"ACTUALMENTE LA CIBERSEGURIDAD EN EL TRATAMIENTO DE AGUA SE CENTRA EN LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS, COMO PLANTAS DE TRATAMIENTO Y DISTRIBUCIÓN, CONTRA LAS AMENAZAS"

"CYBERSECURITY IN WATER TREATMENT CURRENTLY FOCUSES ON PROTECTING CRITICAL INFRASTRUCTURES, SUCH AS TREATMENT AND DISTRIBUTION PLANTS, AGAINST THREATS"

Alicia Pérez-Ballester
Directora del Departamento ee Optimización y Procesos de Acciona Agua
Director of the systems and process optimisation department of Acciona Agua

¿Cómo definiría el trabajo que realiza en su departamento actualmente? ¿Qué sinergias o de qué forma repercute su trabajo en el desarrollo de otros departamentos de la compañía más dirigidos a la materialización del proyecto? ¿Cómo se articula la relación entre estos departamentos?

Dentro de las responsabilidades del departamento de Optimización de Sistemas y Procesos se incluyen Automatización, Optimización y Ciberseguridad en las operaciones. En concreto en el departamento de Ciberseguridad nos encargamos de velar por el cumplimiento de la normativa vigente en cada uno de los países en los que operamos, de mantener un inventario de activos actualizado, de que las conexiones

How would you define the work you currently carry out in your department? What are the synergies or how does your work influence activities in other departments of the company that are more focused on project development? How is the relationship between these departments articulated?

The responsibilities of the Systems and Process Optimisation Department include Automation, Optimisation and Cybersecurity in operations. In the Cybersecurity Department, we are responsible for ensuring compliance with current legislation in each of the countries in which we operate, maintaining an updated inventory of assets, ensuring that connections to our plants are secure and that the

a nuestras plantas sean seguras y de que se cumpla la Política de Ciberseguridad. Además, promovemos la concienciación a través de la formación de las personas, creando una cultura de ciberseguridad.

Trabajamos en colaboración con nuestros equipos corporativos de Ciberseguridad y de IT y damos soporte a nuestros departamentos de Construcción y O&M. En Construcción, por ejemplo, colaboramos durante el diseño de las plantas para implementar la ciberseguridad desde el inicio del proyecto, así como en la fase de puesta en marcha, donde participamos en las pruebas de los sistemas de ciberseguridad. Para el departamento de Operación y Mantenimiento realizamos informes de estado inicial a nivel de ciberseguridad de las plantas o servicios en las que vamos a iniciar las operaciones y también de forma periódica. En dichos informes evaluamos las posibles carencias y proponemos soluciones. También colaboramos en la resolución de las incidencias que puedan surgir y en la implantación de las soluciones necesarias.

El departamento de Optimización de Sistemas y Procesos trabaja en todo el ciclo de vida de las infraestructuras, lo que nos permite tener una visión global y nos ayuda a generar soluciones adecuadas a largo plazo.

En una realidad cada vez más asumida de equipos multidisciplinares, ¿qué no puede faltar en un departamento como el que Vd. dirige?

Las ganas de aprender y la curiosidad para mantenerse siempre al día. La tecnología evoluciona rápidamente y en el mundo de la ciberseguridad hay que ir más deprisa que los atacantes por lo que se necesitan personas que sean capaces de estar en constante aprendizaje.

Tampoco puede faltar el espíritu de colaboración, ya que poco se puede conseguir trabajando solo, es necesario ser capaz de escuchar y entender las necesidades de los demás para conseguir un objetivo común. En necesaria la colaboración entre las personas del equipo, entre los departamentos y con diferentes empresas tecnológicas que nos aportan y a las que aportamos conocimiento y experiencia.

¿Dónde está y hacia dónde se dirige la ciberseguridad en un área tan decisiva en la actualidad como es la del tratamiento de agua?

Actualmente la ciberseguridad en el tratamiento de agua se centra en la protección de infraestructuras críticas, como plantas de tratamiento y distribución, contra las amenazas. Se busca evitar intrusiones, manipulaciones no autorizadas o posibles sabotajes que podrían poner en riesgo la calidad y la disponibilidad del agua potable o producir vertidos.

Cybersecurity Policy is complied with. We also promote awareness by training people and creating a culture of cybersecurity.

We work in collaboration with our corporate Cybersecurity and IT teams and support our Construction and O&M departments. In Construction, for example, we collaborate during the plant design stage to enable implementation of cybersecurity from the beginning of the project, as well as in the commissioning phase, where we participate in the testing of cybersecurity systems. For the Operation and Maintenance Department, we carry out initial status reports on cybersecurity at the plants or services in which we are going to start operations and we also draw up periodic reports. In these reports, we evaluate possible shortcomings and propose solutions. We also collaborate in the resolution of any incidents that may arise and in the implementation of the necessary solutions.

The Systems and Process Optimisation Department works on the entire lifecycle of infrastructures, which allows us to have a global vision and helps us to generate appropriate solutions in the long term.

Given the increasingly accepted reality of multidisciplinary teams, what qualities are essential in a department such as the one you lead?

The desire to learn and the curiosity to keep up to date. Technology evolves rapidly and in the world of cybersecurity you have to move faster than the attackers, so you need people capable of learning constantly.

The spirit of collaboration is also vital, as little can be achieved working alone. The ability to listen and understand the needs of others is vital in order to achieve a common goal. Collaboration is necessary between team members, between departments and with different technology companies that provide us with knowledge and experience.

Where is cybersecurity in today's critical area of water treatment and in what direction is it moving?

Cybersecurity in water treatment currently focuses on protecting critical infrastructures, such as treatment and distribution plants, against threats. The aim is to prevent intrusions, unauthorised manipulation or potential sabotage that could jeopardise the quality and availability of drinking water or lead to discharges.

In the immediate future, the NIS2 Directive is expected to be transposed into Spanish law this year. NIS2 extends the number of critical sectors and

En el futuro más inmediato se espera que la Directiva NIS2 sea traspuesta al ordenamiento jurídico español en este año. La NIS2 amplía el número de sectores críticos y el número de entidades que deben adoptar medidas y cumplir con sus requisitos de seguridad. Como Entidades Esenciales (EE), se encuentran la Distribución de agua potable y el Tratamiento de aguas residuales.

Entre los cambios que introduce la NIS2 se incluye que la responsabilidad de su cumplimiento recae en los órganos de dirección de las empresas, se refuerzan las exigencias en la cadena de suministro, se incluye como novedad un régimen sancionador y la obligación de la notificación de incidentes a la autoridad.

¿Cómo afecta la ciberseguridad al diseño de los sistemas de control?

La integración de la ciberseguridad desde el diseño en los sistemas de control es esencial para proteger las infraestructuras de las amenazas. La segmentación de las redes, la creación de DMZ (zonas desmilitarizadas), la seguridad en los accesos remotos, los sistemas de autenticación, los procedimientos de actualización y parcheo, así como la selección de proveedores teniendo en cuenta la ciberseguridad, deben definirse desde el diseño.

¿Cómo puede repercutir la implantación de una correcta tecnología de ciberseguridad y control en el coste de la inversión y el mantenimiento de un proyecto de gestión de agua?

Lo realmente importante es el coste que puede tener no implementarla. Los costos asociados con la recuperación de ciberataques y la reparación de daños pueden superar ampliamente las inversiones en medidas preventivas.

En lo relativo a la inversión en grandes infraestructuras de nueva construcción, el costo asociado a la ciberseguridad es mínimo en comparación con el coste total de la infraestructura, más aún cuando ya que se integra desde el diseño. En las infraestructuras existentes el coste puede llegar a ser alto, en muchos casos los sistemas de control son antiguos y puede ser necesario realizar migraciones completas para adaptarlos a las normas de ciberseguridad.

En cuanto al coste del mantenimiento de la tecnología de ciberseguridad en los proyectos de operación y mantenimiento de infraestructuras de agua, podría equipararse al coste del mantenimiento de los sistemas de control, para hacernos una idea. Deben seguirse los procedimientos de ciberseguridad definidos para el proyecto e integrarse las operaciones necesarias en los sistemas de gestión del mantenimiento CMMS. Igualmente, hay que tener en cuenta que es necesario personal capacitado y concienciado con la

the number of entities that must adopt measures and comply with its security requirements. As Critical Entities (CE), drinking water supply and wastewater treatment facilities are governed by the Directive.

New aspects of the NIS2 Directive include the responsibility for compliance lying with the management bodies of companies, reinforced requirements in the supply chain, a new system of sanctions and the requirement to report incidents to the authority.

How does cybersecurity affect the design of control systems?

It is essential to integrate cybersecurity into control systems from the design stage in order to protect infrastructures from threats. Network segmentation, the creation of DMZs (demilitarised zones), remote access security, authentication systems, updating and patching procedures, as well as the cybersecurity considerations associated with selection of suppliers, must be defined from the design stage.

How can the implementation of the appropriate cybersecurity and control technology impact on the cost of investment and maintenance of a water management project?

What is really important is the cost of not implementing it. The costs associated with recovering from cyber-attacks and repairing damage can be far higher than investments in preventive measures.

In terms of investment in large new-build infrastructures, the cost associated with cybersecurity is minimal compared to the total cost of the infrastructure, especially when cybersecurity is integrated from the design stage. In existing infrastructures, the cost can be high. In many cases, the control systems are old and complete migrations may be necessary to bring them into line with current cybersecurity standards.

The cost of maintaining cybersecurity technology in water infrastructure operation and maintenance projects could be compared to the cost of maintaining control systems, to give an idea. Cybersecurity procedures defined for the project must be followed and the necessary operations must be integrated into computerised maintenance management systems (CMMS). It should also be borne in mind that trained, cybersecurity-aware personnel are required.

Each plant or service is unique in terms of design, operation and cyber security risks, so the measures needed to mitigate these risks will vary, as will the investment required. There is no single one-size-fits-all solution.

Are there big differences in the implementation of the solutions you work with in your

ciberseguridad.

Cada planta o servicio es único en cuanto a diseño, operación y riesgos en ciberseguridad, por lo que las medidas necesarias para mitigarlo variarán, así como la inversión necesaria. No hay una única solución correcta.

¿Existen grandes diferencias a la hora de implantar las soluciones sobre las que Vds operan en su departamento dependiendo del tipo de planta de tratamiento de agua sobre la que se va a trabajar: depuradora, desaladora, potabilizadora?

No hay grandes diferencias por la tipología de las plantas, se aplican las mismas tecnologías. Sí hay algunas diferencias en función del país, ya que las regulaciones pueden variar en algunos casos.

A nivel internacional, ¿en qué mercados están trabajando más intensamente implantada la ciberseguridad en estos momentos?

A nivel internacional, la implantación de la ciberseguridad se está dando en diversos mercados, siendo algunos de los más destacados:

- Infraestructuras críticas: los países están trabajando en reforzar la seguridad de sectores con infraestructuras críticas como energía, agua, transporte y salud.
- Sector financiero: la seguridad en el sistema financiero es prioritaria. Las instituciones financieras siempre han estado a la cabeza en medidas de ciberseguridad.
- Salud: la protección de los datos de los pacientes y la seguridad de las instalaciones hospitalarias son áreas críticas y que en los últimos años se han convertido en objetivo de ciberdelincuentes.
- Tecnología de la información y comunicaciones: debido a la interconexión global y la dependencia de las comunicaciones, la ciberseguridad en el ámbito de las TI y las comunicaciones es vital. Los países están intensificando los esfuerzos en ciberseguridad para proteger las infraestructuras y sistemas militares, asegurando la integridad y confidencialidad de la información estratégica.
- Empresas de Tecnología y Fabricación: se está trabajando en la seguridad de la cadena de suministro, para asegurar la producción de elementos críticos.

La ciberseguridad es un tema transversal y su implantación es relevante en una amplia gama de sectores, y avanza a la misma medida que la digitalización. La colaboración internacional y el intercambio de mejores practicas son fundamentales para hacer frente a las ciberamenazas de manera efectiva en los diversos mercados.

department depending on the type of water treatment plant you are going to work on: wastewater treatment plant, desalination plant, drinking water treatment plant?

There are no major differences for the different plant types. The same technologies are applied. There are some differences depending on the country, as regulations may vary in some cases.

At international level, in which markets is cybersecurity currently being implemented most intensively?

Internationally, cybersecurity is being implemented in a number of markets, some of the most prominent being:

- Critical infrastructure: countries are working to strengthen the security of critical infrastructure sectors such as energy, water, transport and health. Financial sector: security in the financial system is a priority. Financial institutions have always been at the forefront of cybersecurity measures.
- Health: the protection of patient data and the security of hospital facilities are critical areas that have been targeted by cybercriminals in recent years.
- Information and communications technology: Due to global interconnectedness and dependence on communications, cybersecurity in the IT and communications domain is vital. Countries are stepping up cybersecurity efforts to protect military infrastructures and systems, with a view to guaranteeing the integrity and confidentiality of strategic information.
- Technology and manufacturing companies: work is being done on supply chain security to secure the production of critical items.

Cybersecurity is a cross-cutting area. Its deployment is relevant across a wide range of sectors and it is advancing at the same pace as digitisation. International collaboration and sharing of best practices are essential to effectively address cyber threats in different markets.

How would you assess the level of cybersecurity in the Spanish water treatment sector? What added value can we offer in today's competitive market?

In broad terms, the maturity of cybersecurity in this sector can vary, but it is imperative to continue to strengthen existing measures and take proactive approaches. In the water treatment sector, we face new cybersecurity challenges arising from the digitisation of processes and systems, which often make the separation between the OT and IT worlds indistinguishable.

¿Cómo valoraría el nivel en ciberseguridad que mantiene el sector del tratamiento del agua en nuestro país? ¿Qué valor añadido podemos ofrecer en un mercado tan competitivo como el actual?

En general, la madurez de la ciberseguridad en este sector puede variar, pero es imperativo seguir fortaleciendo las medidas existentes y adoptar enfoques proactivos. En el sector del tratamiento del agua nos enfrentamos a nuevos desafíos en materia de ciberseguridad debido a la digitalización de procesos y sistemas, que hacen indistinguible en muchas ocasiones la separación entre mundo OT y mundo IT.

El valor añadido que podemos aportar es la innovación continua, adoptando tecnologías avanzadas como inteligencia artificial y aprendizaje automático, la aplicación de estándares internacionales como la IEC 62443, ofreciendo un enfoque integral que, junto a la propia tecnología, aporte concienciación y conlleve a una formación continua, contribuyendo a un proceso de cambio para tratar de evolucionar, al menos, a la misma velocidad que las amenazas.

El valor añadido radica en la capacidad de garantizar la seguridad de las infraestructuras críticas de tratamiento de agua de manera proactiva, eficiente e innovadora. La transparencia, la colaboración y el compromiso continuo con la mejora de la ciberseguridad son elementos clave.

¿Cómo dibujaría el futuro de la ciberseguridad a partir de los desarrollos que están previstos o se prevén- se puedan implantar?

Por un lado, continuará el incremento de los ciberataques industriales, pero por otro, y afortunadamente, la concienciación en la importancia de la ciberseguridad está aumentando cada vez más y lo hará a ritmo exponencial.

La tipología de los ciberataques ha condicionado nuestra respuesta, impulsándonos a adoptar enfoques más proactivos, por lo que es primordial mejorar nuestras capacidades de detección y respuesta ante amenazas, considerando ataques específicos del sector para desarrollar estrategias adaptadas y eficaces.

Se generalizará la aplicación de tecnologías avanzadas, como la inteligencia artificial y el aprendizaje automático, que ya se están utilizando para detectar patrones anómalos en el trafico y prevenir ataques. Además, habrá una mayor adopción de sistemas de monitoreo en tiempo real en los entornos de operación, lo que permitirá la detección temprana de amenazas.

The added value we can bring is continuous innovation, adopting advanced technologies such as artificial intelligence and machine learning, the application of international standards such as IEC 62443, providing a comprehensive approach that, together with the technology itself, raises awareness and leads to ongoing training, contributing to a process of change to try to evolve at least at the same speed as the threats.

The added value lies in the ability to ensure the security of critical water treatment infrastructures in a proactive, efficient and innovative manner. Transparency, collaboration and continuous commitment to improving cybersecurity are key elements.

How would you envisage the future of cybersecurity based on the developments that are planned, or expected to be deployed?

On the one hand, the increase in industrial cyber-attacks will continue, but on the other hand, and fortunately, awareness of the importance of cyber-security is growing and will do so at an exponential rate.

The type or nature of cyber-attacks has conditioned our response, prompting us to adopt more proactive approaches. This makes it vital to improve our threat detection and response capabilities by looking at sector-specific attacks to develop tailored and effective strategies.

The application of advanced technologies, such as artificial intelligence and machine learning, which are already being used to detect anomalous traffic patterns and prevent attacks, will become more widespread. Moreover, there will be increased adoption of real-time monitoring systems in operating environments, enabling early detection of threats.