MAURIZIO DE STEFANO

director global de la Práctica de Agua de Indra

"ES NECESARIO FOMENTAR UNA CULTURA Y CONCIENCIACIÓN EN MATERIA DE CIBERSEGURIDAD EN EL SECTOR DEL AGUA"

Las empresas dedicadas al tratamiento, abastecimiento y saneamiento del agua tienen ante sí uno de los mayores desafíos: la implantación tecnológica digital. Si bien es cierto que muchas de las *utilities* apostaron en su momento por la I+D tecnológica, sobre todo en relación a la lectura de contadores y la sectorización de redes, los nuevos retos que marca la industria 4.0 hace que todavía queden retos por cumplir, como las conexiones de sistemas (incluyendo máquinas y herramientas y no solo sistemas informáticos), el intercambio de información gracias a esas conexiones y su aprovechamiento por las diferentes industrias para temas de seguridad, realidad aumentada, impresión 3D, *cloud computing*, internet de las cosas (IoT) y, sobre todo, *big data* y *data science*. Para hablar sobre todo de seguridad y ciberseguridad, Tecnoaqua entrevista a Maurizio De Stefano, director global de la Práctica de Agua de Indra, una de las principales compañías globales de tecnología y consultoría y socio tecnológico para las operaciones clave de los negocios como el agua.

Rubén J. Vinagre García
coordinador editorial de *Tecnoaqua*

¿Es la seguridad un elemento a tener en cuenta en las decisiones de gestión de los operadores de agua y demás empresas del sector?

Sin ninguna duda. Solo hay que tener en cuenta que, desde el principio de los tiempos, el agua ha sido objeto de disputa entre civilizaciones y objetivo de ataques en tiempos de guerra por su potencial para causar gran daño a la población. En los últimos años, han surgido nuevos riesgos y amenazas de la mano de la transformación digital, lo que ha provocado una tendencia creciente de ciberataques en el mundo. Solo hay que prestar atención a las cifras: según los Equipos de Respuesta a Incidentes de Ciberseguridad de España, en 2017 se ha vuelto a experimentar un crecimiento significativo del número de ciberincidentes gestionados con respecto a 2016. Además, el Centro de Respuesta a incidentes de Seguridad e Industria (CERTSI) gestionó más de 123.000 incidentes (885 en operadores críticos) durante 2017. Esto supuso un aumento de un 7% con respecto a 2016, año que ya triplicaba las cifras del año anterior.

La incursión de las nuevas tecnologías en el mundo del agua para mejorar la gestión hace que aparezcan nuevas vulnerabilidades ante las cuales las empresas de agua deben prepararse. Este tipo de compañías están expuestas a impactos que van desde el mal funcionamiento de las instalaciones o el desabastecimiento del suministro, hasta perjudicar su imagen al perder la confianza de los ciudadanos e incluso desencadenar crisis de pánico en la población. No hay que olvidar que las empresas del sector son un blanco potencial para ataques terroristas.

¿Y está el sector del agua preparado en cuestión de seguridad de instalaciones y sistemas??

Se está empezando a trabajar, desde las organizaciones privadas y los organismos públicos, en concienciar de

la necesidad de estar prevenidos y en desarrollar medidas y sistemas, pero todavía queda mucho camino por recorrer. Solo el 54% de las *utilities* cuentan con un programa para inventariar y proteger sus activos con información sensible.

Las empresas del sector están expuestas a robos de identidad, ataques web, denegación del servicio, *ransomware*, entre otros. Los impactos a los que se enfrentan al recibir un ciberataque van desde el cifrado de información y la consiguiente petición de rescate hasta el fraude, la parada en la producción, el ataque a terceros o la pérdida de control de los equipos. Las empresas muchas veces no son conscientes de que han sido hackeadas hasta que notan los efectos del ataque, como en el caso de una parada en una bomba o un mal funcionamiento en una válvula, pero pueden estar meses siendo víctimas de robo de información sin ser conscientes. Por ello, es importante que internamente las organizaciones apuesten por invertir en seguridad.

Ya existe un Plan Nacional de Protección de las Infraestructuras Críticas, que incluye las infraestructuras relacionadas con el suministro de agua ¿Crees que son las únicas que deben estar o se debe ampliar a otras? Y si es así, ¿cuáles?

Todas las empresas involucradas en el ciclo del agua, desde la captación hasta la depuración y vertido, deben estar incluidas en el Plan Nacional de Protección. La ciberseguridad en las empresas de este sector no debe ser una preocupación para el futuro, sino algo que desde hace años debía estar en la cabeza de todos. Algún ejemplo es que ya en 2000, un exempleado de una empresa que había instalado los SCADA en una depuradora de aguas residuales en Australia provocó el vertido de 800.000 litros de aguas sucias en ríos, parques y en los terrenos cercanos. Con esto, podemos ver cómo las empresas relacionadas con el agua son realmente infraestructuras críticas y un ciberataque no daña solo a la compañía, sino también al medio ambiente y a la seguridad y salud de los ciudadanos.

Este mismo plan contempla como infraestructuras estratégicas sobre todo las de las grandes ciudades. ¿Pero qué debe hacer entonces una ciudad pequeña o mediana cuyas infraestructuras de agua también son críticas para su administración?

Todas las infraestructuras de agua deben estar protegidas, independientemente de su tamaño. Es cierto que el impacto de la parada de funcionamiento de una suministradora de agua en una gran ciudad es mucho mayor, si atendemos al número de ciudadanos afectados, pero el agua debe entenderse como un bien protegido globalmente y todos los ciudadanos deben contar con un suministro asegurado y de calidad. Un vertido incontrolado no solo afecta a los habitantes de esa ciudad, afecta al río, a la cuenca y al mar. El agua, al igual que el medio ambiente, es un tema a tratar de manera global y debe protegerse desde esta perspectiva.

¿Qué ofrece Indra al sector del agua en términos de seguridad?

Como tecnología y consultoría, ofrecemos soluciones orientadas a la ciberseguridad. Combinamos nuestro conocimiento del sector energético con nuestras capacidades de seguridad, con el objetivo de proporcionar la oferta más completa para el sector *utilities*. Nuestras soluciones y servicios abarcan toda la cadena de valor y están enfocados a usuarios internos, redes y *cloud*, zonas protegidas, controles de acceso, así como a en-

Conozca un poco más a... MAURIZIO DE STEFANO

Apasionado, creativo, provocador, visionario... afincado en España desde los 18 años, Maurizio De Stefano es titulado en Ingeniería Industrial. Experto en innovación y estrategia digital, con más de 20 años de experiencia, ha desarrollado su carrera profesional en el área de la consultoría y los servicios, pasano por empresas familiares, *startups* y multinacionales en diferentes países del mundo. Actualmente es director global de la Práctica de Agua de Indra, área en la que esta compañía quiere ofrecer soluciones disruptivas para la *industry*. Indra es una de las principales compañías de desarrollo de soluciones tecnológicas integrales, aplicables en campos como Defensa y Seguridad; Transporte y Tráfico; Energía e Industria; Telecomunicaciones y Media; Servicios Financieros; y Administraciones Públicas y Sanidad. En el ámbito académico, es máster por IESE (Barcelona) y máster en Dirección por el Instituto de Empresa (Madrid). Es profesor de Dirección Logística, Supply Chain y Trasformación Digital en el máster Digital Business Trasformation de la Universidad Politécnica de Cataluña.

Vista del i-CSOC (CyberSecurity Operations Centre), un centro especializado en operaciones de ciberseguridad desde el Indra protege los sistemas y redes de las empresas, organizaciones e instituciones que lo requieren.

trenamiento o consultoría de ciberseguridad y servicios de seguridad gestionada. Contamos con más de 200 expertos para llevar a cabo soluciones propias de ciberseguridad, y acuerdos con los principales proveedores de este ámbito. Adicionalmente, colaboramos también con los principales organismos públicos y privados para impulsar la seguridad.

¿Cómo diferencia Indra los distintos tipos de seguridad: física, lógica, ciberseguridad... y cómo actúa ante ellos?

En ciberseguridad, los servicios cubren tanto la informática del negocio como los sistemas de control y operación. En este ámbito, trabajamos elaborando planes de ciberseguridad integrales corporativos, así como para redes y sistemas OT (tecnologías de operación), con el despliegue de infraestructuras de ciberseguridad para la protección de redes y sistemas corporativos y particularizados para OT: SCI, SCADA, PCL, etc. También brindamos soluciones para la seguridad de las operaciones de las empresas en Internet y servicios de homologación y pruebas de seguridad de dispositivos OT, de seguridad gestionada para la operación de la ciberseguridad en IT y OT, y de ciberinteligencia y de alerta temprana.

Para la seguridad física, en Indra disponemos de soluciones que generan control, seguridad, agilidad y trazabilidad en el registro y accesos de personas en las inmediaciones de la empresa, basada en control de accesos mediante reconocimiento facial, así como soluciones para zonas protegidas y aisladas.

En cuanto a la seguridad lógica, para la protección de acceso a los datos, una de nuestras soluciones es la *suite* de gestión del fraude operacional, que garantiza la correlación entre identidad física y digital de los operadores de los procesos BPO mediante mecanismos de biometría, que monitoriza las acciones de los usuarios, evitando fugas de información y protege las aplicaciones corporativas ante posibles ataques o usos malintencionados.

Porque en el sector del agua... ¿es más real o probable un ataque terrorista físico o un ciberataque?

El problema de los ciberataques es que pueden originarse en cualquier parte del mundo con acceso a Internet.

» Todas las infraestructuras de agua deben estar protegidas, sea cual sea su tamaño. El agua debe entenderse como un bien protegido globalmente y todos los ciudadanos deben contar con un suministro asegurado y de calidad

Hasta ahora, el atacante tenía que desplazarse hasta las instalaciones para poder causar el daño. Hoy en día, el atacante puede estar en la misma ciudad o en la otra punta del mundo y el número de potenciales atacantes es mayor que nunca. No solo ha aumentado el origen de los ataques si no también los objetivos. El alcance de un ciberataque es mucho mayor que el de un ataque terrorista físico, pudiendo desde un solo origen atacar simultáneamente a múltiples empresas que cuenten con una misma tecnología vulnerable, por ejemplo, y la tendencia de los ataques a las infraestructuras críticas es creciente.

¿Qué medidas preventivas y correctivas deben realizarse ante cualquier ataque?

La prevención es fundamental. La mayoría de las medidas pasan por estar preparados y monitorizar en tiempo real el estado de nuestros sistemas. La seguridad debe estar integrada desde el diseño, en todo el ciclo de vida del producto. Hay que promover pruebas independientes de seguridad y priorizar las inversiones en ese rubro, dado que muchas empresas solo se preocupan por el tema cuando tienen incidentes. La mayoría de los incidentes se podrían haber evitado si se hubieran seguido políticas de seguridad apropiadas en las empresas.

Y es necesario que los operadores informen a los órganos competentes del Estado cada vez que crean que son víctimas de un ciberataque. De esta forma, se podrá evitar que otras empresas puedan ser víctimas de ese mismo ataque y se mejorará el conocimiento en el sector sobre nuevos métodos de defensa. Al final, la labor de prevención y detección y de la de reacción, análisis y recuperación tras los incidentes es una carrera de mejora continua.

¿ Está el sector capacitado ante estos nuevos retos de seguridad o falta formación?

Creo que cada vez más las empresas toman conciencia de la importancia de invertir en la seguridad sus instalaciones, de sus equipos y de la información. Aun así, queda un gran camino, sobre todo para las pequeñas y medianas empresas. Es un trabajo de concienciación de los riesgos de seguridad asociados a la tecnología, de promover el conocimiento entre la población, y entre los responsables de la toma de decisiones de las empresas. También es vital la observación de las mejores prácticas nacionales e internacionales para su incorporación progresiva al diseño de nuevas soluciones de ciberseguridad.

¿ Y es necesario certificar la seguridad en infraestructuras de agua?

Es necesario tener en cuenta las políticas nacionales de ciberseguridad y trabajar de forma coordinada con los organismos responsables en esta materia, tanto nacionales como internacionales. Las administraciones públicas deben colaborar con leyes para que la industria incorpore tecnologías de ciberseguridad, de manera que las empresas del sector mantengan los máximos niveles de ciberseguridad y operación. Velar por la seguridad es velar por la garantía de la continuidad del servicio, por la seguridad de las instalaciones, de los sistemas informáticos y de la población en su conjunto.

Por último, ¿cómo ves el tema de la seguridad en el sector del agua a corto, medio y largo plazo?

En mi opinión, a corto plazo hay un interés creciente pero lento en la inversión en ciberseguridad, debido, en cierto modo, a que va muy de la mano con el proceso de transformación digital de las empresas. Por esto es necesario fomentar una cultura y concienciación en materia de ciberseguridad, fundamentalmente entre los usuarios y responsables de los sistemas de información, dirigida a garantizar la integridad, la confidencialidad la disponibilidad de los sistemas y la gestión de las infraestructuras críticas.

Sin embargo, en el futuro próximo, al construir nuevas infraestructuras o al integrar nuevos dispositivos inteligentes con el IoT, la seguridad ya estará integrada desde el diseño y, a largo plazo, no existirán empresas que no cuenten con un equipo experto de ciberseguridad en su plantilla. Además, con el desarrollo de la Inteligencia Artificial, la gestión de la ciberseguridad mejorará exponencialmente y nos permitirá ir aprendiendo y evolucionando constantemente.

» Hay un interés creciente pero lento en la inversión en ciberseguridad, debido, en cierto modo, a que va muy de la mano con el proceso de transformación digital de las empresas