Digital Security en la nueva era de transformación digital

Gianluca D'Antonio | Socio de Risk Advisory de Deloitte | @infosecadvocate

Miguel Olías de Lima Pancorbo | Manager responsable de Cyber Strategy Transformation and Assessment de Deloitte.

Tema

La transformación digital obliga a redefinir el concepto de ciberseguridad para asegurar que los nuevos elementos no asociados a las tecnologías de la información tradicionales (core IT) quedan recogidos en el enfoque más amplio de la Seguridad Digital.

Resumen

La transformación digital aporta un gran avance a la sociedad con la aparición de nuevas tecnologías y dispositivos digitales de todo tipo como *smart things,* ciudades inteligentes, *smart-grids,* coches autónomos, robótica, inteligencia artificial, la propia nube, el Internet de las Cosas (IoT) o el Internet Industrial de las Cosas (IIoT), entre otros. Todas estas tecnologías pueden ser interoperables y permiten a los usuarios experimentar nuevas experiencias haciendo desaparecer las barreras entre el mundo físico y el mundo digital.

No obstante, la era de la transformación digital conlleva una serie de nuevos riesgos digitales que tienen un impacto mayor que cualquier otro de los que se cometen a través de Internet porque empieza a ser plausible causar daños físicos a distancia. Para evitar lo que podríamos definir como *digital chaos,* se necesita redefinir la ciberseguridad para que se aproxime a la seguridad digital, puesto que la ciberseguridad tradicional, tal y como la entendemos, no es capaz de cubrir las necesidades de seguridad que implica este nuevo paradigma de transformación digital. En este ARI se analizarán los factores de éxito de la transformación digital, los principales riesgos digitales, algunos casos de incidentes ya conocidos o vulnerabilidades encontradas, así como una primera aproximación a los aspectos claves de la seguridad digital que hay que tener en cuenta para su desarrollo.

Análisis

¿Cómo hemos llegado a la era de la transformación digital y cuáles son los nuevos retos desde la perspectiva de seguridad?

La revolución 4.0, ligada a la transformación digital, ya está presente tanto en el entorno personal como profesional, con una clara evolución convergente entre los dos entornos. Antes de entrar en su análisis, es necesario echar un vistazo atrás para ver cuál ha sido la evolución de la tecnología en estos años y dónde ha estado en cada caso el foco desde la perspectiva de seguridad.

Inicialmente, se crearon los primeros sistemas informáticos centralizados y formados por un hardware y software básicos, cuya misión era el almacenamiento y procesado de información. La casi totalidad de sus interacciones hacia el exterior (usuarios) se realizaba a través de periféricos (normalmente integrados) y de acceso físico al hardware, es decir, sin ningún tipo de conexión hacia otros sistemas a través de redes. Posteriormente, se desarrollaron las redes de telecomunicaciones, Internet y otras redes privadas, que permitieron a esos sistemas comunicarse con otros, realizar procesamiento distribuido en la red e interactuar de forma coordinada. Estas redes no fueron diseñadas pensando en la seguridad, motivo por el cual, resultaba necesario focalizar la seguridad en el perímetro y administrar de forma correcta las redes, en prevención de intrusos. Con esto se ha intentado evitar, por ejemplo, ataques *man-in-the-middle.*

Tras el *auge* de Internet, se desarrollaron las relaciones a través de la red, en una época conocida como la *era de la información*, donde la seguridad se centró en la privacidad de la información, más allá de la seguridad del perímetro, mediante regulaciones como la antigua Ley Orgánica de Protección de Datos (LOPD) en España[1].

La posterior *era de la movilidad* llegó con la aparición de los teléfonos móviles (*smartphones*) que permitían a los usuarios de Internet acceso 24/7 a todo tipo de servicios, sin necesidad de estar en sus domicilios. Gracias a esto se desarrollaron los sistemas de pago online, las redes sociales, el consumo de contenido vía *streaming* multidispositivo o la virtualización e interoperabilidad de aplicaciones y sistemas, entre otros, permitiendo al usuario acceder desde cualquier plataforma a cualquiera de sus contenidos gracias a la nube. En contrapartida, la ruptura total del perímetro de las organizaciones y administraciones públicas planteó a estas el reto de la ciberseguridad tal y como hoy la conocemos. Las organizaciones y empresas tuvieron que enfrentarse a las ciberamenazas de mayor impacto potencial, desarrollar medidas de control de los datos o en las infraestructuras que pueden -incluso- no pertenecer a la propia compañía, disponer de servicios de monitorización continua de sus sistemas y amenazas externas como son los denominados centros de operaciones de seguridad (Security Operations Centre, SOC) y equipos de respuesta (Computer Security Incident Response Team, CSIRT), o la necesidad de estar preparado ante cualquier evento disruptivo a través de la denominada ciberresiliencia. Todas estas nuevas estructuras de ciberseguridad están encaminadas a proteger, prevenir y gestionar los ciberfraudes, las fugas de información, los denominados *ransomwares* (secuestro de los dispositivos), ataques de denegación de servicios (DoS) y denegación de servicios distribuido (DDoS), suplantación de identidad y ataques a la reputación, entre otros.

El nivel de madurez de empresas y administraciones públicas en materia de ciberseguridad es actualmente bajo. En la mayoría de ellas, las medidas suelen ser *ad-hoc*, poco definidas y reactivas y solo unas pocas organizaciones, consiguen alcanzar niveles razonables de madurez, gestión y optimización de su ciberseguridad. La madurez es mayor en las empresas que pertenecen a sectores muy regulados como son las entidades financieras y telecomunicaciones, donde la presión por el

[1] Ley Orgánica 15/1999 de Protección de Datos de carácter personal, de 13 de diciembre, https://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf.

cumplimiento regulatorio ha obligado a estas organizaciones a invertir mayores recursos para hacer frente a sus necesidades de ciberseguridad. Por el contrario, presentan un nivel de madurez insuficiente aquellos sectores productivos donde prevalece la tecnología de las operaciones (OT).

La IT y OT pertenecían a "mundos" diferentes e inconexos, pero han comenzado a converger con la aparición del Internet de las cosas (Internet of Things, IoT) y el Internet industrial de las cosas (Industrial Internet of Things, IIoT), por lo que infraestructuras que hasta ahora estaban al margen de la ciberseguridad tienen ahora que ocuparse de ella. Regulaciones como la Ley PIC[2] en España o la Directiva NIS[3] en Europa ayudan, pero no garantizan la implantación de medidas reales y prácticas ante el nuevo escenario de ciberamenazas.

Mientras las organizaciones se estaban adaptando al nuevo escenario de riesgos, éste ha mutado de la mano de la digitalización y ahora, independientemente del nivel de madurez de ciberseguridad alcanzado, deben afrontar un cambio de paradigma por la transformación digital representada en la Figura 1. La era digital tiene como principal componente la ruptura de la barrera del mundo físico y el mundo lógico o digital. La aparición, por ejemplo, de los *wearables* permite a las personas llevar consigo más dispositivos que los propios teléfonos móviles. Estos nuevos dispositivos no solo se encuentran en formato de relojes inteligentes, sino que están alrededor de nuestra vida en diferentes ámbitos como el de la salud que cuenta, por ejemplo, con marcapasos digitales o bombas de insulina con administración remota. En los hogares aparecen neveras y televisores inteligentes, aspiradoras autónomas, básculas digitales con conectividad wifi o bluetooth, asistentes del hogar (por ejemplo, Amazon Echo, Google Home, etc.), termostatos inteligentes (Google Nest), drones, etc. Al mismo tiempo, la industria 4.0 ya ha llegado a las ciudades y los ciudadanos pueden interactuar con las grandes urbes gracias a su transformación en *smart cities*, etc.

[2] Ley 8/2011 de Protección de Infraestructuras Críticas (https://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf) complementada por el Real Decreto 704/2011 (https://www.boe.es/buscar/pdf/2011/BOE-A-2011-8849-consolidado.pdf).

[3] Directiva 2016/1148 sobre seguridad de las redes y sistemas de Información de la Unión, de 6 de julio, https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=ES.

Figura 1. Evolución de la transformación digital

Fuente: Deloitte Cyber Strategy.

La transformación digital obliga a redefinir el concepto de ciberseguridad o, al menos, a identificar las nuevas áreas donde no llega la ciberseguridad tradicional. Día a día se comprueba la necesidad de asegurar ciertos elementos no asociados al mundo de las tecnologías de la información (IT), fuera de la capa de software y datos como los protocolos *machine-to-machine*.

La transformación digital nos trae el Internet de todo (IoT) y entraremos en una nueva era de riesgo digital global. Para mitigar este riesgo, debemos desarrollar un nuevo enfoque holístico de la seguridad, donde se integren lo físico y lo virtual, lo humano y la máquina. Este enfoque que Gartner denomina *Digital Security* es la respuesta conceptual a los desafíos que plantea el avance tecnológico en todas las dimensiones de riesgo. El uso de una tecnología invasiva en todos los aspectos de la actividad humana genera nuevas interdependencias no evaluadas hasta ahora desde la perspectiva de la protección de las personas, medio ambiente (*safety*).

La Seguridad Digital se enfrenta a nuevos retos de ciberseguridad para los dispositivos inteligentes, la robótica, la computación en la nube o la inteligencia artificial, entre muchos otros. Incorpora aspectos como la privacidad, la ética y la resiliencia, más complejos que los que se abordan en las tecnologías de operaciones (OT), de información (IT), del Internet de las cosas (IoT) o de la seguridad física en general. La transformación digital llevada a cabo en las empresas cambia el paradigma tradicional de la seguridad debido al riesgo de alteración de los elementos inteligentes que acompañan a la economía digital si no se reúnen unos atributos mínimos de seguridad. El concepto de Seguridad Digital constituye, en sí mismo, un cambio de visión necesario para la seguridad de las empresas porque deben incorporar el riesgo de los entornos físicos dentro de los procesos de análisis de riesgos tecnológicos. Por este motivo, debemos tener en cuenta que la Seguridad Digital es el resultado de aplicar la gestión de riesgos a todos los elementos de la transformación digital:

Seguridad Digital = Transformación Digital x Gestión del Riesgo Digital.

Para asegurar la confianza digital en un mercado donde interactúan clientes, socios y trabajadores, las empresas deben afrontar este nuevo reto: la gestión del riesgo digital, con la vista puesta en desarrollar las capacidades que la Seguridad Digital demanda.

Entendiendo el nuevo escenario de amenazas que conlleva la era digital

Los medios son el gran elemento disruptivo en la era de la transformación digital. Mientras que en el pasado los medios capaces de producir daños se reducían a unos pocos dispositivos como los ordenadores, servidores, redes de telecomunicaciones y últimamente los teléfonos móviles, hoy en día la lista crece significativamente. Entre ellos podemos incluir, entre otros, los drones, la robótica en general y los dispositivos IoT, los asistentes digitales y la inteligencia artificial (con independencia del medio en el que se encuentre), los *smart things*, las infraestructuras críticas, los servicios esenciales, servicios en la nube o las redes sociales.

Los actores también cambian, porque quienes más pueden poner en peligro la seguridad digital no son, como antes, *hacktivistas*, hackers individuales o empleados internos, sino cibercriminales organizados, otras naciones y otras empresas[4]. Para hacerlo, utilizarán nuevas técnicas como la explotación de vulnerabilidades en los sistemas, la explotación de redes vulnerables, la ingeniería social, el *spoofing* de usuario, la denegación de servicio, malware, escuchas, errores no intencionados, las amenazas avanzadas persistentes (Advanced Persistent Threats, APT) o la concesión excesiva de privilegios o accesos, entre otras. Estas técnicas pueden ocasionar daño económico, extorsión, daño reputacional, destrucción de activos, toma de control de sistemas, alteración de procesos, espionaje o interrupciones de servicio.

Muchas de las amenazas tradicionales pueden presentarse ahora con mayor frecuencia e, incluso, causar daños a la integridad física de las personas. La pérdida de fronteras entre el mundo digital y el mundo físico puede hacer que un simple clic o un *script* acabe con nuestra vida, ya el actor que genera la amenaza dispone de nuevos medios para realizar un ataque. Se producen nuevas combinaciones de riesgo para la seguridad digital (hibridas) como, por ejemplo, que un terrorista cause daño en la integridad física de otro país explotando las vulnerabilidades de un sistema IIoT a través de las infraestructuras críticas del país como, por ejemplo, una depuradora de agua. O que una organización criminal extorsione y espíe a un político o directivo haciendo uso del dispositivo móvil de la víctima, su aspirador inteligente, su asistente virtual del hogar y extrayendo información a través de sus redes sociales y otra información disponible en nubes de información no seguras.

Pasando de la prospectiva al presente, se pueden plantear varios escenarios de riesgo que evidencian la llegada de la seguridad digital. Actualmente, se están incorporando juegos/retos digitales basados en inteligencia artificial a través de los cuales las

[4] "Threat Landscape Report 2017, 15 Top Cyber-Threats and Trends" ENISA, 2018, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

empresas son capaces de definir un patrón psicotécnico del candidato. Por ejemplo, mediante el software Pymetrics de IA que mide la creatividad en la resolución de problemas, la tolerancia a la frustración y la perseverancia, entre otros; un proceso automático se usa en el 38% de las multinacionales y que el 68% espera hacerlo en el medio plazo[5]. Si toda esa información se asociase dentro de la misma nube, ¿le sería posible a una persona catalogada como no apta presentarse a una entrevista en otra empresa sin ser rechazada automáticamente? ¿cómo se garantiza que no se use la información de nuestro perfil psicotécnico en nuestra contra?

La policía británica quiere predecir un delito antes de que se produzca, haciendo uso de la estadística y la inteligencia artificial, a través de un sistema denominado *National Data Analytics Solution (NDAS)*. Esto lo haría centralizando la información y explotándola con algoritmos de IA de hasta ocho fuentes diferentes de los archivos de la policía. Tras identificarse a un criminal potencial, el objetivo sería ofrecerles apoyo de los servicios sociales y asesoramiento. Sin lugar a duda sería un gran avance en la prevención de crímenes y delitos, pero ¿qué riesgos puede generar que la policía mantenga etiquetados/catalogados a los ciudadanos como potenciales delincuentes? ¿qué ocurriría si esta información se hiciese pública y todo el mundo pudiera ver si su vecino es o no es un potencial delincuente?

En un escenario más próximo, las aspiradoras inteligentes generan mapas exactos de nuestras casas, así como el reconocimiento por voz y cámara en las unidades más modernas. Toda esa información, ¿dónde se almacena? ¿para qué se usa? ¿acabará siendo pública? Al igual que en el caso anterior, otros dispositivos como son los asistentes virtuales están recogiendo información 24/7 sobre las conversaciones que se mantienen en las casas de sus usuarios. Estos dispositivos ya se admiten en los tribunales como medios de prueba, pero ¿y si se explotara esta información contra los propios usuarios?

El número de escenarios plausibles podría aumentar más allá de los límites de este análisis. Un grupo de hackers demostró en la DEF CON cómo se puede lanzar un *ransomware* contra un termostato inteligente, subiendo la temperatura a la máxima temperatura hasta que no se pagase un rescate en una cuenta de *bitcoin*. Amazon retiró unos ositos de peluche inteligentes, CloudPets, del fabricante Spital Toys, porque podían espiar a sus usuarios, los niños. Estos son solo algunos ejemplos que facilitan el entendimiento del nuevo panorama de riesgo digital que viene de forma directa de la transformación digital.

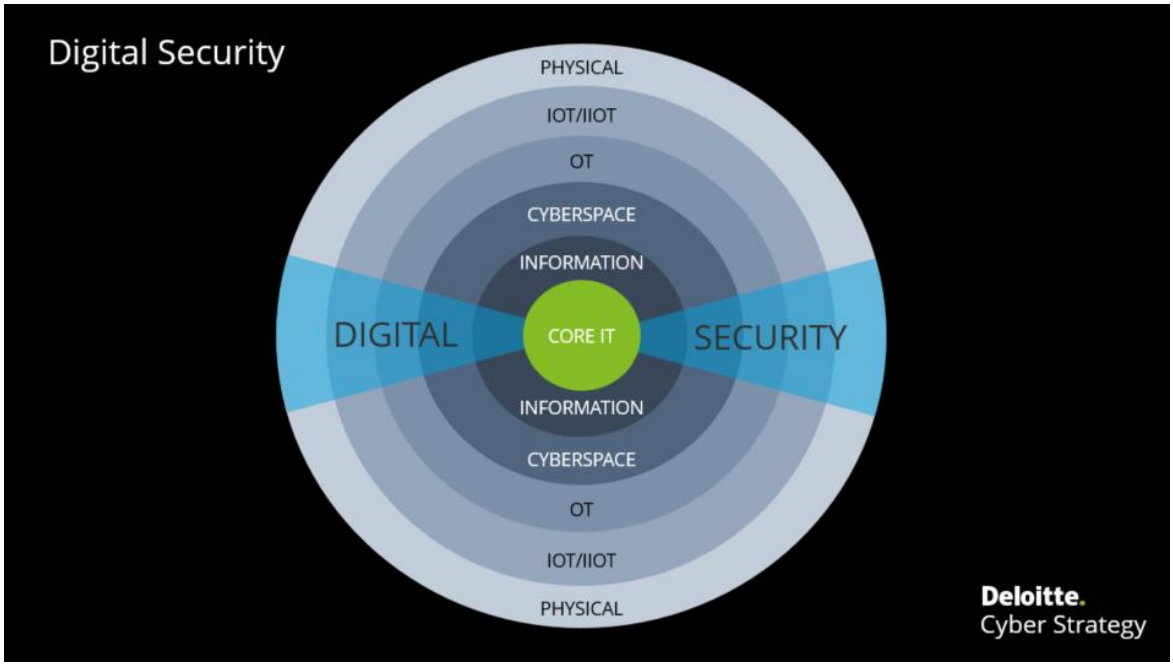
Digital Security para hacer frente al riesgo digital

Para hacer frente a los distintos elementos que conforman el riesgo digital, la seguridad digital constituye el núcleo de las respuestas, tal y como refleja la Figura 2. En la actualidad se dispone de algunas normas que pueden contribuir a la seguridad digital como las mencionadas sobre protección de datos, infraestructuras críticas o redes y

[5] Informe de “Tendencias Globales de Capital Humano 2018”, Deloitte, https://www2.deloitte.com/cl/es/pages/human-capital/articles/cl-tendencias-globales-capital-humano-2018.html.

sistemas de información, pero ninguna está enfocada específicamente a la transformación digital. La futura regulación debería atender a los nuevos dispositivos inteligentes, incluir en su diseño las medidas mínimas de seguridad, así como la información que se almacena, viaja, se genera y usa entre estos dispositivos y la nube. Al mismo tiempo, debería tener en cuenta el uso de infraestructuras compartidas, la complejidad de identificar por donde circula la información y trazar un *workflow* (flujo de trabajo) del mismo, así como la generación y explotación de información a través de algoritmos de inteligencia artificial. Todo ello hace realmente difícil legislar de forma práctica generando un equilibrio entre no poner demasiadas barreras al progreso, la innovación y la evolución, y controlar al mismo tiempo los riesgos derivados de todas estas nuevas tecnologías.

Figura 2. El paradigma de la seguridad digital



Fuente: Deloitte Cyber Strategy.

Legislar en materia de seguridad digital es un reto realmente complicado, puesto que, a la dificultad de abordar un problema tan complejo y tan amplio, hay que añadir la necesidad de legislar de forma global a través de un acuerdo internacional. En el momento en que las empresas y ciudadanos consumen y producen servicios y productos de diferentes países que, a su vez, proceden de distintos países, resulta necesario que la regulación mantenga una línea base mínima para todos los países. En caso de no ser así, la eficacia de las futuras normas se verá dañada por la complejidad de su cumplimiento y, en lugar de ver en el futuro una única regulación que englobe todos estos aspectos mencionados anteriormente, es probables que veamos muchas regulaciones dedicadas a áreas específicas de seguridad digital.

En referencia a los *frameworks* o estándares, si bien no hay uno que sirvan de forma directa para la seguridad digital, sí que podemos hacer uso de algunos estándares, especialmente del campo de OT e IOT/IIOT que puede asentar ciertas bases en la

seguridad digital[6]. La mayoría de estos estándares provienen de EEUU y están enfocados a la protección de infraestructuras críticas, infraestructuras de OT e IOT y del sector energía, pero ninguno de ellos cubre de forma holística los riesgos derivados de la tecnología que sustenta la transformación digital (*wearables*, IA, nube, *smart things* o *smart cities*).

Digital Security como una responsabilidad de la *Digital Transformation*

Según una encuesta de Gartner[7], las principales barreras para el desarrollo de las actividades de IoT en las organizaciones son la seguridad (28%), la privacidad (25%) y la integración de la tecnología en las operaciones (24%). Como las tres están relacionadas con la falta de seguridad digital en las fases más tempranas del diseño, si se incluyese la seguridad digital entre las responsabilidades de quienes lideran la transformación digital de las compañías, se incentivaría la presencia de la seguridad en todo el ciclo de vida de los productos y servicios relacionados, en este caso, con las actividades de IoT. No es necesario que la seguridad digital sea competencia exclusiva del departamento de transformación digital, pero sí que éste deba también rendir cuentas (*accountability*) de los riesgos digitales de las tecnologías que se impulsan desde su área de responsabilidad.

Nuevo rol en la organización y organizaciones bimodales

Como es de suponer, las empresas precisan nuevas figuras para hacer frente a los nuevos ecosistemas digitales, muchas de ellos con labores claras en relación a la seguridad digital: responsable de riesgos digitales (Digital Risk Officer, DRO), defensor de la seguridad (Security Ombudsman), técnico de seguridad de datos (Data Security Scientist, DSS), gestor del ecosistema digital (Digital Ecosystem Manager, DEM) y jefe de responsables de seguridad (Chief of Staff for Security, CSS).

Según Gartner[8], los siguientes cinco nuevos roles vienen a cubrir ciertas necesidades creadas por el cambio de paradigma y requieren de ciertas capacidades. Entre ellas destacan la adaptabilidad a los cambios, la visión del negocio, la destreza digital, la orientación a los resultados y colaborativos. El rol de un responsable de seguridad digital es el de influir en el resto de las áreas de negocio, frente al rol tradicional de un responsable de ciberseguridad que estaba orientado a la supervisión y al control. Estos nuevos roles y capacidades son claves en aquellas organizaciones bimodales, en las cuales, tanto desde la perspectiva tecnológica como de seguridad, cuentan con dos velocidades diferentes: la *tradicional*, que mantiene las infraestructuras heredadas y suele ser el *core business* de las organizaciones y la de *transformación*, que suele aplicar metodologías ágiles y para las cuales no se pueden aplicar los sistemas de control tradicionales. Estas organizaciones tienen el reto de salvaguardar la seguridad

[6] IoT Security Compliance Framework de la IoT Security Foundation, NIST CSF, ISA/IEC 62443 Standards, NERC CIP V5, Cybersecurity Capability Maturity Model (C2M2) y SP 800-82 - Guide to Industrial Control Systems (ICS) Security.

[7] "Focus More on the Realities of Cyber-Physical Systems Security Than on the Concepts of IoT", Gartner, 11/X/2018, https://www.gartner.com/doc/3891442?ref=AnalystProfile&srcId=1-4554397745.

[8] "New Security Roles Emerge as Digital Ecosystems Take Over", Gartner, 29/VI/2018, https://www.gartner.com/doc/3880667/new-security-roles-emerge-digital.

sin entorpecer la agilidad del negocio, motivo por el cual se requiere de nuevos perfiles, como los anteriormente mencionados, para hacer frente a esta realidad.

Nuevos atributos del dato y de los servicios a ser gobernados por la seguridad digital

A los atributos o dimensiones tradicionales de la seguridad: confidencialidad, integridad, disponibilidad, se deben añadir algunos nuevos en la seguridad digital. Primero, la ética debe concebirse como una premisa necesaria ante el diseño, desarrollo y operación de cualquier servicio o producto de la transformación digital. Cuando se descubre una nueva vulnerabilidad, esta debería ser reportada al fabricante o proveedor, imponiéndose la ética ante el beneficio individual (a través de *black markets*). La ética debe imponerse también a la hora de decidir cómo las organizaciones deben proteger la información que se recopila de los dispositivos digitales de sus usuarios y cuál será el uso que se hará de esta. En situaciones donde pueda generarse un beneficio económico, comercial o, incluso, el posible daño reputacional de un competidor, hay que decidir si se está actuando éticamente antes de hacer uso de la información de la que se dispone. Es necesario preguntarse acerca del origen del dato, si es ético usar esa información para sacar partido ante una situación dada y si el usuario desea realmente que se actúe de una determinada manera, aunque haya habido un consentimiento por su parte. La ética va más allá del *compliance* y, en la seguridad digital, la ética ayudará al ser humano a no generar situaciones de discriminación o prevenir el daño físico a las personas que vivirán en las ciudades del mañana.

Segundo, la trazabilidad que permite conocer el ciclo de vida del dato: su creación, modificación, uso, reposo/almacenamiento, cuando este se encuentra en movimiento y su eliminación. La trazabilidad es un atributo crítico cuando este viaja, por ejemplo, desde un *smartwatch*, a la nube pasando por varias plataformas de diferentes proveedores hasta que llega a un servidor de una empresa a través de Internet, porque en esa trayectoria se pierde el control del ciclo de vida del dato y, por tanto, resulta complicado su protección.

Tercero, la privacidad es un atributo que evita la identificación y divulgación de los datos de las personas físicas almacenada como información. En la privacidad inversa, cuando las compañías disponen de información de sobre sus clientes que ni siquiera ellos conocen debido a la información recogida por todos los nuevos dispositivos digitales junto con la IA, generan patrones e información desconocida hasta el momento por el individuo. En este caso se podría hablar de la capacidad del individuo para tomar control de los datos que se han generado sobre su persona y su libertad para cederlos e incluso venderlos para ser explotados por terceros.

Finalmente, la auditabilidad o la capacidad que tiene una organización de examinar, verificar o demostrar que no se alteran los datos y que se pueden revisar por terceros de confianza; y la seguridad física, o la protección de las personas y el medio ambiente frente a los nuevos riesgos de la automatización y la digitalización.

Inclusión del *Cyber-Physical Systems (CPS)* en el entorno completo de seguridad

El perímetro actualmente tiene tres fronteras. Una primero (*edge)* donde se conectan e interactúan los humanos, las infraestructuras físicas, la geolocalización, el tiempo y los sensores de todo tipo. Esta información es enviada a la frontera siguiente (plataforma) desde el que viajan por Internet los datos e información hacia los diferentes proveedores, normalmente en la *nube*, donde se pierde su rastro, se desconoce su uso, almacenamiento y acceso. Finalmente, esta información acaba llegando al perímetro tradicional (empresa) donde se encuentran las bases de datos, los servidores o las redes internas a través de los cuales se explota y trabaja con esta información. La seguridad digital debe contemplar estas tres fronteras en el diseño de soluciones y, además, todas las tecnologías asociadas a las mismas: servidores, redes de comunicaciones, nube, IA, IoT o IIoT, entre otros.

Conclusión

Se puede concluir que Internet no fue diseñado pensando en la seguridad, motivo por el cuál hoy en día asegurar la red no es una tarea trivial. Estamos ante un nuevo paradigma, la transformación digital, que requiere aprender de los errores del pasado y progresar hacia la seguridad digital. El nuevo ecosistema es aún más complejo que el anterior y los elementos que lo componen se multiplican, por ello, se deben dar pasos firmes para poder preservar la confianza digital y evitar que se produzcan incidentes con consecuencias irreparables como describe el experto en ciberseguridad Bruce Schneier en su obra: “Click here to kill everybody”.