CincoDías

| | | | |
|---|---|---|---|
| Publicación | Cinco Días General, 32 | Fecha | 01/07/2020 |
| Soporte | Prensa Escrita | País | España |
| Circulación | 26 609 | V. Comunicación | 15 204 EUR (17,040 USD) |
| Difusión | 18 595 | Tamaño | 423,34 cm² (67,9%) |
| Audiencia | 38 000 | V.Publicitario | 7555 EUR (8467 USD) |


# Los robots menosprecian la ciberseguridad

**Tras décadas de desatención, el sector de la robótica intenta revertir una inseguridad y vulnerabilidad evidentes ▶ El eslabón más débil es el Sistema Operativo Robótico (ROS)**

JORGE G. GARCÍA
MADRID

Los robots se han convertido en el gran agujero de la ciberseguridad. Una falla del sistema desatendida por la industria desde hace décadas. Su misión no es protegerse de un ciberataque, por comprometida que sea su función, y el auge de la automatización y la conectividad han expuesto aún más a una tecnología en plena expansión. España, situado entre los 10 países del mundo con más autómatas, cuenta con 16 robots por cada 1.000 trabajadores, según cifras de la Federación Internacional de Robótica. "Casi ninguna empresa publica realiza actualizaciones de seguridad para estos productos", asegura Alfredo Reino, experto en ciberseguridad.

Uno de los eslabones más débiles aparece en el Sistema Operativo Robótico, conocido como ROS. Las grandes productoras lo han adoptado casi como estándar, pero surgió simplemente como una investigación de la Universidad de Stanford en 2007 para mejorar los protocolos de comunicación. Como explica Óscar Lage, experto en ciberseguridad de Tecnalia, nació sin nada de ciberseguridad porque no era la finalidad del proyecto. No fue hasta hace cuatro años, con la evolución a ROS2, cuando comienzan a desarrollarla; aunque casi ninguna máquina lo tiene instalado. "Son sistemas críticos muy poco protegidos. Al igual que en otras industrias, quienes los diseñan, crean y venden se han centrado en la parte funcional. Hasta que no ha habido sustos importantes nadie se ha preocupado".

Algún emprendedor ya ha intentado revertir la tendencia. Es el caso de Víctor Mayoral, director técnico y cofundador de Alias Robotics. La solución que propone la ha bautizado como Sistema Inmunológico de Robots (RIS). Este software expone a las máquinas a diferentes amenazas virtuales y prepara a sus sistemas para evitar posibles contagios por parte de virus informáticos. Con la ayuda de la inteligencia artificial, aprende a prevenir mejor estas amenazas, así como a identificarlas incluso antes de que ocurran. "La robótica está en el mismo punto que estaba la informática hace 20 años. Es de total inseguridad y total alarma. Los fabricantes no están preparados para combatir ciberataques", sostiene.

### Sectores estratégicos

La ausencia de un estándar internacional no ayuda. De fábrica a lo más que aspiramos es a tener la opción de configurar la seguridad una vez que recibimos los robots. El motivo que aducen las marcas es la interoperabilidad con prototipos más viejos. Evitar que los lenguajes sean tan dispares que no se comuniquen entre ellos. Sin embargo, en las líneas masivas de producción y en las redes eléctricas inteligentes –*smart grid*– prefieren no jugársela. Son sectores estratégicos. "Hablamos de riesgos personales y de funcionamiento industrial. Con un *ransomware* nos pueden echar abajo toda la electricidad de un país o condicionar la seguridad física de los empleados. Esto es más peligroso", expone Lage.

GETTY IMAGES

**Quienes los diseñan, crean y venden se han centrado en la parte funcional**

**La ausencia de un estándar internacional no ayuda a mejorar la seguridad**

La Unión Europea, cada vez más implicada con la digitalización, ha comenzado a tomarse en serio el asunto. Historia diferente son los plazos. La propia Comisión, en una recomendación publicada el 19 de febrero, pedía que desde Bruselas comenzara a legislar para proporcionar mejor protección a los usuarios y mayor seguridad jurídica. Los Gobiernos nacionales también cuentan con demasiados vacíos legales. Reino Unido, Francia y Alemania han dado algunos pasos, aunque insuficientes, alejados de corregir la precariedad instalada en la robótica. "Debería imperar la ética, pero es problemática cuando los fabricantes se desentienden de la seguridad y la gente es inconsciente de que los robots están descontrolados".

Parte de las debilidades que explotan los malos se debe a los elementos comunes que comparten los dispositivos robóticos. El internet de las cosas ha provocado que estén muy presentes en múltiples entornos. Según la consultora Gartner, este año habrá cerca de 6.000 millones de elementos conectados. Lo mismo son indispensables en el diseño de los coches autónomos que en un dron. En palabras de Reino, en un intento por producir en masa, estas herramientas emplean tanto el mismo nivel de software como de microprocesadores. Si alguien ataca un brazo robótico, podrá replicarlo en otro que juegue con un niño.

## ¿Qué hacemos con los robots?

- **Legislación.** Una posible solución ante tanta inseguridad, aparte de mejorar la legislación, ha de venir de la formación. La robótica demanda talentos diferentes. Es insuficiente graduarse como ingeniero industrial o arquitecto de ciberseguridad. El propio Mayoral asegura que las empresas ni saben a quién recurrir –"y eso que pueden provocar accidentes terribles", precisa–.
- **Colaboración.** La colaboración científica forma parte de la respuesta. "Es un problema de silos. En robótica, los ingenieros no saben de sistemas ni de seguridad. Tampoco quienes programan están al tanto de cómo funciona la seguridad. Viven separados los unos de los otros", razona Alfredo Reino, experto en ciberseguridad.
- **Covid.** La crisis del coronavirus ha acentuado la digitalización, al igual que la exposición de los sistemas. El punto de partida de los robots parece bastante comprometido de antemano, y costará ver un cambio. "Las empresas no tienen presión social o gubernamental para cambiar su comportamiento. No existen normas", concluye el emprendedor Víctor Mayoral.

**Artículo completo en retina.elpais.com**