IN
DUS
TRIAL
bites Ebook-3

Ciberseguridad

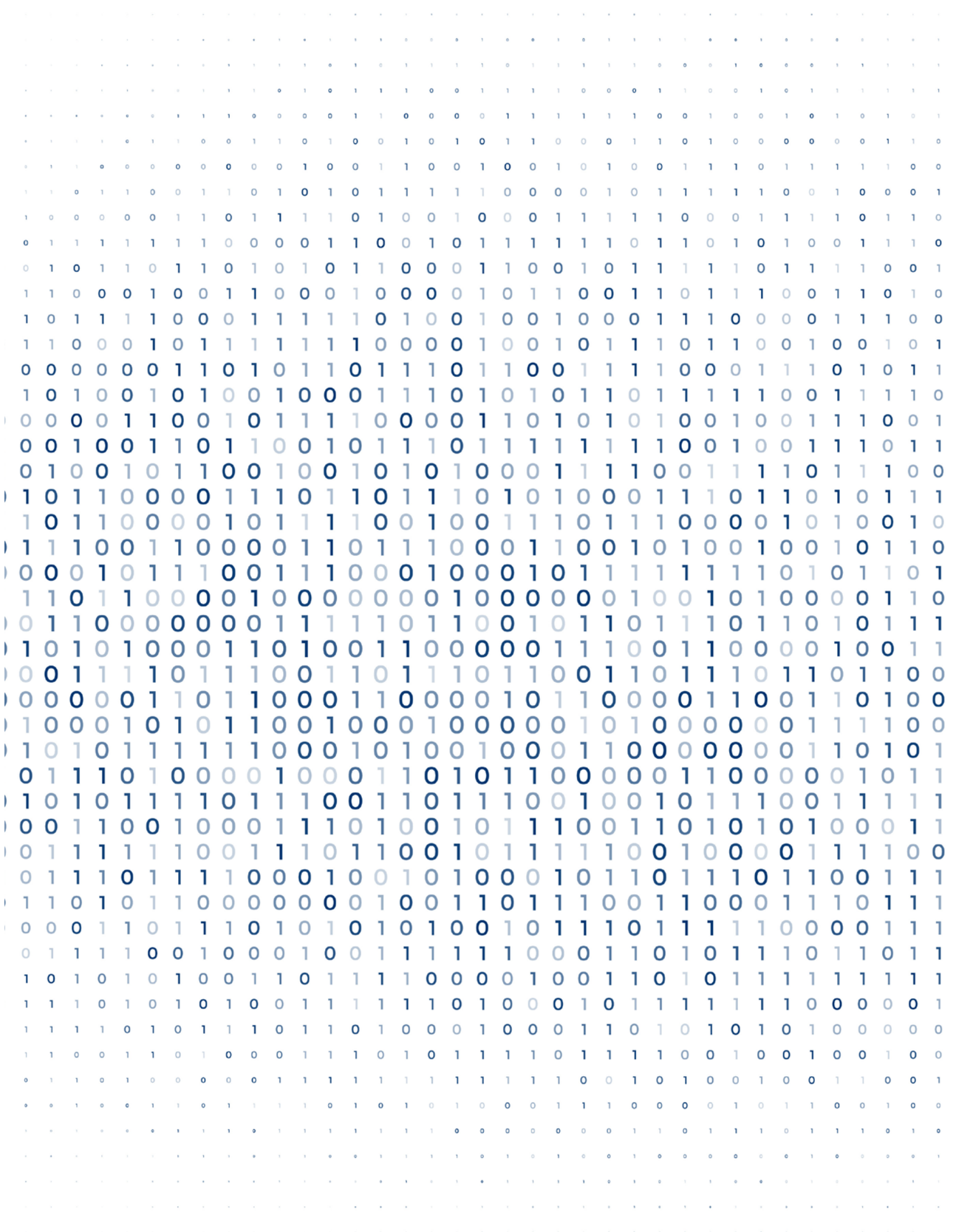
bigD

bigD
Design
that matters

La seguridad, tan importante como el dato.

A medida que la industria se conecta, la seguridad digital se desconecta. Cuanto más dispositivos en el IoT, más arquitecturas y tecnologías entren en juego, la ciberseguridad acabará siendo una cuestión de Estado o lo que es lo mismo, de comité de dirección.

Los datos nos avanzan que el 90% de las organizaciones apenas disponen de expertos en ciberseguridad, el 82% no actualiza los registros digitales que deben de proteger y el 55% dispone de un Centro de Operaciones de Ciberseguridad para detectar y contrarrestar ciberataques, según el informe Madurez Digital en Ciberseguridad de Minsait y SIA (2021).



«Según un informe reciente de Frost & Sullivan y de Ricoh, el 90% de las empresas a nivel mundial han sido vulneradas en los últimos 10 años. Un dato nada desdeñable».

Si la ciberseguridad es una tendencia, la ciberdelincuencia la acompaña y sigue en aumento. Si en España se produjeron 133.155 incidentes entre 2019 y 2020, en 2021 lejos de reducirse, los ciberataques en España han seguido incrementándose, un 26% respecto al año anterior según Deloitte.

Los ciberataques son nuestro enemigo a batir, y cuanto antes nos demos cuenta de ello, un nuevo futuro se abrirá ante nosotros.

Debemos de saber que la seguridad del dispositivo es lo más importante porque es el eslabón más débil de la cadena y por tanto, el más accesible. Y es que tenemos y debemos cambiar nuestra percepción de la realidad. La gran mayoría de los usuarios de IoT integran tecnologías emergentes y es una gran apuesta pero también una

apuesta a ser vulnerables si no somos conscientes de que necesitamos protegernos.

Por ejemplo, el 5G por diseño aporta seguridad y privacidad, lo cual nos ayudará a estar protegidos aunque no será suficiente, tendremos que poner todos los medios disponibles para evitar los ataques desde todos los puntos de la cadena.

Según Microsoft en su encuesta «IoT Signals»: el 50%, aproximadamente, de empresas que han adoptado IoT están preocupados por la privacidad de datos, el 40% por la seguridad de la red y menos del 40% están preocupados por la seguridad del dispositivo.

La seguridad cognitiva promete revolucionar la ciberseguridad porque aúna las tecnologías de redes neuronales, la Inteligencia Artificial y el Big Data y las integra junto con las soluciones de seguridad convencionales.

La ciberseguridad será un trabajo de todos, de equipos y de esfuerzo transversal entre empresas.

«Comunicarse y entenderse son operaciones que van más allá de lo intelectual».

2 Biometría

De la ciberseguridad autoimpuesta al reconocimiento facial, aunque ya no nos recozamos ni a nosotros mismos en el espejo. Últimamente la llegada o la aplicación de tecnologías en ámbitos nunca imaginados superan con creces los vaticinios de Nostradamus.

Pero no nos desviemos de lo importante, la biometría y su percepción. Existen muchas ideas sobre la biometría, pero lo que no se pueden negar son sus usos y beneficios para evitar ciberataques.

Según un nuevo informe del Foro Económico Mundial (WEF), los datos robados aumentó un 151% en 2021. Pero aquí es donde entra en juego la biometría,

ya que es la solución más fiable para verificar la identidad a diferencia de los tokens tradicionales. El propósito es crear mecanismos eficientes de ciberseguridad que no permitan a los delincuentes digitales realizar robos de identidad o fraudes.

De hecho, las empresas europeas aumentarán su gasto en sistemas biométricos a cierre de 2022 en un 20%, hasta los 3.300 millones de euros. Y aunque la biometría tiene que hacer frente a algunos retos, como la privacidad, seguridad y la posibilidad de sesgos, el 59% de las compañías ya la utilizarán en 2023 según la consultora IDC.

Desde Veridas comparten esta visión de seguridad y nos dicen que:

«cuando utilizamos nuestra biometría de manera voluntaria, cuando las personas queremos hacerlo, nos estamos protegiendo y además tenemos una mejor experiencia y facilidad de acceso a trámites o gestiones que jamás podríamos hacer».

Además, puntualizan que:

«Las tecnologías biométricas facial y de voz son ya disruptivas en sectores como el financiero, las telecomunicaciones, el de la educación o la salud».

Las ventajas que nos ofrece la biometría son muchas. Tanto las organizaciones como las personas confían en este tipo de validaciones por su seguridad, ya que los datos son mucho más difíciles de falsificar o robar en comparación con los métodos basados en tokens o contraseñas comunes.

En almacenaje, no ocupan mucho espacio y se pueden guardar en cualquier sistema de almacenamiento. Aunque quizás el coste sí que es algo más alto, su mantenimiento no lo es tanto y merece la pena invertir en este tipo de seguridad que invertir en recuperar datos robados. Es decir, es un sistema, fácil de usar e intransferible.

Obviamente, la biometría también puede ser susceptible de ser atacada por los ciberdelincuentes y romper los sistema de seguridad, pero al ser un método de autentificación que sigue innovándose, se reducen considerablemente las posibilidades de sufrir algún delito cibernético.

La inmensa realidad de 'lo virtual' se está integrando con la irrealidad de 'lo natural', quizás algún día la inteligencia artificial haya vencido a la inteligencia humana e internet con su Web 3 o el Metaverso será el centro pero mientras, está claro que debemos de proteger los datos y todo aquel dispositivo que sea susceptible de ser atacado.

«La desconfianza es la madre de la seguridad».

Aristófanes

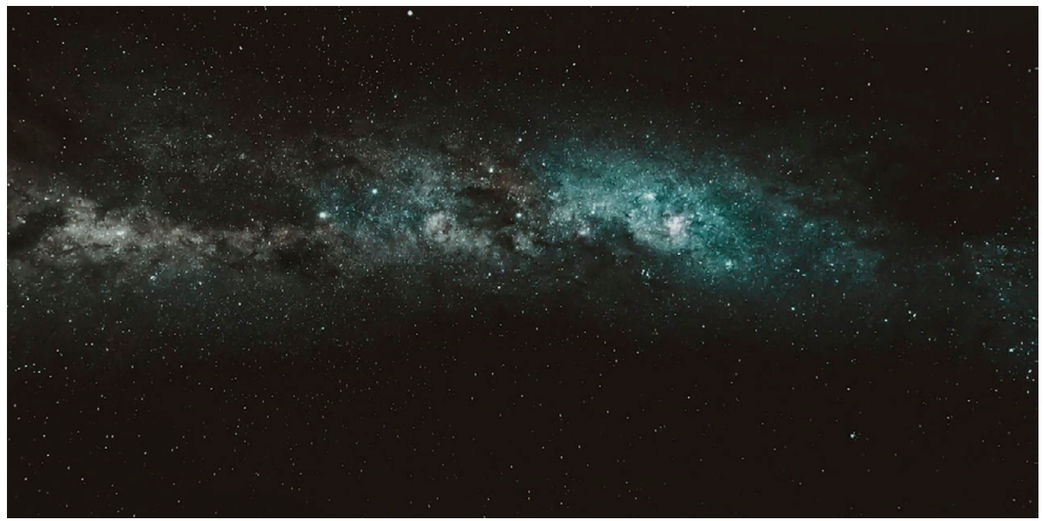
3 El Metaverso o la seguridad en el *verso*

El próximo escenario es el Metaverso, el espacio digital con posibilidades infinitas en el universo (verso). El Metaverso o el multiverso de Marvel, no sabemos hasta dónde llegarán las posibilidades e incluso las de la Web3 pero está claro que la ciberseguridad es uno de los pilares clave.

La seguridad en el Metaverso o en cualquier otra nueva tendencia o tecnología será parte del éxito. Nos prometen interacción y eso significa acceso y datos. Tanto la Web3 como el Metaverso emplean tecnologías que se basan en el Blockchain y gracias a ello, se pueden generar las criptomonedas o los NFTs o como método seguro para el inicio de sesión o identificación del usuario.

Desde el punto de vista industrial, lo que empezó con diseños digitales sencillos ha evolucionado hacia entornos cada vez más inmersivos en los que las simulaciones de procesos que nos permiten la interacción entre robots y avatares humanos digitales es lo más común. Ahora imaginemos que estamos trabajando en la industria conectada. Tenemos nuestro avatar junto con los «nuevos gemelos digitales» o lo que es lo mismo, nuestra maquinaria en el Metaverso a nuestro alcance, como nunca antes. Pero de repente, sorpresa, nuestro avatar se ha independizado y está gestionando la maquinaria. ¿Imaginas que suplantan tu identidad en el Metaverso? Si ya no teníamos suficiente con la realidad, encima nos «roban» al avatar.

Pues puede ocurrir, pero he aquí donde la industria y las empresas tecnológicas están poniendo el foco. Tanto con las nuevas tecnologías como el 5G, que ya nacen prediseñadas para ser seguras, como el uso de la biometría que está a la cabeza de los sistemas de identificación



más seguros se aúnan para que casi se un «sistema invencible».

Dicho esto, trabajar en entornos digitales, por ejemplo desde el Metaverso, nos va a aportar una visión y un margen de maniobra muy amplio. ¿Quién no quiere adelantarse a los cuellos de botella de la cadena de suministro y desarrollar «gemelos digitales» si soluciono el problema? Disponer de una plataforma digital para trazar un mapa de las líneas de suministro de forma virtual, nos ayudará a simular las ejecuciones de productos por adelantado y detectar cualquier problema que pueda surgir. Y si hablamos de un nivel muy avanzado, nos permitirá tener una visión general de todos los activos (productos, empleados, cadena de distribución, etc.) y recopilar información para poder analizarla y aplicarla.

Y si además usamos tecnologías de visión por ordenador para medir diferentes ratios de oferta y la demanda en tiempo real o analizar qué tareas son prioritarias para desarrollos futuros, la ejecución será casi perfecta.

Crear mundos sintéticos y subconjuntos para comprobar qué efecto provocan multitud de variables es una ventaja. Como decía el Doctor Strange en una de las películas de Marvel:

«Jamás vi tu futuro, solo sus posibilidades».

Como en Marvel, quizás tengamos varios universo, ¿el 838 o el 616? La simulación virtual tiene la respuesta, al menos en la realidad del universo.

Contacto bigD

info@bigd.es
www.bigd.es

+34 948 15 63 64