En colaboración con:
Softeng

Autor:
José A. Cano

Febrero de 2020

Ciberseguridad inteligente para habilitar la confianza digital

Resumen ejecutivo

La nueva era digital está transformando no sólo la forma en que las empresas están gestionando su relación con los clientes reales, sino que también está transformando la forma en que ofrecemos servicios y aplicaciones.

En este escenario cada vez más digital en el que ya se mueven el 62% de las empresas españolas según datos de IDC, las fronteras de seguridad se difuminan y la inversión requerida para garantizar tanto la seguridad en dispositivos como de evitar fuga de datos, aumenta. El ciberterrorismo y el cibercrimen son las principales amenazas a las que las organizaciones se enfrentan en cualquiera de las industrias. Por ello, es necesario articular mecanismos de seguridad que permitan detectar, analizar y eliminar las amenazas, así como planes de actuación que establezcan con claridad qué hacer ante una brecha de seguridad.

En este escenario, la IA permite a las organizaciones automatizar de manera más eficiente el proceso de detección de amenazas, y habilitar el concepto de "confianza digital", que permita securizar el dato que generan todos los actores con los que interacciona (empleados, proveedores y clientes) con independencia del origen de este.

A lo largo de este documento trataremos de entender el impacto de la transformación digital en las empresas, la sociedad y las nuevas aplicaciones desarrolladas para atender las nuevas necesidades digitales con el más alto nivel de seguridad. Un nuevo nivel de seguridad en el que la IA juega un papel fundamental al permitir habilitar la "confianza digital" que permita a las organizaciones competir en este escenario digital y garantizar una experiencia digital segura.

En el siguiente documento se analiza:

- Cómo **será el nuevo escenario digital de seguridad que dibujará la IA** y en el que las organizaciones desplegarán sus nuevas estrategias de ciberseguridad.
- El **framework de confianza** en el que las organizaciones deben configurar su plataforma de ciberseguridad inteligente **para habilitar la confianza digital**
- La forma en la que las organizaciones están **consumiendo los servicios de seguridad** en los que la IA está participando como actor clave.

la IA permite a las organizaciones automatizar de manera más eficiente el proceso de detección de amenazas, y habilitar el concepto de "confianza digital"

- Cómo la solución y capacidades de Softeng permiten a las empresas disponer de una plataforma de ciberseguridad integral e inteligente, capaz de proteger, identificar riesgos y amenazas y reaccionar ante ellas de manera automatizada.

El escenario de seguridad cuando la IA se incorpora en las organizaciones

La convergencia de los procesos de transformación digital que las organizaciones están acometiendo en la actualidad, está llevando a estas hacia un nuevo entorno que es multicloud, donde las nuevas estrategias de posicionamiento digital alrededor del dato se erigen como la ventaja competitiva en este entorno.

En 2020, más del 90% de las organizaciones utilizará múltiples plataformas y servicios en la nube

De hecho, según datos de IDC, a finales del 2020, **el 50% del gasto de TI de las empresas europeas estará asociado al dato, y en 2023 el 80% de los ingresos provendrán de la venta de productos o servicios basados en datos**.

Por ello, este incremento de datos a manejar en cualquier escenario digital va a implicar la necesidad de no sólo de automatizar los procesos internos para poder sacar partido a los altos volúmenes de información, sino de implementar procesos inteligentes que doten de valor al dato. No hay que olvidar, que la verdadera ventaja competitiva en el escenario digital vendrá de la mano de las decisiones asociadas al dato inteligente generado con soluciones capaces de aplicar esa inteligencia de negocio.

Por ello, para lograr el objetivo de digitalización, se espera que, **en 2020, más del 90% de las organizaciones utilizará múltiples plataformas y servicios en la nube** (frente al 78% en 2019). Prueba de ello es que la inversión que las organizaciones españolas realizarán en servicios en la nube seguirá creciendo hasta 2022 a una tasa del +21,2% (CAGR).

En 20202, el 68% de las nuevas aplicaciones y servicios digitales se habrán desarrollado específicamente para un entorno cloud

En este aspecto, el área de mayor relevancia en el escenario cloud será el de las aplicaciones, que deberán ir migrando y adaptándose al nuevo escenario multicloud. Se espera que, en **2020, el 68% de las nuevas aplicaciones y servicios digitales se habrán desarrollado específicamente para un entorno cloud**.

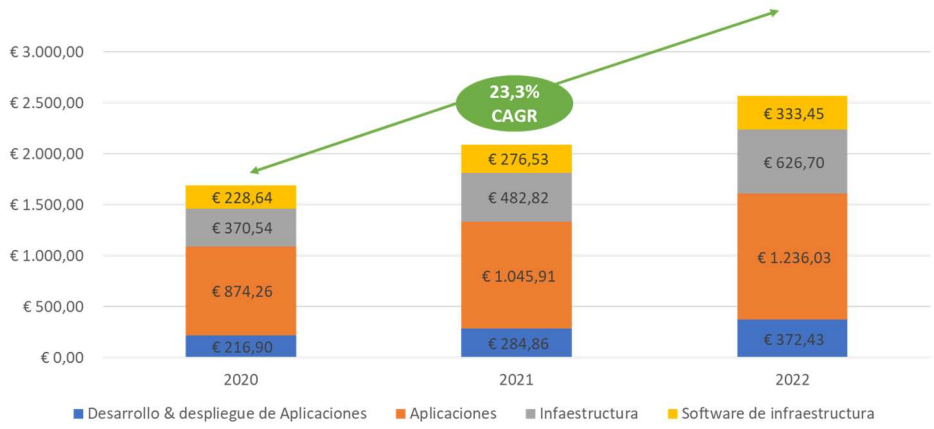

Figura 1. Inversión en servicios de nube pública en España (2020-2022). Fuente: IDC

De hecho, IDC prevé que para 2025, aproximadamente **80 mil millones de dispositivos estarán conectados a Internet (hoy 11 mil millones)**. Una persona conectada promedio en cualquier parte del mundo interactuará con dispositivos conectados casi 4.800 veces al día (una interacción cada 18 segundos).

Por ello, acorde a los datos de IDC, el 50% gasto de TI de la empresa en 2020 estará orientado fundamentalmente al dato y en 2023, el gasto de DX crecerá del **36%** actual al **50%. El mayor crecimiento se dará en inteligencia de datos y analítica,** dado que las empresas crean ventajas competitivas basadas en información, acorde a cómo se está comportando actualmente el mercado de IA en España que **crece a una tasa del 30,6% en el periodo 2020-2022**, siendo el segmento de plataformas de software cognitivo un mercado que crecerá a una tasa del 45% en dicho periodo en España.

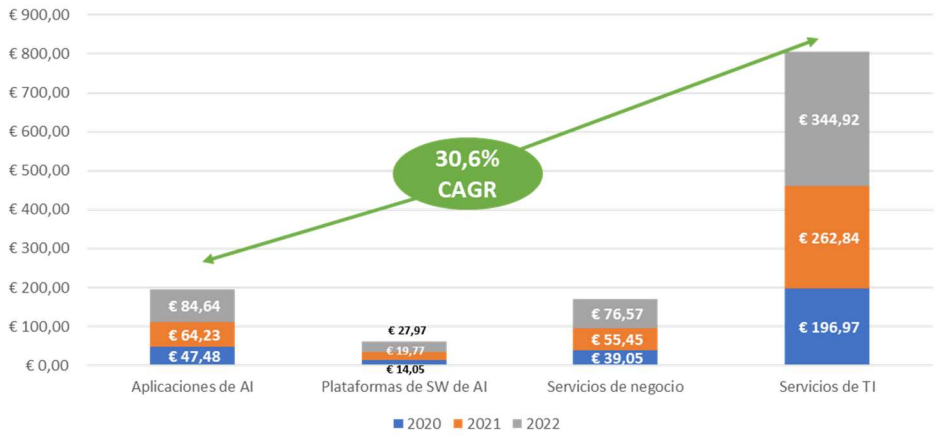

Figura 2. Mercado español de sistemas de IA en España (2020-2022). Fuente: IDC

Para afrontar este nuevo escenario, las áreas de TI de las organizaciones deben evolucionar y adaptarse a las demandas del mercado actual. Por ello, en este proceso de transformación, deben ser ágiles y por tanto más rápidas y eficientes de cara a poder maximizar la **experiencia de usuario**, ya para ello, la calidad del servicio se basa en la forma en la que se realiza la gestión del riesgo digital en la organización. En este contexto, la seguridad se erige como una de las tres prioridades de inversión en España para 2020, donde las organizaciones se están enfrentando a los siguientes desafíos:

1. **Nueva dimensión interconectada del riesgo digital**. Todas las industrias se han visto impactadas por la digitalización. De hecho, según datos de IDC, todas las industrias crecen en inversión para la digitalización en más de un 20% en el periodo 2019-2021. En este escenario las fronteras de seguridad se difuminan y la inversión en seguridad necesaria para garantizar tanto la seguridad de dispositivos como de evitar fuga de datos, aumenta. El ciberterrorismo y el cibercrimen son las principales amenazas a las que nos enfrentamos en cualquiera de las industrias. Por ello, es necesario articular mecanismos de seguridad que permitan detectar, analizar y eliminar las amenazas, así como planes de actuación que permitan establecer con claridad qué hacer ante una brecha de seguridad.

En 2025, con el aumento empresarial de la confianza digital, el 25% del gasto en servicios de seguridad se dedicará a desarrollar, implementar y mantener un "framework de confianza"

2. **Incremento del tráfico cifrado en la red.** Más del 70% del tráfico que circula actualmente por la red es tráfico cifrado, lo que el proceso de automático de amenazas requiere de la incorporación de la IA para garantizar la confianza digital requerida.
3. **Cumplimiento de las exigencias regulatorias**. La entrada en vigor de GDPR ha establecido claramente las directrices a incorporar para la gestión y protección de los datos. En este escenario, será clave determinar cómo se hará la gestión del riesgo y el cumplimiento normativo dentro de las organizaciones. En este contexto, IDC prevé que para el 90% de las organizaciones en este 2020 tendrán como prioridad incorporar la seguridad desde el diseño.
4. **Framework de confianza**. En un escenario donde el modelo de TI es híbrido (on prem con algún tipo de nube, y con múltiples servicios en la nube) y donde la experiencia de usuario es la piedra pivotal de la estrategia de la organización, la seguridad se ha desplazado a la seguridad el dato, por lo que la confianza digital es clave, hasta el punto de que según IDC, **en 2025, con el aumento de la importancia empresarial de la confianza digital, el 25% del gasto en servicios de seguridad se dedicará a desarrollar, implementar y mantener un "framework de confianza".**
5. **Evolución de la estrategia de seguridad, evitando silos y evolucionado hacia una plataforma integral de ciberseguridad**

El mercado de la seguridad en España refleja no es ajeno a esta evolución en el proceso de digitalización de las organizaciones, donde se produce un desplazamiento como comentábamos anteriormente de la seguridad hacia la seguridad del dato y específicamente, en un entorno híbrido multicloud que es donde confluirá el tráfico de datos, por lo que el consumo de los servicios de seguridad se dará a través de servicios gestionados de seguridad y de integración, tal y como muestra la figura.

El mercado de Ciberseguridad en España alcanzará los 1.381 millones de euros en 2022, lo que supone un CAGR del 6% en el periodo 2020-2022

Con un crecimiento respecto del año pasado del **5,8%, IDC prevé que alcanzará los 1.380 millones de euros en España en 2022 con un crecimiento agregado compuesto en el periodo 2020-2022 del 6%**.

Los segmentos de mayor crecimiento son los relativos a servicios gestionados de seguridad (27%), servicios de integración (25%) y los servicios de identidad y confianza digital (4%).

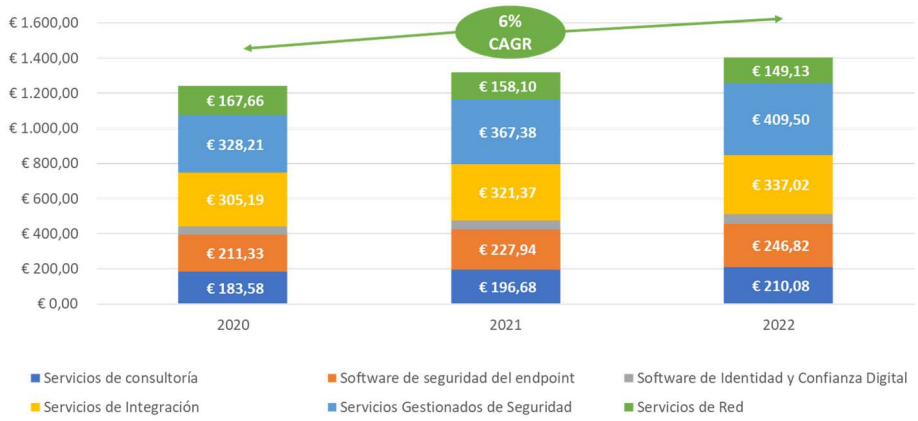

Figura 3. Inversión en seguridad en España (2020-2022). Fuente: IDC

Hacia la búsqueda de un "Framework de confianza seguro"

Las organizaciones deben evolucionar su modelo de TI hacia una plataforma digital que permita garantizar la confianza digital y habilitar la experiencia de usuario mediante el correcto tratamiento y monetización de los datos.

El concepto de framework de confianza surge como respuesta a la necesidad de dotar al modelo de TI de la organización de las capacidades necesarias para poder garantizar no sólo la seguridad del dato, sino también la confianza digital necesaria que permita a la organización poder competir en el nuevo mercado digital.

En 2025, con el aumento empresarial de la confianza digital, el 25% del gasto en servicios de seguridad se dedicará a desarrollar, implementar y mantener un "framework de confianza"

En esta plataforma de ciberseguridad inteligente, todos los elementos y dispositivos conectados deben disponer de una evaluación de riesgos que determine la necesidad y que pueda restringir el acceso dentro de sesiones o transacciones. Los datos llegan a las organizaciones a través de activos conectados, sus empleados, procesos conectados o como otros flujos de datos a través de API que se han autenticado en función del riesgo evaluado. Estos datos, que pueden cifrarse y supervisarse en busca de ataques y compromisos, circulan a través del núcleo inteligente donde se aplican los análisis de seguridad al contenido agregado, que puede extraer información de los flujos de ingresos o identificar las amenazas en curso.

Esas ideas vuelven a su organización como procesos internos mejorados, mientras que la actividad de amenazas proporciona información para endurecer el entorno y la postura de seguridad. Pero los datos también llegan a través de las interacciones de su ecosistema a través de bots autenticados, dispositivos móviles, AR/VR, vehículos conectados, etc. Estos datos, que pueden ser cifrados y monitoreados en busca de actividad maliciosa, circulan a través del núcleo inteligente, lo que convierte los datos en acciones para proteger el ecosistema a tomar cuando se interactúa con el ecosistema, tal y como muestra la figura 5.

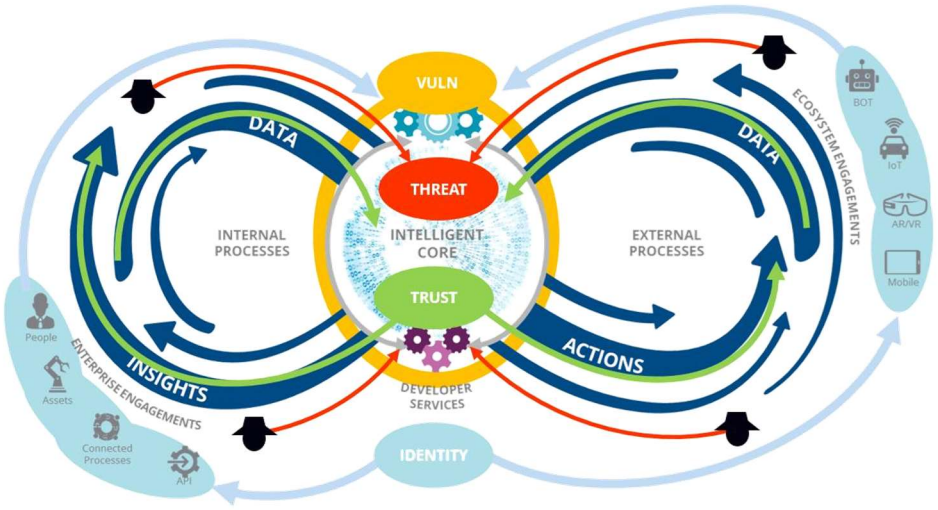

Figura 4. Framework de confianza definido para el nuevo entorno digital

Dicho de otro modo, la postura de seguridad de los activos y recursos del ecosistema se fortalece a través de técnicas de gestión de vulnerabilidades y se reevalúa y actualiza constantemente a través de procesos orquestados. Los orígenes de actividad, como los usuarios y los dispositivos, se autentican mediante credenciales que se aprovisionan y administran en función de las necesidades. Se aplican políticas adecuadas al uso de los datos y las aplicaciones. Los activos de TI aprovechan los certificados de confianza que aplican medidas criptográficas para garantizar la confidencialidad e integridad de los datos a medida que fluyen por todo el entorno. Por último, los análisis de seguridad se utilizan constantemente para evaluar el estado y la actividad en todo el entorno, identificando amenazas y otras actividades malintencionadas que se pueden abordar a través de acciones de respuesta para mantener un entorno resistente.

Conclusiones

El progresivo desplazamiento de los modelos de TI de las organizaciones al entorno cloud y el consumo de cada vez más servicios en diferentes nubes está motivando el desarrollo de productos, servicios y experiencias de usuario que están basadas en datos.

El mercado de la seguridad no ha sido ajeno a este movimiento y, sumado a la transformación del puesto de trabajo y la movilidad del empleado, está asistiendo a un cambio en la forma en la que se consumen los servicios de seguridad en las organizaciones. La importancia de la securización del dato requiere un cambio profundo en la forma en la que las empresas se enfrentan a este desafío en un entorno multicloud, donde la frontera de seguridad se difumina y el riesgo digital adquiere cada vez más importancia.

La cuantificación de este riesgo digital es la principal clave para que la organización pueda estructurar una estrategia de ciberseguridad adecuada que posteriormente pueda integrar en su plataforma digital.

La automatización de los procesos de detección automática de amenazas es otro elemento clave para garantizar la confianza digital, por lo que la incorporación de la IA como una tecnología que permitirá no sólo analizar el cada vez mayor

La complejidad de la ciberseguridad junto a la constante innovación de la nube, presentan un reto para los departamentos IT de cualquier organización.

volumen de tráfico cifrado que circula por las organizaciones, sino que incrementará la seguridad de las organizaciones, y el disponer de una plataforma integral de ciberseguridad (inteligente) donde la empresa consuma esa inteligencia a través de servicios gestionados de seguridad y servicios de integración dibujan cómo es el destino al que las organizaciones deben dirigirse para disponer de este marco de confianza necesario que permita generar y comunicar la "confianza digital" que se requiere en esta nueva década.

¿Por qué considerar a Softeng como partner de ciberseguridad inteligente?

La complejidad, el principal reto con el que topan las empresas

Aumentar el nivel de confianza digital de las empresas, vista como la percibida por clientes, proveedores y empleados sobre la protección de sus datos y privacidad, debe ser una de las prioridades de cualquier organización.

El principal habilitador estratégico del proceso de transformación digital es la nube, y la confianza digital es una característica que debe acoplarse necesariamente en esta transformación. Además, debido a que nuestros datos, aplicaciones, dispositivos e identidades están en múltiples ubicaciones, protegernos con y desde la nube, es, de hecho, la única solución viable.

No obstante, la constante innovación tecnológica que ofrece la nube en seguridad e inteligencia artificial tiene como contrapartida una complejidad, a la que a menudo muchas empresas se enfrentan solas y con extrema dificultad.

Adoptar una plataforma integral e inteligente de ciberseguridad implica no solo desplegarla sino también adaptarla a las necesidades de cada organización y posteriormente gestionarla. Estas tareas requieren de un grado de especialización relevante para evitar riesgos y acelerar los cambios de la manera adecuada, evitando así una dedicación demasiado elevada por parte de nuestros departamentos de IT.

Por todos estos motivos y dada la complejidad a la que se enfrentan las empresas, IDC recomienda establecer alianzas estratégicas con partners expertos capaces de ayudar a crear, desplegar, operar y escalar las capacidades de ciberseguridad que requieren las organizaciones.

Y en esa línea, analizamos cómo Softeng, un Partner de Microsoft especialista en acompañar a las empresas de manera segura en su viaje a la transformación digital, dispone de las capacidades necesarias para abordar y resolver los retos de seguridad que plantea este nuevo escenario de negocio.

Softeng ofrece servicios y soluciones propias basadas en la nube de Microsoft, para acoplar la seguridad que requieren las empresas en su transformación digital, de manera más simple.

La plataforma de ciberseguridad inteligente de Microsoft, simplificada por Softeng

Softeng, apoyándose en las capacidades de ciberseguridad inteligente incluidas en la plataforma Microsoft 365 y Azure, incorpora soluciones propias diseñadas para facilitar su implantación, personalización, gestión y adopción.

Concretamente, Softeng ayuda a proteger todas las superficies vulnerables de una empresa ("Identidad", "Aplicaciones", "Datos", "Dispositivos" e "Infraestructura") allí donde estén, y a tener la capacidad de validar en tiempo real cada acceso y operación a cualquier dato o recurso, detectando y reaccionando de manera inmediata ante una posible amenaza o intrusión. También, en base a toda la información recopilada en tiempo real, Softeng determina e informa a sus clientes sobre cúal es el nivel de riesgo que tienen de sufrir un incidente de seguridad en cada momento, el origen de los motivos y las acciones a realizar.

Además, partir de una plataforma de ciberseguridad inteligente y holística como la de Microsoft es clave. De este modo, las empresas evitan el típico escenario de "productos que no se entienden entre sí", lo que no sólo genera ineficiencias y una mayor complejidad (principal enemigo de la seguridad), sino también una gran dedicación por parte de TI para revisar múltiples consolas, correlacionando eventos de alertas de distintos productos y fabricantes.

Softeng aborda los retos de las empresas en materia de ciberseguridad globalmente mediante su metodología Softeng ZeroTrust, a partir de servicios gestionados y herramientas propias e innovadoras incluidas en:

Portal Softeng CSP: Automatiza tareas de gestión de la nube de Microsoft, proporcionando recomendaciones e indicaciones sobre el estado de la seguridad, cómo mejorarla y cómo actuar en caso de amenazas concretas.

Softeng cuenta con la certificación Microsoft Gold Security, siendo hasta el momento uno de los pocos partners que ha logrado conseguirla.

Figura 5. Portal Softeng CSP

Minerva: Aplicación integrada en Microsoft Teams, que impulsa a las personas de su organización para trabajar en la nube de Microsoft de manera productiva y segura, desde cualquier lugar y mediante cualquier dispositivo.

Figura 6. Aplicación Minerva integrada en Microsoft Teams

IDC SPAIN

Serrano 41, 3ª
28001 Madrid
+34 91 787 21 50
Twitter: @IDCSpain
www.idcspain.com

Acerca de IDC

International Data Corporation (IDC) es el principal proveedor global de inteligencia de mercado, servicios de consulta y acontecimientos para la tecnología de la información, telecomunicaciones y mercados de tecnología de consumo. IDC ayuda a los profesionales de Tecnologías de la Información, ejecutivos de negocio, la comunidad inversionistas toman decisiones basándose en hechos sobre compras de tecnología y la estrategia de negocio. Más de 1100 analistas en IDC proporcionan experiencia global, regional, y local sobre la tecnología y oportunidades de industria y tendencias en más de 110 países por todo el mundo. Durante más de 50 años, IDC ha proporcionado informaciones estratégicas para ayudar a nuestros clientes a alcanzar sus objetivos claves de negocio. IDC es una filial de IDG, líder en los medios de comunicación de tecnología, investigación de mercados y eventos.

Acerca de SOFTENG

Softeng es una consultoría e ingeniería de software cuya misión es ayudar a las empresas a incrementar su ventaja competitiva optimizando sus sistemas, mejorando su productividad e impulsando la innovación. Para ello, acompaña a sus clientes con seguridad en su transformación digital mediante soluciones modernas en el cloud de Microsoft, avaladas mediante numerosas certificaciones, casos de éxito y reconocimientos importantes como: Mejor partner del año en España "Cloud Excellence 2016", finalista mundial en los "Partner of the Year Awards 2017" y al "Mejor partner de servicios gestionados 2018" en España.