NUEVOS RIESGOS Y AMENAZAS: EXIGENCIA DE SEGURIDAD Y RESILIENCIA

Fortalecer la seguridad y la resiliencia es objetivo prioritario de instituciones y organizaciones públicas y privadas

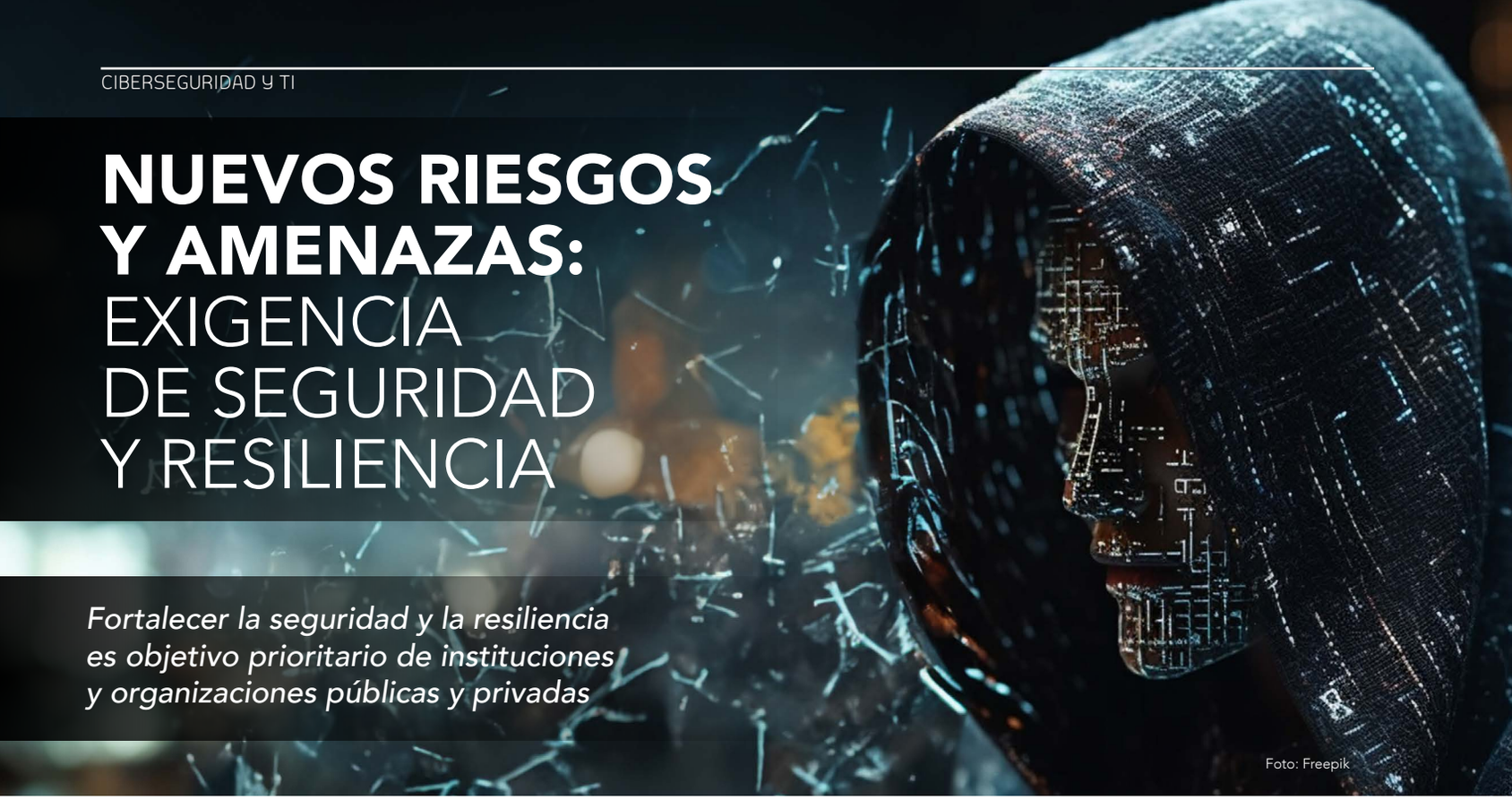


Foto: Freepik

ESPAÑA

Manuel Sánchez Gómez-Merelo

Actualmente, vivimos tiempos convulsos en las ciudades de todo el mundo derivados de una cierta globalización de las crisis políticas, económicas y sociales que, de una u otra manera, conllevan también nuevos riesgos y amenazas que precisan de una mayor exigencia de seguridad y resiliencia, adecuada al momento.

Estos nuevos requisitos, junto con la expansión exponencial de la digitalización, los nuevos dispositivos de Internet de las Cosas (IoT) y las aplicaciones de la Inteligencia Artificial (IA), están ampliando los límites de la red a la vez que aumentan las vulnerabilidades y el riesgo de ciberataques.

NUEVOS RIESGOS Y AMENAZAS

Estamos ante la necesidad de una revisión de la realidad de nuestras seguridades por un incremento de nuevas amenazas al desarrollo de la vida social y sus infraestructuras estratégicas y críticas, principalmente por un aumento de la ciberdelincuencia y otras consecuencias derivadas de los conflictos armados como los existentes en Ucrania y la Franja de Gaza e Israel. A esto se suman los fenómenos meteorológicos severos y los desastres naturales derivados del cambio climático.

En este sentido, los ciberataques contra instituciones públicas aumentaron un 95 por ciento sólo en la última mitad de 2022 y, para 2025, se estima que el 30 por ciento de las infraestructuras críticas experimentarán una brecha de seguridad.

El incremento de los riesgos y amenazas y la significación de las vulnerabilidades pone de manifiesto, de nuevo, que gobiernos y entidades públicas y privadas deben mejorar su capacidad para prevenir y proteger contra los riesgos y reaccionar ante las amenazas.

No hacer nada ya no es una opción. Continuar confiando en sistemas no actualizados u obsoletos, y redes y tecnologías de las comunicaciones aisladas, al tiempo que los riesgos continúan multiplicándose, no es un enfoque viable, y ya no se puede confiar en estrategias anteriores para construir la seguridad y resiliencia que el Siglo XXI impone.

Cabe destacar algunas consideraciones y desafíos especiales para las redes y tecnologías para la protección de la información y de las comunicaciones, así como aplicar nuevas formas de pensar sobre las vulnerabilidades que, con el desarrollo de la digitalización, están más expuestas a riesgos y amenazas que pueden propagarse rápidamente.

La digitalización también estrecha la conexión entre los riesgos físicos y cibernéticos. La convergencia entre TI y las tecnologías operativas (OT) crea nuevas vulnerabilidades y oportunidades para ataques.

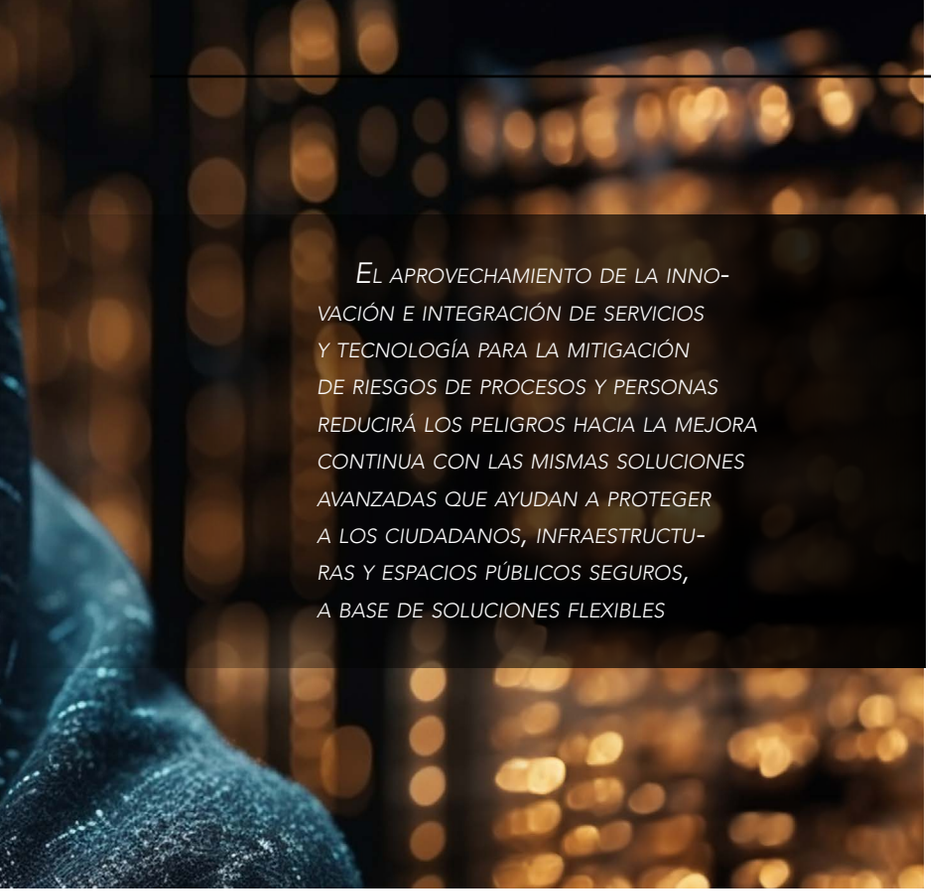
Foto: Freepik

NUEVAS EXIGENCIAS DE SEGURIDAD Y RESILIENCIA

El desarrollo de iniciativas de digitalización aumenta la agilidad operativa, la eficiencia y la productividad, pero han de revisarse y plantearse nuevas seguridades para proteger a los ciudadanos y las operaciones públicas y privadas, y se ha de fortalecer su resiliencia para que puedan garantizar la continuidad del funcionamiento en cualquier circunstancia.

Las organizaciones son un objetivo potencial para los ataques y, por tanto, se requiere una atención renovada al riesgo, la resiliencia y la seguridad para:

- Garantizar la continuidad de los servicios críticos y estratégicos y proteger los datos e información confidenciales.
- Minimizar los costes de seguridad, implementando



El aprovechamiento de la innovación e integración de servicios y tecnología para la mitigación de riesgos de procesos y personas reducirá los peligros hacia la mejora continua con las mismas soluciones avanzadas que ayudan a proteger a los ciudadanos, infraestructuras y espacios públicos seguros, a base de soluciones flexibles

la protección adecuada para cada tipo de riesgo ciber o físico a los que se enfrentan.

- Reducir las pérdidas económicas y de prestigio debidas a ataques cibernéticos y físicos.
- Mantener la reputación y la confianza ante los ciudadanos.
- Proteger a los ciudadanos brindándoles información importante relacionada con la salud y la seguridad (prevención y protección).

En este sentido, los sistemas de notificaciones masivas pueden alertar rápidamente a las personas sobre los procesos a implementar ante emergencias, para que puedan tomar las medidas necesarias y realizar las acciones apropiadas basadas en su seguridad y las de los suyos.

Una red institucional y empresarial segura y resiliente admite comunicaciones y acciones de misión crítica, así como IoT, tecnologías de seguridad física y cibernética, que son esenciales para operaciones confiables.

Para incrementar la seguridad y protección en edificios y espacios públicos se requiere una red multiservicio segura para soportar las aplicaciones y procesos necesarios para proteger contra riesgos y amenazas y mantener la disponibilidad y continuidad del servicio en todo momento, con aumento de la confiabilidad.

Cada organización, pública o privada, debe desarrollar, con enfoque holístico, estratégico y táctico, procesos estandarizados para la seguridad y la resiliencia adaptados a su perfil personalizado de riesgo, ubicación, objetivos, etc.

Para aumentar la seguridad y la resiliencia, teniendo en cuenta la evolución de las inseguridades se han de perfilar y elegir las soluciones adecuadas reevaluando los riesgos cibernéticos y físicos, áreas de exposición y posibles consecuencias, así como las diferentes opciones para prevenir, proteger y reaccionar ante ataques en cada caso, comenzando por una auditoría para evaluar los riesgos y el potencial de pérdida para cada vulnerabilidad identificada.

Para contrarrestar la amenaza que cambia rápidamente el panorama, es importante reevaluar periódicamente los riesgos y monitorear continuamente los riesgos cibernéticos y físicos con los recursos también para las nuevas vulnerabilidades.

NUEVAS TECNOLOGÍAS Y PROCEDIMIENTOS

Como ya hemos comentado, el rápido desarrollo de la digitalización traerá beneficios, además de nuevos riesgos y vulnerabilidades, en un mundo y una sociedad globalmente digitalizada, en los que las personas, los objetos, los sistemas y los procesos están conectados.

Esta especial conexión facilita el aprovechamiento de la tecnología IoT y, la información que proporciona, automatiza los flujos de trabajo para aumentar la eficiencia y acelerar las respuestas para que organizaciones y ciudadanos utilicen datos precisos y en tiempo real para poder, tanto aumentar su visibilidad, como tomar decisiones informadas.

Sin embargo, es preciso repetir que las tecnologías también introducen un nuevo conjunto de riesgos físicos y cibernéticos que deben abordarse, puesto que pueden utilizarse a favor y en contra de las organizaciones.

Podemos tomar como ejemplo la inteligencia artificial (IA). La IA ayuda a prevenir, proteger y acelerar las respuestas ante amenazas cibernéticas y físicas, pero también pone de manifiesto vulnerabilidades para malas acciones, como descifrar contraseñas de sistemas o la propia manipulación de datos.

El aprovechamiento de la innovación e integración de servicios y tecnología para la mitigación de riesgos de procesos y personas reducirá los peligros hacia la mejora continua con las mismas soluciones avanzadas que ayudan a proteger a los ciudadanos, infraestructuras y espacios públicos seguros, a base de soluciones flexibles y compatibles desde las primeras etapas de diseño.

Fortalecer la seguridad y la resiliencia es objetivo prioritario de instituciones y organizaciones públicas y privadas, siguiendo el enfoque y proceso holístico recomendado, y las nuevas oportunidades para aprovechar las soluciones de redes y comunicaciones son esenciales para permitir una toma de decisiones más eficiente, efectiva y colaborativa, protegiendo y garantizando la seguridad ciudadana. ■

Foto: Freepik

Manuel Sánchez Gómez-Merelo, presidente y director general de ET Estudios Técnicos, S.A. *Más sobre el autor:*