llegar a esa generación de valor es el cambio y, ese cambio, debe tener como base el conocimiento, sea científico, técnico o de otro tipo; la innovación viene estimulada en gran parte por el hecho de que existe una necesidad no resuelta, o que no se resuelve de manera eficaz o eficiente con las soluciones o enfoques existentes, y es en la búsqueda de una nueva solución a esa necesidad que se gesta la innovación.

Por tanto, la transformación digital es claramente innovación, pero surge la duda de si innovación y regulación se pueden compatibilizar.

Dado que la actividad de las empresas y de los individuos debe ajustarse al ordenamiento jurídico, la "innovación", con carácter general, y como actividad que tiene como origen y destino a personas físicas y jurídicas, también recibirá el impacto de la regulación, ya que ésta deberá sujetarse a las leyes y normas.

Los Estados, en su papel de regulador, influyen sobre la actividad innovadora, hasta tal punto que la pueden fomentar o dificultar, por tanto, la regulación nunca va a ser neutra respecto del desarrollo de las actividades vinculadas a la innovación.

El equilibrio está en conseguir que la regulación no sea un obstáculo a la innovación, sin devaluar los derechos y libertades de los ciudadanos, y propiciando a la vez el crecimiento económico y el bienestar social, objetivos todos ellos compatibles, si se dispone de una regulación adecuada.

A la hora de analizar el posible impacto que una norma puede tener sobre la innovación, la mayoría de los estudios parten de la base de que se pueden distinguir hasta tres tipos de regulación: económica, social e institucional.

La regulación económica tiene como principal objetivo mejorar la eficiencia de los mercados y suele centrarse en la defensa y estimulación de la competencia. En este encuadre podemos encontrar regulaciones antimonopolio, reglas dirigidas a los procesos de fusión y adquisiciones –especialmente en relación a grandes compañías-, los requisitos y condiciones para entrar en los diferentes mercados, la regulación de precios y en general la regulación de los monopolios, del tipo que sean (energéticos, telecomunicaciones, tecnológicos, etc.).

La regulación social irá dirigida a reducir el impacto negativo, sobre las personas, de ciertas actividades, como, por ejemplo, la protección del medio ambiente, o de la salud y la seguridad de consumidores y trabajadores, se trata de una regulación que suele influir de una manera relevante en la actividad de innovación, tanto para inducirla, como para limitarla, en el caso de que ponga en riesgo a la sociedad en general.

La regulación institucional se identifica con aquella actividad normativa que va orientada a sentar las bases para el desarrollo de las diferentes actividades desarrolladas por empresas y particulares, que si nos centramos en la actividad económica implica, por ejemplo, la elaboración de leyes de responsabilidad –sin este tipo de regulación la aceptación de nuevos productos por parte de los consumidores podría verse afectada– o las leyes relacionadas con la propiedad industrial e intelectual.

Si nos detenemos en casos concretos, por ejemplo, en la industria automovilística, ésta ha ido innovando des de sus inicios (finales del siglo XIX), pasando de una situación en la que no existía ningún tipo de regulación, a ser un sector altamente regulado, que afecta a todos los agentes implicados, desde el fabricante al usuario final, pasando por los diferentes intermediarios y proveedores relacionados con la industria del automóvil, una regulación intensa y muy completa que en ningún caso ha impedido la innovación en este sector productivo, que sigue innovando en diferentes direcciones (seguridad, energía, consumo, comodidad, diseño, etc.).

Nos hemos referido en diversas ocasiones a la inteligencia artificial, como pieza tecnológica que puede estar muy presente en el proceso de transformación digital desde muchas perspectivas; los riesgos de su desarrollo y uso han sido puestos claramente de manifiesto[37], así como las grandes posibilidades que potencialmente puede ofrecer en muchos ámbitos: el diseño, la salud, la educación, la vigilancia, la seguridad, etc.

Si nos referíamos al proceso de transformación digital como algo disruptivo, es evidente que la inteligencia artificial es una tecnología disruptiva, de ahí que encaje como tecnología a tener en cuenta en cualquier proceso de transformación digital, incluso en el contexto de pequeñas y medianas empresas.

[37] Los medios de comunicación se han hecho eco de tales manifestaciones, por ejemplo, https://cadenaser.com/nacional/2023/03/29/musk-y-otros-cientificos-piden-el-cese-inmediato-de-los-experimentos-con-inteligencia-artificial-cadena-ser , https://elpais.com/opinion/2023-04-24/una-moratoria-artificial.html o https://www.elperiodico.com/es/tecnologia/20230329/inteligencia-artificial-elon-musk-yuval-noah-harari-gpt-4-chatgpt-frenar-85333020 por tanto solo citar algunos ejemplos

En abril de 2022 el Parlamento Europeo planteó una hoja de ruta sobre la inteligencia artificial (IA), que respondía a la pregunta de *"¿Cómo puede la UE mejorar su posición mundial en el ámbito de la IA?"38*, esa hoja de ruta tiene en cuenta el informe [39]de la comisión especial sobre Inteligencia Artificial en la Era Digital (AIDA[40]), que propone *"un enfoque integral para conseguir una posición común a largo plazo que destaque los valores y objetivos principales de la UE"*.

A grandes rasgos, lo que proponía el citado informe de la Comisión especial AIDA, era crear *"un entorno normativo favorable, que incluya una legislación dinámica y una gobernanza moderna, ya que la actual legislación nacional y de la UE está fragmentada, es lenta y no ofrece seguridad jurídica"*, a lo que se añade que para apoyar la innovación y evitar que la carga normativa suponga un límite a esta, solo aquellas aplicaciones de la IA que pudieran ser de alto riesgo deberían tener una regulación más restrictiva, ese entorno normativo lo constituye la propuesta de Reglamento de Inteligencia Artificial, aún pendiente de aprobación.

La propuesta de Reglamento de Inteligencia Artificial, incluye el enfoque a riesgos, de modo que establece obligaciones según el nivel de riesgo que pueda suponer el sistema de IA.

La propuesta distingue entre: (I) los usos que pueden generan un riesgo inaceptable (en este caso, la aplicación de la IA está prohibida); (II) un riesgo alto (para el uso de estos sistemas de IA se concretan los requisitos que deben cumplir); y (III) un riesgo bajo o limitado (para los que se dispone que cumplan en particular con ciertas obligaciones relacionadas con la transparencia).

En relación a otros sistemas de IA, se prevé que no estarían sujetos a ninguna obligación en particular, quedando a priori fuera del ámbito de aplicación del futuro reglamento, por tanto, una cuestión esencial será clasificar los sistemas de IA.

En resumen, el Reglamento de IA es una iniciativa legislativa pionera a nivel mundial, que está conectada con diferentes normas, con una especial relevancia en lo que respecta a los procesos de transformación digital; una regulación que tiene el reto de limitar el uso de los sistemas de IA, sin impedir la innovación en esta materia, ni los beneficios de interés general que puede llegar a suponer.

---

[38] Se establecen el recorrido que debe seguirse para que la inteligencia artificial sirva a los intereses de las personas y no las perjudique https://www.europarl.europa.eu/news/es/headlines/priorities/inteligencia-artificial-en-la-ue/20220422STO27705/inteligencia-artificial-la-hoja-de-ruta-del-parlamento-para-la-ue

[39] Informe que ha servido de punto de partida a las iniciativas de las instituciones europeas en materia de inteligencia artificial https://www.europarl.europa.eu/cmsdata/246872/A9-0088_2022_EN.pdf

[40] https://www.europarl.europa.eu/committees/es/aida/home/highlights

Capítulo 5

Estado de la regulación de la ciberseguridad a nivel mundial

A pesar del fenómeno global que suponen los ciberataques, lo cierto es que a nivel internacional el desarrollo de normas jurídicas orientadas a imponer obligaciones en materias de ciberseguridad, es muy desigual, hay muchos países que no tienen regulaciones específicas al respecto, por ejemplo, en el 2020 la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, constató que el 66 % de los países tenía algún tipo de legislación sobre datos, mientras que el 10% tenía proyectos legislativos en marcha, y el 24% no disponía de ninguna normativa, ni tenía proyectos legislativos en marcha.

África

Tal vez África refleje de la manera más evidente, esa desigualdad existente a nivel global, ya que algunos países tienen leyes específicas de ciberseguridad, mientras que otros han incorporado obligaciones relacionadas con la ciberseguridad en normas generales. Sin ser exhaustivos a continuación se hace referencia a algunas de esas normas.

En Argelia (2018), Marruecos (2009), Kenia (2019) y Sudáfrica (2013), tienen leyes de protección de datos personales, que incluyen obligaciones de seguridad.

En Egipto, se incluyen medidas de seguridad es en La Ley de Telecomunicaciones (2003) y en Nigeria (2015) tiene regulados los delitos informáticos.

El documento "Marco político de la Unión Africana en materia de datos"[41] (febrero de 2022) es de interés por describir las tendencias normativas sobre la protección de datos.

Asia

En Asia el desarrollo de normativa relacionada con la ciberseguridad viene motivado tanto por el desarrollo de la industria relacionada con las TIC, como por el control de la información en las redes.

En el 2021 China aprobó la Ley de Seguridad de Datos, que tiene como objetivo regular la obtención, almacenamiento, procesamiento, uso, y transferencia de datos de cualquier tipo (sean personales, o no).

En el 2019 entró en vigor la ley de ciberseguridad de Vietnam, no exenta de polémica ya que las empresas de Internet están obligadas a almacenar información personal de sus usuarios y a entregarla al Estado si éste lo considera necesario.

Hay otros ejemplos, como la legislación de protección de datos de Corea del Sur o la Ley de Protección de Información Personal de Japón, actualizada en el año 2020, además Japón tiene una Ley de Seguridad de la Información.

Por su parte, Singapur tiene Ley de Protección de Datos Personales desde el 2012 y también tiene una ley que regula la seguridad de la información.

Por último, en la India existe la Ley de Tecnología de la Información de la India (2000), que fue objeto de actualización en el 2008 para incluir la seguridad de los datos personales, y desde el 2013 cuenta con una Política Nacional de Seguridad Cibernética.

[41] En su apartado 4.1 https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ES1.pdf

Latinoamérica

Buena parte de la legislación relacionada con la seguridad de la información se deriva de las leyes de protección de datos, como es el caso de Brasil, México, Colombia, Chile, Argentina o Uruguay, entre otros.

La regulación relacionada con los ciberdelitos está muy extendida en Latinoamérica, países como Brasil, Colombia, Chile o Argentina, entre otros, cuentan con ese tipo de normativa.

En Centroamérica la situación es similar, con países como Costa Rica, El Salvador, Guatemala, Honduras o Nicaragua, que tienen regulación tanto en materia de protección de datos como en relación con los ciberdelitos.

En Latinoamérica no se encuentran desarrollos normativos específicos relacionados con leyes de ciberseguridad.

Norteamérica y Oceanía

Tanto en los Estados Unidos, como en Canadá, junto con Australia y Nueva Zelanda, el desarrollo de leyes de ciberseguridad es equivalente al europeo, sin perjuicio de que, especialmente en el caso de los Estados Unidos, la normativa de protección de datos se ha venido desarrollando más en relación con el derecho a la privacidad, y no tanto como un derecho fundamental a la protección de datos.

Capítulo 6

Conclusiones y recomendaciones

La correcta ejecución de un proceso de transformación digital implica a muchos agentes y variables, tanto internos como externos, es una iniciativa que tiene como fin último posicionar a las organizaciones en la nueva era digital, en la que las tecnologías son prácticamente el centro de todas las actividades, pero ello no puede plantearse sin las debidas garantías de seguridad tecnológica y jurídica.

- El proceso de transformación digital es eminentemente disruptivo, es decir, no se trata de una mera evolución, precisa de cambios radicales en las organizaciones, y hay que ser conscientes de ello para alcanzar los máximos beneficios.
- La transformación digital, no deja de ser un reto, no asumirlo puede tener graves consecuencias para las organizaciones, particularmente en términos de competitividad y posicionamiento en el mercado, así que debemos afrontarlo con la actitud y la aptitud necesarias para que sea un éxito; las premisas básicas son: el liderazgo del proceso, la planificación, la especialización y la implicación.
- Estamos a tiempo de iniciar nuestro proceso de transformación digital, por tanto, debe estar recogido en las agendas de los directivos de las organizaciones, aún no estamos llegando con retraso, pero no podemos permitirnos el lujo de esperar mucho más.
- Sin perjuicio de que deban tomarse decisiones de carácter organizativo y jurídico, la transformación digital es, en primer lugar, un proceso eminentemente tecnológico, por tanto, la toma decisiones adecuadas en esta área servirá de soporte y de disparador del resto de decisiones.
- La naturaleza del proceso de transformación digital implica la ejecución de un ciclo continuado, que no tiene fin. Hay que tomar conciencia de ello, se trata de avanzar para mejorar, sin descanso, de nada sirven los grandes esfuerzos puntuales, debemos afrontar el reto con un esfuerzo continuado y planificado.

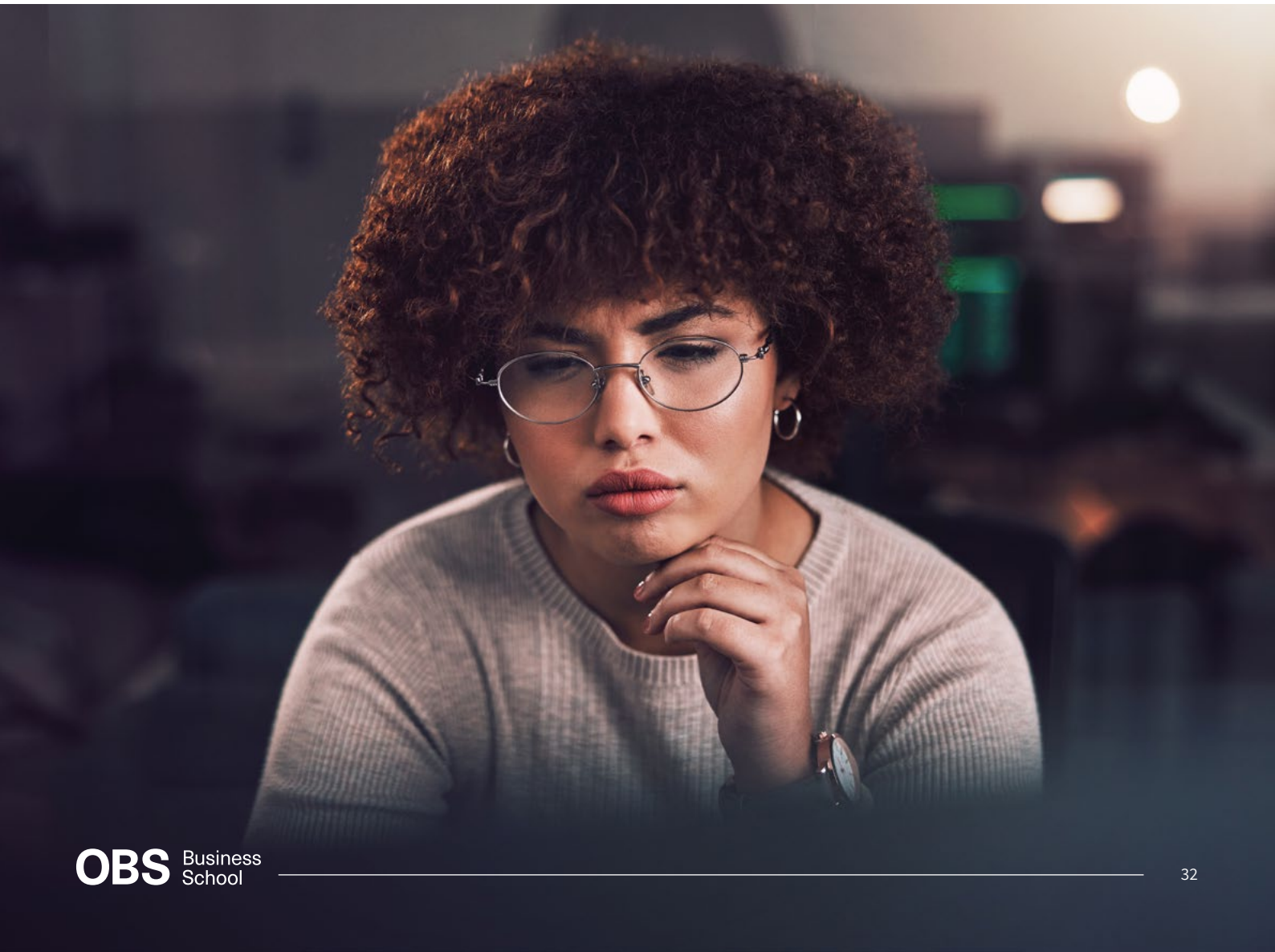
El proceso de transformación digital no se entiende sin la toma de decisiones sobre ciberseguridad, ni tiene sentido, ni nos llevará al éxito y resultados que esperamos; llevar a sus últimas consecuencias un proceso de transformación digital pone a las empresas en riesgo, por la alta dependencia que tiene el negocio de las tecnologías, la gestión de ese riesgo debe abordarse con firmeza.

- Cuando las organizaciones empiezan a detectar que están en una situación de alta dependencia respecto de las tecnologías, aparecen los temores de que los sistemas y las tecnologías no cumplan con su misión a causa de los incidentes de seguridad, particularmente se ven afectadas aquellas organizaciones que basan toda su actividad de negocio en las tecnologías de la información y en el manejo o tratamiento de información, no pueden permitirse fallos de seguridad.
- El proceso de transformación digital debe apoyarse en un escenario en el que la ciberseguridad ha sido tenida en cuenta desde el primer momento, de otro modo, la toma de decisiones tardías puede afectar a los resultados en tiempo y forma.
- Se puede afirmar que el proceso de transformación digital que no vaya acompañado de decisiones en materia de ciberseguridad fracasará,

ya que el extensivo e intensivo de las tecnologías que implica la transformación digital es una fuente de riesgo, que va a generar amenazas de todo tipo.

- La ciberseguridad precisa ser abordada de forma ordenada, sin improvisaciones, por tanto deberemos llevar a cabo: la planificación de la seguridad, la implementación de los procedimientos de seguridad, la gestión de la seguridad y el control y la verificación del nivel de seguridad de los sistemas y tecnologías a la información.
- La ciberseguridad es un proceso estratégico, que debe alinearse con los objetivos de negocio sin perder de vista su objetivo operativo: proteger los activos de información.

Todo el proceso de transformación digital, incluyendo las decisiones en materia de ciberseguridad, va a verse impactado por la regulación, en particular en lo que se refiere al tratamiento de datos. Por tanto, la componente jurídica deberá ser tenida muy en cuenta en la toma de decisiones, y esa presencia del asesoramiento y apoyo jurídico especializado, debe articularse desde el mismo momento en que se plantea el proceso de transformación digital, para no encontrarnos posteriormente con serias dificultades de orden legal que retrasen o impiden alcanzar que nuestra organización sufra los cambios necesarios para transformarse digitalmente.



Referencias bibliográficas

1. Cotino, L., (2023). *La digitalización en las administraciones públicas en España.* Recuperado de https://fundacionalternativas.org/wp-content/uploads/2023/10/DIGITALIZACION_ADMIN_PUBLICAS.pdf

2. Schwab, Klaus. (2016). *La cuarta revolución industria*"; ISBN: 9788499926940

3. Villar, J. y Mendoza, C. (2023). *Impacto de la transformación digital en España: 1998-2023.* Fundación Orange. Recuperado en https://fundacionorange.es/25a/informe/Informe-25a.pdf

4. CPAL. (2022). *Acceso y uso de internet en América Latina y el Caribe. resultados de las encuestas telefónicas de alta frecuencia de ALC 2021.* Recuperado en https://www.undp.org/sites/g/files/zskgke326/files/2022-09/undp-brlac-Digital-ES.pdf

5. Comisión Europea. (2023). *Informe del estado de la Década Digital en Europa.* Recuperado en https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade

6. Patiño, A. et al. (2022). *Datos y hechos sobre la transformación digital.* Recuperado en https://www.cepal.org/sites/default/files/publication/files/46766/S2000991_es.pdf

7. Three Points,The School for Digital Business. (2021). *Think Digital Report 2021.* Recuperado en http://crm.threepoints.com/comunicacion/prensa/ThreePoints_Think_Digital_Report_2021_ResumenEjecutivo.pdf

8. Parlamento Europeo. (2023). *Ciberseguridad: amenazas principales y emergentes.* Recuperado en:

9. https://www.europarl.europa.eu/pdfs/news/expert/2022/1/story/20220120STO21428/20220120STO21428_es.pdf

10. Oficina Europea de Policía (Europol). (2016). *Internet Organised Crime Threat Assessment*., Recuperado en: https://www.europol.europa.eu/cms/sites/default/files/documents/europol_iocta_web_2016.pdf

11. Ministerio del Interior del Gobierno de España. (2022). *Informe sobre la cibercriminalidad en España.* Recuperado en https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2021_126200212.pdf

12. Díaz, R. y Núnez, G. (2023). *Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe.* Recuperado en: https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content

13. Parlamento Europeo. (2022). *Informe sobre Inteligencia Artificial en la Era Digital.* Recuperado en: https://www.europarl.europa.eu/cmsdata/246872/A9-0088_2022_EN.pdf

OBS Business School

School of **Business Administration & Leadership**

School of **Innovation & Technology Management**

Planeta Formación y Universidades