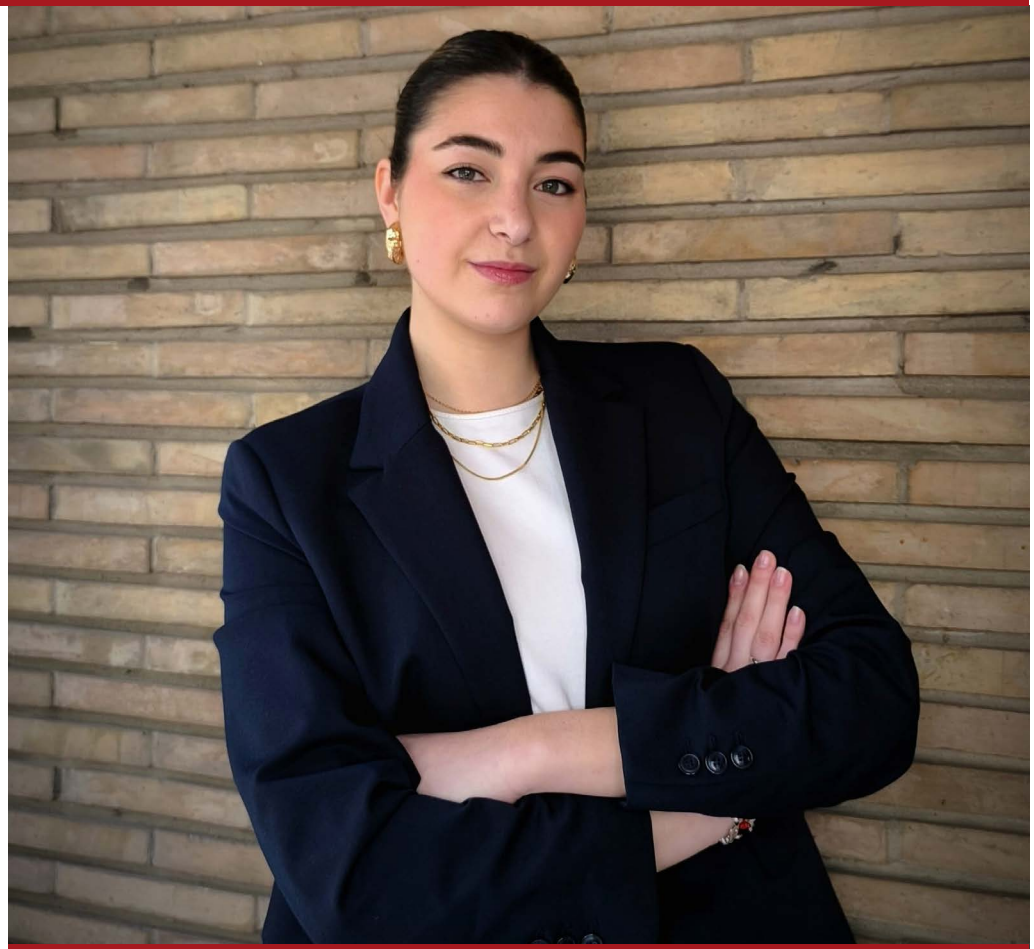
Laura Guiance (Harvong Holding): “Sin capacidad de adaptación, un CISO fracasa”

Hablamos con Laura Guiance, International Business Developer de Harvong Holding, quien deja claro que, a la hora de escoger, se valora a los proveedores “que entienden nuestro negocio y recomiendan desde la experiencia, no desde el catálogo” o que se necesitan herramientas que validen la legitimidad de las comunicaciones, sea cual sea el canal.



Laura Guiance,
International Business Developer de **Harvong Holdin**

Harvong Holding es una compañía con presencia internacional dedicada a sectores estratégicos como la ingeniería, la energía y la logística. Su modelo de negocio global, basado en colaboraciones con múltiples socios y proveedores en distintos países, exige una estrategia de ciberseguridad altamente adaptable, capaz de anticiparse a amenazas complejas y de cumplir con normativas locales e internacionales.

Con una visión estratégica, práctica y muy enfocada en la concienciación y la adaptación, Laura Guiance, International Business Developer de Harvong Holding y quien está en contacto constante con el equipo de seguridad, ya que, al estar en primera línea de batalla, debe estar al tanto de todas las amenazas posibles. Muy valorada la perspectiva que puede dar

IR A PÁGINA SIGUIENTE

sobre su día a día, asegura necesitar “estar bien formada y contar con un conocimiento mínimo de los temas relacionados con la ciberseguridad”. En esta entrevista, repasa el impacto de normativas como NIS2, el papel de la inteligencia artificial, la gestión de riesgos globales y la necesidad de combinar innovación y seguridad sin perder el foco en lo esencial: las personas.

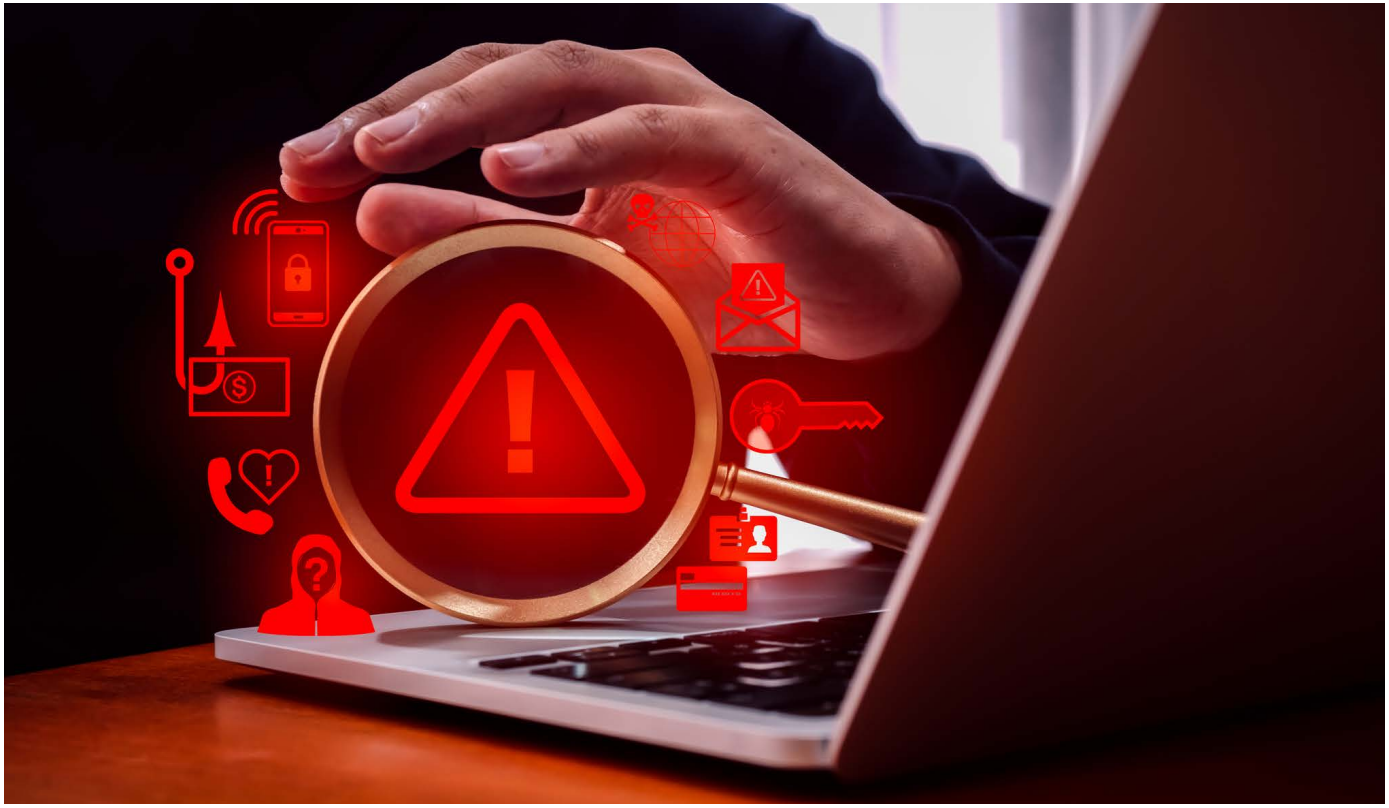
La importancia de saber comunicar

Para Laura, las cualidades técnicas de un CISO son fundamentales, pero no suficientes. “Puedes tener toda la teoría, pero si no sabes comunicarlo, no sirve de nada”, afirma. La capacidad de transmitir la estrategia y los riesgos al resto de la organización, desde los empleados hasta la alta dirección, es uno de los pilares de su liderazgo. A eso suma experiencia, análisis, visión estratégica y, sobre todo, flexibilidad para adaptarse a distintos entornos y necesidades empresariales.

Harvong Holding opera a nivel global, lo que implica una complejidad adicional en la gestión del riesgo. Laura destaca que uno de los mayores retos es adaptarse a las cadenas de suministro de otras empresas y a las normativas que aplican en diferentes países. “Muchas veces tú lo haces de una manera, pero en otros países no está aceptado o se requiere un enfoque distinto. Hay que cubrirse las espaldas lo más posible”, explica Laura Guiance. Por eso, insisten en seguir procesos rigurosos y proteger cada paso con especial atención a la legislación local.

Phishing e inteligencia artificial

Cuando se le pregunta por la amenaza que más le inquieta, Laura no duda: “El phishing, totalmente”. Especialmente le preocupa la suplantación de identidades que afectan a los métodos



> “El phishing y la suplantación de identidades, especialmente en métodos de pago, son preocupantes”

de pago. “Puede parecer algo pequeño, pero en nuestro negocio se hacen transacciones muy importantes. Por eso necesitamos tener un buen sistema de backup y estar siempre alerta”, indica Laura Guiance.

En Harvong Holding, se han incorporado herramientas de inteligencia artificial con el objetivo de agilizar procesos clave, como la verificación de proveedores y clientes. Según explica Laura, CISO de la compañía, “en ocasiones, un proveedor puede ofrecer una buena impresión inicial, pero al avanzar en el proceso surgen señales de alerta, como la negativa a realizar videollamadas o inconsistencias en las firmas. En esos casos, el uso de IA resulta fundamental para contrastar registros y detectar posibles incoherencias que podrían pasar desapercibidas en una revisión convencional”.

No obstante, Laura advierte sobre los riesgos de utilizar herramientas de inteligencia artificial sin la formación adecuada. “Lo estamos abordando desde la educación. No se trata de generar miedo, sino de fomentar el respeto hacia estas tecnologías”, señala. Desde su punto de vista, la formación continua es esencial para que los empleados comprendan qué tipo de información debe protegerse y cuáles son las posibles consecuencias de compartir datos sensibles sin el debido control. “Del mismo modo que nadie subiría su DNI a una herramienta de IA, los datos corporativos deben tratarse con el mismo nivel de precaución”, subraya.

NIS2 y concienciación

En relación a la directiva NIS2, Laura reconoce que uno de los mayores desafíos ha sido lograr una estrategia homogénea. “Cada país ha traspuesto la normativa a su manera, y eso nos obliga a dedicar mucho tiempo a buscar esa homogeneidad”, explica Laura Guiance. Esa fragmentación normativa añade complejidad a la protección de activos e infraestructuras críticas, algo que desde su equipo se está abordando con planificación y trabajo colaborativo.

Desde hace aproximadamente un año, Harvong Holding ha incorporado de forma estructural la concienciación en su estrategia global de ciberseguridad. La compañía ha puesto en marcha un programa continuo que combina simulaciones periódicas de ataques de phishing con píldoras formativas quincenales, diseñadas para mantener a los empleados actualizados frente a las amenazas más recientes.

“Nuestro objetivo es que los profesionales sepan identificar correos que, aunque aparentan legitimidad, presentan señales de alerta —como un dominio ligeramente alterado que simula ser el de un superior jerárquico—”, explica Laura Guiance. En este sentido, insiste en que

el enfoque no pasa por generar miedo, sino por fomentar el pensamiento crítico. “No se trata de que los empleados eliminen todo por precaución, sino de que aprendan a analizar con sentido común y actúen con criterio ante posibles riesgos”.

Cómo elegir soluciones en un mercado saturado

A la hora de seleccionar soluciones de ciberseguridad, desde Harvong Holding se priorizan aspectos como la confianza, la claridad y la capacidad de adaptación a las particularidades del negocio. Laura destaca la importancia de trabajar con proveedores que vayan más allá de una propuesta comercial estándar y que demuestren un conocimiento real de las necesidades de la organización. “Valoramos especialmente a quienes no se limitan a vender, sino que escuchan, entienden y recomiendan lo que realmente encaja con nuestro entorno operativo”, explica la responsable de Ciberseguridad de la compañía añadiendo que, para ella, la honestidad es un factor determinante: “Buscamos sinceridad, incluso si eso implica apostar por soluciones más costosas. Lo prioritario es estar bien protegidos y garantizar la continuidad del negocio”.

> “Puedes tener toda la teoría, pero si no sabes comunicarla, no sirve de nada”

En el caso de los servicios gestionados, Laura Guiance subraya que la experiencia práctica del proveedor es tan importante como la solución que ofrece. “Tiene que notarse que saben de lo que hablan”, afirma, advirtiendo que, en ocasiones, algunos interlocutores simplemente repiten información sin comprenderla a fondo. Por ello,

considera esencial que los proveedores sean capaces de comprender con agilidad el contexto específico de la organización y proponer alternativas adecuadas, incluso si eso implica reorientar las expectativas iniciales. “Ese conocimiento aplicado marca la diferencia entre un buen partner y una relación fallida”, concluye.

La línea roja del fracaso

Sobre lo que podría hacer fracasar a un CISO, Laura no duda: “No saber adaptarse y no saber comunicar. Si no eres capaz de transmitir a la dirección que algo es importante y que hay que hacerlo, has fracasado”. En su opinión, un CISO necesita una mínima autoridad y la capacidad de influir en las decisiones estratégicas. “Si no tienes eso, es como darte golpes contra la pared”, concluye.

Aunque reconoce que el ecosistema tecnológico ofrece un abanico cada vez más amplio de soluciones, Laura considera que una de las prioridades a corto plazo será reforzar el control sobre los canales de comunicación. De manera concreta habla de un “filtro avanzado de comunicaciones” explicando que se reciben contactos por vías tan diversas como WhatsApp o llamadas directas, “y en muchos casos es difícil verificar la identidad real del interlocutor o el origen del contacto”, señala. En este contexto, subraya la importancia de incorporar herramientas de filtrado avanzadas que permitan validar la legitimidad de las comunicaciones y evitar que estos canales se conviertan en puertas de entrada para ataques de ingeniería social o suplantación de identidad.