# “Las normativas como NIS2 son clave para que la ciberseguridad deje de ser opcional”

**Hablamos con Alfonso Barea Martín-Castaño, Administrador IT y Ciberseguridad de DCOOP, una de las mayores cooperativas agroalimentarias de Europa, sobre su visión estratégica de la seguridad, los desafíos diarios a los que se enfrenta y cómo están abordando en su compañía tendencias como Zero Trust, la inteligencia artificial o el cumplimiento normativo. Una conversación que deja claro que la tecnología es solo una parte del reto: el verdadero cambio empieza en la cultura.**

**Alfonso Barea Martín-Castañoz,**
Administrador IT y Ciberseguridad de **DCOOP**

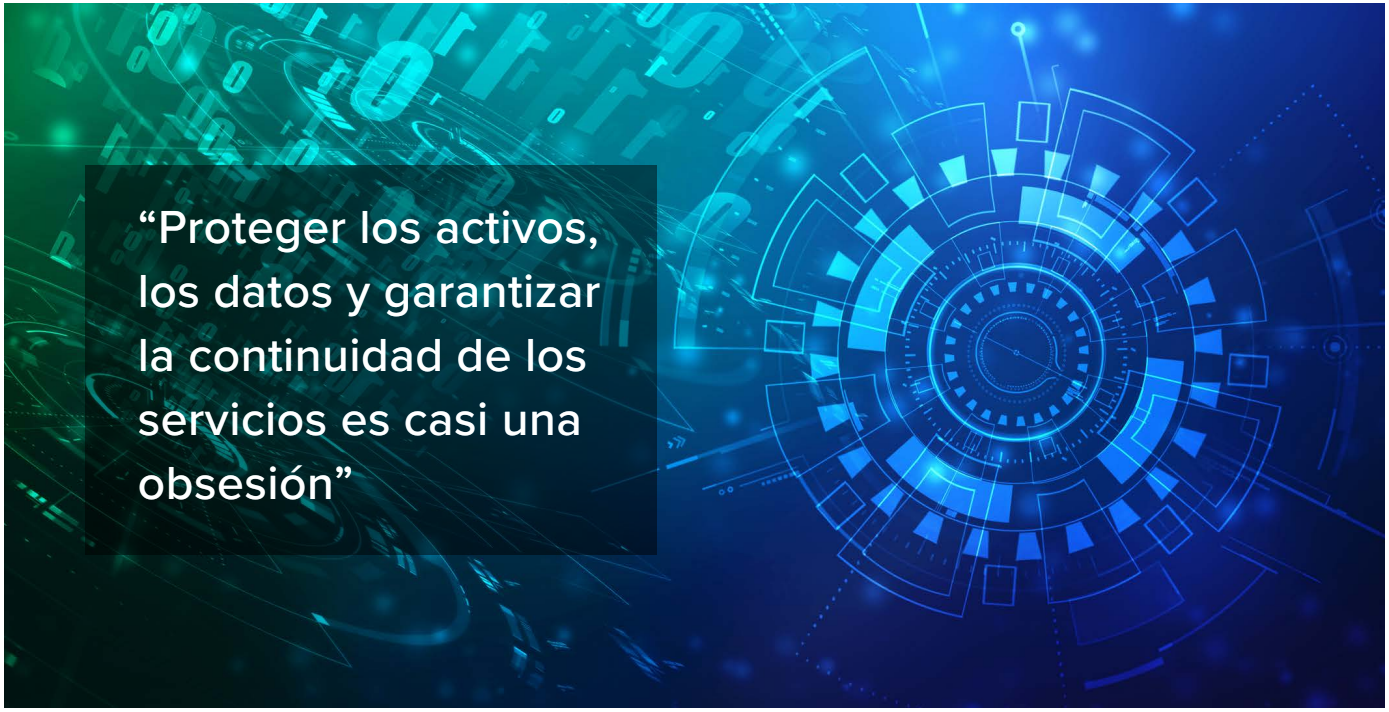
Alfonso Barea Martín-Castaño llegó a la ciberseguridad tras trabajar en sectores altamente exigentes como el sanitario y el industrial, donde esta disciplina requiere el máximo rigor y dominio de los conceptos clave. Su salto a DCOOP, una de las principales cooperativas agroalimentarias de Europa, supuso un nuevo reto, pero también una oportunidad para aplicar todo ese conocimiento en un entorno en plena transformación digital.

Nada más incorporarse a la organización, Barea realizó una auditoría interna para conocer el estado real de la ciberseguridad y definir una hoja de ruta que permitiera fortalecer los puntos débiles. Fue entonces cuando la dirección decidió apostar firmemente por la seguridad como pilar estratégico; “nuestra dirección apostó por hacer de la ciberseguridad una prioridad, y asumí el reto de reforzar la protección de la organización y garantizar un entorno más seguro”, asegura el responsable de ciberseguridad de DCOOP.



IR A PÁGINA SIGUIENTE

El trabajo de un responsable de ciberseguridad se desarrolla en un terreno cada vez más hostil, donde las amenazas evolucionan constantemente. Barea lo sabe bien. En su día a día, se enfrenta a una gran variedad de amenazas digitales y considera que proteger los activos, los datos y garantizar la continuidad de los servicios es más que una responsabilidad: “Es casi una obsesión”, afirma. La presión diaria para asegurar infraestructuras críticas se ve además multiplicada por la necesidad de implicar a toda la plantilla en esta tarea colectiva. “Siempre digo que puedes tener la mejor tecnología, pero si los empleados no siguen buenas prácticas, tienes un problema”, advierte.




Además, destaca la importancia de estar siempre un paso adelante, ya que las amenazas evolucionan constantemente. “Mantenerse actualizado es clave para anticiparse a los riesgos”. Otro desafío que enfrenta es lograr el equilibrio entre seguridad y operatividad, especialmente en una organización con más de 800 empleados y múltiples sedes. “A veces es complicado que todo esté en armonía, pero es fundamental que la seguridad no sea un obstáculo, sino un facilitador del negocio”, sostiene.

## Tecnología al servicio de la visibilidad

En materia tecnológica, Barea no duda al señalar que la base de cualquier estrategia eficaz comienza por una correcta ‘ciberhigiene’. Parchear sistemas, cerrar sesiones inactivas o controlar accesos son tareas básicas, pero a menudo olvidadas. “No sirve de nada invertir en grandes soluciones si hay vulnerabilidades abiertas por falta de mantenimiento”, apunta.

En cuanto a las tecnologías esenciales para la seguridad de TI, Barea considera imprescindibles herramientas como EDR/XDR, firewalls bien configurados y una monitorización completa de la red. “Si no tienes visibilidad de lo que está pasando en tu red, vas a ciegas”, advierte. También subraya la importancia de man-

tener los equipos parcheados y actualizados, pues no sirve de nada invertir en grandes soluciones si hay vulnerabilidades abiertas por falta de mantenimiento. En DCOOP, han apostado recientemente por la tecnología Zero Trust y la protección del DNS, un punto que, según Barea, muchas empresas descuidan en sus estrategias de seguridad.

Cuando se le pregunta por la amenaza que más le preocupa, no duda en señalar el ransomware. “Es una amenaza que no deja de evolucionar y, si un ataque tiene éxito, puede paralizar por completo una empresa”, explica. Destaca que este tipo de ataque se propaga con gran rapidez y cada vez es más sofisticado, por lo que es crucial estar preparados tanto para prevenirlo como para recuperarse en el menor tiempo posible. “Es importante tener una estrategia bien definida. Un ataque de este tipo puede hacer mucho daño...”, advierte.

Para Barea, su mayor fracaso no sería solo un incidente crítico que paralizara la actividad, sino también no conseguir que la dirección y los empleados comprendan la importancia de la seguridad. “Si no logro inculcar esa cultura, todo lo demás carece de sentido”, afirma. En este sentido, destaca que el mayor logro de su carrera no ha sido un proyecto tecnológico en sí, sino haber conseguido transmitir la cultura de ciberseguridad en las organizaciones donde ha trabajado. “Concienciar, reforzar nuestro ‘escudo humano’ y elevar el nivel de ciberresiliencia ha sido clave. Cambiar el status quo y ver cómo la seguridad se convierte en una prioridad real dentro de la empresa es, sin duda, lo más gratificante”, asegura.


## NIS2 y el necesario cambio de mentalidad

El nuevo marco normativo europeo, representado por la directiva NIS2, está marcando un antes y un después para muchas organizaciones. Su objetivo: elevar el nivel mínimo de ciberseguridad en sectores esenciales y de importancia para la economía y la sociedad. Para Barea, este avance es bienvenido, pero con matices.

“Está elevando el nivel de exigencia en ciberseguridad, algo positivo y necesario”, reconoce. Sin embargo, también advierte de las dificultades que supondrá para muchas empresas: “La adaptación no será sencilla, ya que implica cambios estructurales”.

En el caso de España, señala un reto particular. “Todavía hay empresas que ven la ciberseguridad como un gasto en lugar de una inversión estratégica”, comenta. Y concluye que normativas como NIS2 son esenciales para que la seguridad “deje de ser opcional y pase a ser un pilar clave del negocio”.

Sobre las tendencias en ciberseguridad, señala que en DCOOP llevan un año trabajando en un entorno basado en Zero Trust y SASE, lo que ha supuesto un gran avance respecto al modelo tradicional de VPN. “Hoy en día, ya no se puede confiar en nada por defecto, ni dentro ni fuera de la red”, sostiene. También considera crucial la gestión de la postura de seguridad en datos, aplicaciones y entornos cloud (DSPM, ASPM, CSPM), ya que cada vez más empresas

> “La seguridad no debe ser un obstáculo, sino un facilitador del negocio”

dependen de estos entornos. En cuanto a la seguridad IoT, subraya que la segmentación y el control de accesos externos son vitales.

Respecto a los servicios de ciberseguridad, destaca su importancia como complemento a la infraestructura interna de TI. “En muchas ocasiones, no podemos cubrir todo, y ahí es donde entran los partners”, señala. En DCOOP, trabajan con proveedores de primer nivel que los asesoran, auditan y monitorizan 24/7, ayudándolos a mantener un alto nivel de protección. “Su aporte es clave para seguir fortaleciendo nuestra estrategia de ciberseguridad”, enfatiza.

Por último, al abordar la irrupción de la inteligencia artificial, destaca que, desde el punto de vista de la seguridad, es una herramienta poderosa para la detección de amenazas y la automatización de procesos, pero también reconoce su potencial para facilitar los ataques. “Ya estamos viendo phishing hiperrealista y hasta malware que se adapta en tiempo real”, advierte. Asimismo, señala que el gran reto en el uso de la IA a nivel empresarial será la gestión de la privacidad de los datos. “Tenemos que aprender a utilizarla para ser más eficientes y mejorar la seguridad, sin que se convierta en una herramienta que genere nuevos riesgos. La clave está en encontrar ese equilibrio”, concluye.