Nº 74 febrero 2022

Nuevas tendencias, exigencias y retos de las seguridades del año 2022

Como decíamos recientemente respecto a las predicciones de seguridad para el 2022, este será un año de nuevas tendencias, exigencias y retos para las seguridades tanto sea física o lógica, como pública o privada.

Se prevé que cada uno de estos planteamientos y desarrollos permitirá a los profesionales responsables de las seguridades estar mejor preparados para enfrentar y capitalizar las innovaciones en soluciones y servicios y, en última instancia, brindar mayor seguridad en los entornos físicos y digitales.

Manuel Sánchez Gómez-Merelo
Consultor Internacional de Seguridad

La industria de las seguridades se encuentra en una posición única para identificar los potenciadores más importantes, los eventos disruptivos y los desarrollos derivados de las nuevas tendencias, exigencias y retos que darán forma al panorama de la seguridad en 2022. Especialmente, se prevé que sea un año en el que se irá consolidando la importancia de la ciberseguridad para proteger los diferentes ámbitos institucionales, industriales y comerciales.

Tras observar el mercado, escuchar y analizar a grandes usuarios y empresas, creemos que los siguientes temas afectarán a la demanda y la oferta de la industria de las seguridades este año y en el futuro.

Nuevas tendencias

Transformación digital y seguridad. La transformación digital ha traído consigo nuevas implementaciones en la nube y renovados modelos de servicio, lo que ha brindado oportunidades para gestionar el control de acceso en aplicaciones, activos físicos y datos, mientras que el uso de nuevos formatos ha permitido una autenticación confiable y ágil. Operadores y grandes empresas de tecnología están aumentando la funcionalidad de nuevas credenciales en las aplicaciones.

Cultura digital y riesgo digital. Es imprescindible impulsar una toma de conciencia general que permita captar el principio fundamental basado en la idea de que el tratamiento de datos personales, bajo una buena protección, es sinónimo de investigación, desarrollo y crecimiento. La resiliencia de nuestras sociedades y la evolución de habilidades requerirán de un incremento de la cultura de confianza digital y riesgo cibernético, con el surgimiento de nuevas habilidades y programas de formación especializada a todos los niveles.

Accesos securizados. La gestión de accesos securizados ya es y será una necesidad para las organizaciones de todo el mundo en 2022. Se espera que su adopción sea impulsada por medidas regulatorias internacionales, y por los líderes empresariales que se encuentran ya buscando soluciones que puedan ser fácilmente implementadas y gestionadas de forma eficiente.

5G y sus nuevas posibilidades. Si bien las nuevas redes 5G son un avance imprescindible en cualquier relación de tendencias tecnológicas actuales y futuribles, su progresiva expansión va colmando poco a poco las expectativas creadas con ciertas garantías de seguridad. Podemos imaginar que estamos en

un buen momento para destacar el 5G como una tendencia en el ámbito de la videovigilancia, sin embargo, una nueva tecnología solo se convierte en tendencia cuando se empiecen a ver modelos de éxito en el sector de la seguridad y la vigilancia.

Inteligencia artificial. En los últimos años hemos asistido a una popularización de algunas aplicaciones sociales que se han infiltrado en multitud de dispositivos, lo que apunta a que durante 2022 los expertos pondrán a disposición una auténtica invasión de la inteligencia artificial a todos los niveles también en el de la seguridad.

En este sentido, la legislación y la reglamentación relacionadas con el desarrollo y el uso de tecnologías y aplicaciones basadas en la inteligencia artificial en materia de seguridad deben desarrollarse tanto a niveles regional como internacional.

Sostenibilidad y gobernanza. La sostenibilidad ya no debe considerarse una tendencia. Debe estar integrada en todos nuestros ámbitos de actividad: estrategia y política, diseño y fabricación de sistemas, administración de las organizaciones, gestión de proveedores, etc., todo ello, alineado para reducir nuestro impacto ambiental y operar de manera ética y confiable. En este sentido, durante el tiempo de la pandemia se ha puesto en evidencia un consenso cada vez más amplio en cuanto a que los usuarios finales están exigiendo trabajar con proveedores que hacen de la sostenibilidad también un objetivo capital de sus decisiones y operaciones.

Espacio de confianza digital europeo. Además de las acciones a nivel país, la tendencia es que se vaya estableciendo un marco normativo y legislativo estandarizado en la UE (Unión Europea) con el fin de procesar y alojar los datos de los ciudadanos en el propio continente. Este debe atender a los usuarios y a las organizaciones de toda la UE, y abogar por la estandarización e interoperabilidad de las soluciones de seguridad y ciberseguridad europeas. Para ello también se convierte en imprescindible revisar y actualizar el Reglamento General de Protección de Datos (RGPD) en aspectos como los de limitación de datos, duración del almacenamiento, o el derecho de supresión, que son obstáculos reales para la tecnología conectada del IoT y el Blockchain.

Nuevas exigencias

Seguridad en la cadena de suministro. Los problemas en la cadena de suministro seguirán siendo una tendencia de inseguridad dominante, convirtiendo el 2022 en un año en el que la industria debe ser más proactiva en cuanto a la protección. A lo largo del año será fundamental llevar a cabo un control exhaustivo de la cadena de suministro, ya que la mayor parte de las vulnerabilidades y los ciberataques se producen por carencias de seguridad en las operaciones con proveedores.

Protección de las infraestructuras críticas. La tendencia al incremento de ataques a las infraestructuras críticas y estratégicas se mantendrá en el 2022 y debemos seguir avanzando en su protección para no ser objetivo de bandas organizadas, terroristas o ciberdelincuentes. Las nuevas exigencias de protección y el permanente desarrollo de los planes de seguridad, contingencia y continuidad, serán la garantía para el funcionamiento de los servicios esenciales para los ciudadanos.

Soluciones "zero trust". Las organizaciones recurrirán a soluciones y marcos de confianza cero para garantizar una visibilidad y un control completo de sus redes a medida que bandas organizadas y ciberdelincuentes evolucionen sus estrategias y tácticas de ataque. Para asegurar la planificación de las seguridades, es recomendable implementarlas desde un enfoque "security by design", planificación y ejecución que puede garantizar el mejor control y gestión de la seguridad global de forma integral e integrada en todo el proceso.

Seguridad de acceso "just in time". En 2022 se producirá un aumento del acceso a los recursos de IT justo en el momento en el que se necesitan, es decir, la seguridad de acceso en tiempo real, principalmente en las infraestructuras estratégicas, críticas e industriales de mayor relevancia.

Autentificación de procesos. Si bien adoptar un enfoque de confianza cero, principalmente para la ciberseguridad, se centra en autenticar las credenciales de los dispositivos y aplicaciones conectadas, la capacidad de establecer la autentificación de los sistemas de control de acceso biométrico y la videovigilancia en sí, serán cada vez más fundamentales para confiar en su valor.

Biometría sin contacto. Durante el tiempo de recorrido de la pandemia generada por la COVID-19, el uso de la biometría se ha desarrollado y ya está muy difundido, bien sea para asegurar un dispositivo móvil, proteger una licencia de uso u otra identificación personal o gubernamental o, simplemente para hacer el control y seguimiento del estado físico de una persona.

Liderazgo y dirección de seguridad global. Las exigencias, cambios de paradigmas y liderazgos en la gestión de las seguridades, ha motivado la creación de nuevos perfiles profesionales en los últimos años en todos los niveles: Director de Seguridad (CSO), Director de Seguridad de la Información (CISO), Director de Cumplimiento (CCO) y al que hay que añadir otro más reciente, como el Director de Seguridad Global (CGS). Este tiene como misión gestionar la seguridad integral e integrada de todo lo relacionado con actividad de la organización.

Nuevos retos

Seguridad integral e integrada. La pandemia ha sido un especial catalizador en la implementación de las tecnologías de prevención y protección de activos y personas con bajo o nulo contacto, muchas de las cuales ahora están integradas de forma permanente, al igual que el uso de plataformas para el trabajo a distancia o teletrabajo, el video inteligente, el control y gestión del transporte y la logística, etc. para garantizar el funcionamiento de las organizaciones y que se cumplan las pautas de distanciamiento social y salud y seguridad pública y privada.

Modelo de trabajo híbrido. Los modelos de trabajo híbridos son la norma hoy y una de las principales tendencias que dominará la industria de la seguridad en 2022, y es un modelo de seguridad en el que ningún dispositivo es automáticamente confiable y debe ser validado. La modalidad de trabajo híbrido, el aumento de las herramientas de acceso remoto, especialmente en entornos OT, así como la transformación digital acelerada, seguirán siendo una de las mayores amenazas de ciberseguridad empresarial.

Ciberseguridad estructural OT. La seguridad como misión tradicional de la que se ocupaban los departamentos de TI, continuará trasladándose a la OT, creando nuevos retos para las organizaciones al ser nuevas, por lo que todavía no se conocen ni comprenden. No obstante, la amenaza de ciberdelincuencia se ha incrementado y requerirá de nuevas soluciones personalizadas por sectores de actividad. La combinación de IoT, la nube y las tecnologías móviles está impulsando de forma continua la transformación digital en la industria de la seguridad y, por tanto, presentando nuevos retos.

Conexión en entornos híbridos. Para el usuario final de la tecnología, desde un consumidor que usa su teléfono móvil, hasta el personal de seguridad que protege instalaciones, pasando por la gestión de los sistemas videovigilancia o el control y gestión de infraestructuras esenciales, la arquitectura tecnológica que se utiliza para brindar servicios se ha vuelto invisible pero con nuevos retos para la protección.

Ataques de ransomware. A lo largo de 2021 hemos visto incrementarse notablemente el número de amenazas y ataques de *ransomware* con métodos "file" y "fileless", siendo ya habitual su presencia en el mundo digital actual. Los ataques seguirán aumentando y serán cada vez más sofisticados, perjudicando a instituciones u organizaciones públicas y privadas, así como a los ciudadanos en general.

A modo de resumen

Del sondeo, análisis e información captada que nos ha llevado a relacionar las principales tendencias, exigencias y retos de seguridad en este año 2022, se vislumbran líneas de acción para el planteamiento de las mejores soluciones para la gestión del riesgo en materia de seguridad física y ciberseguridad con nuevas coordenadas para la planificación del manejo de la incertidumbre y la resiliencia.

Será un año de cambios y concienciación hacia una nueva cultura de la gestión del riesgo y las seguridades, con lo que prevemos que se registrará una evolución significativa hacia nuevos planteamientos en la formación y estructuras organizativas de los profesionales de la seguridad y la ciberseguridad.