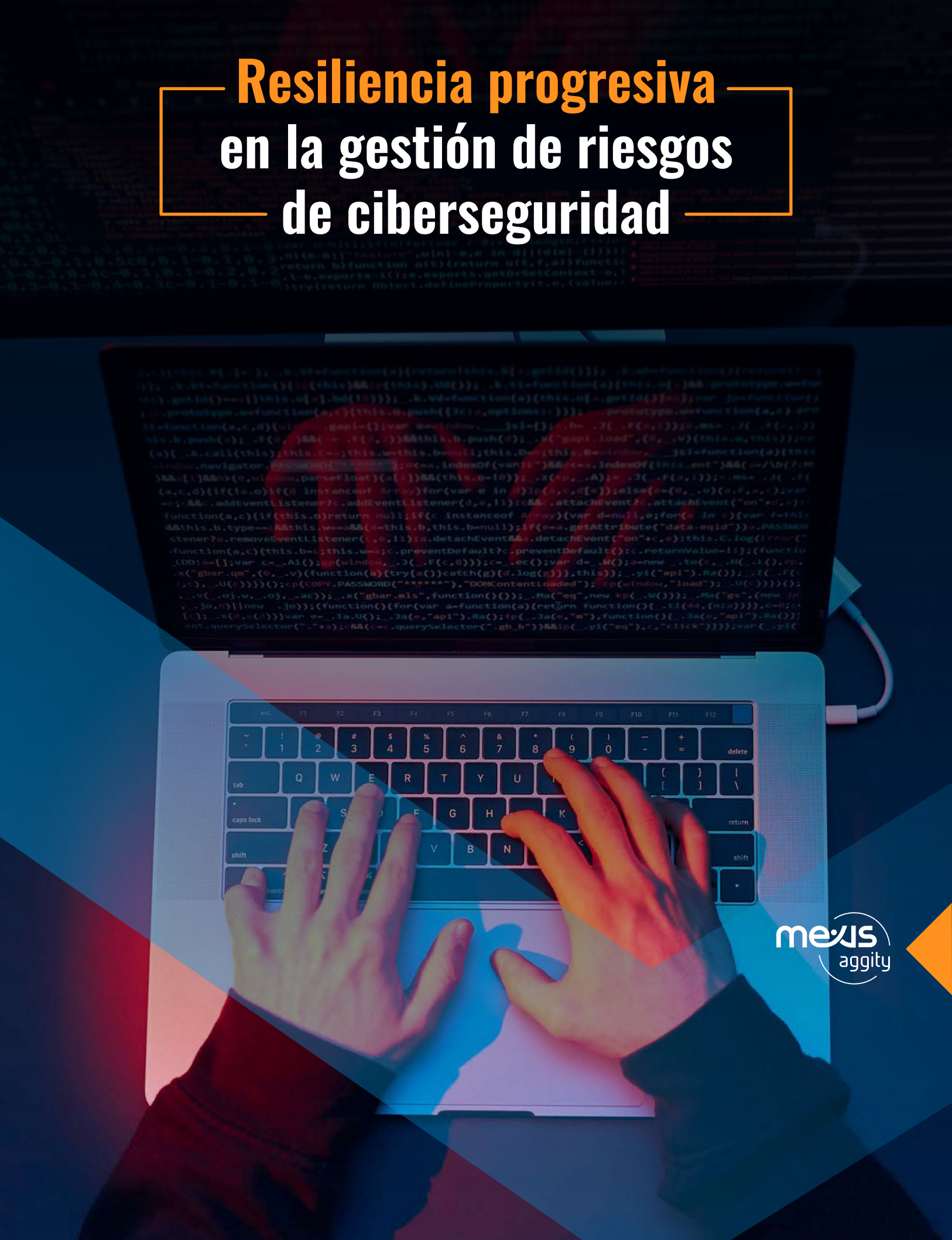
Resiliencia progresiva en la gestión de riesgos de ciberseguridad

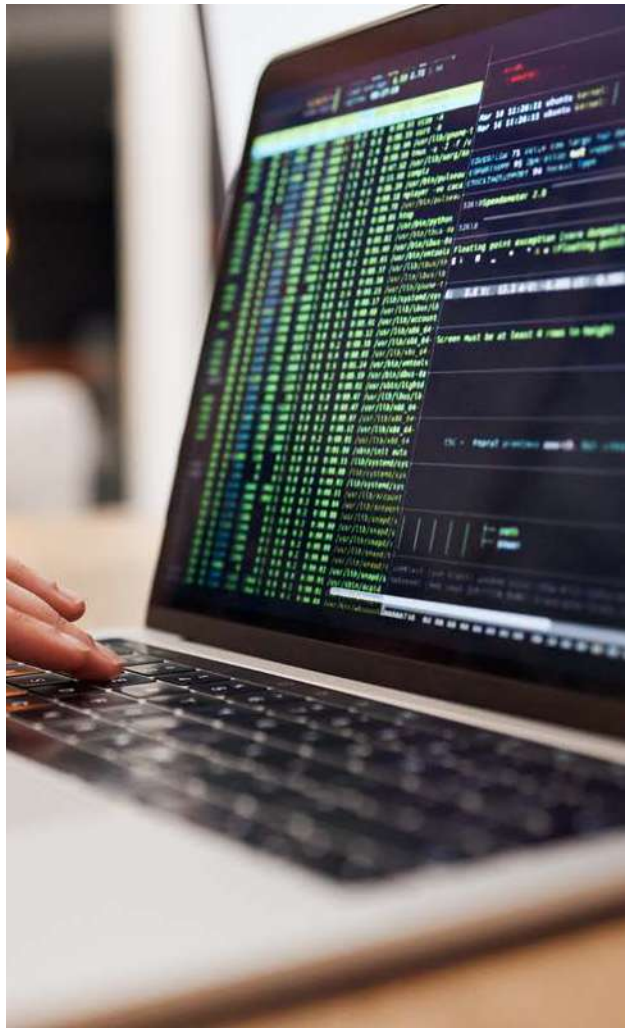


mexis aggity

Los entornos universitarios son naturalmente abiertos, por lo que riesgo de ciberseguridad es una preocupación constante.

Intentar bloquear la red como lo haría con una empresa comercial no está en las cartas. Aun así, resulta tentador en un entorno en el que departamentos, profesores o estudiantes individuales introducen sus propias nuevas tecnologías, dispositivos o aplicaciones en la red. En lugar de intentar acabar con nuevas tendencias, cambiar comportamientos o prohibir nuevos dispositivos y paradigmas de comunicación, nuestro departamento de TI adoptó una estrategia de resiliencia progresiva. **Resiliencia progresiva significa adaptarse a los cambios técnicos y de comportamiento, en lugar de prohibirlos.**

¿Cómo adoptamos esta estrategia? Al reconocer que nuestra infraestructura de gestión de riesgos cibernéticos necesitaba volverse más flexible. Para realizar los cambios necesarios, necesitábamos apoyo administrativo, una plataforma sólida de ciberseguridad y la financiación para hacerlo realidad.

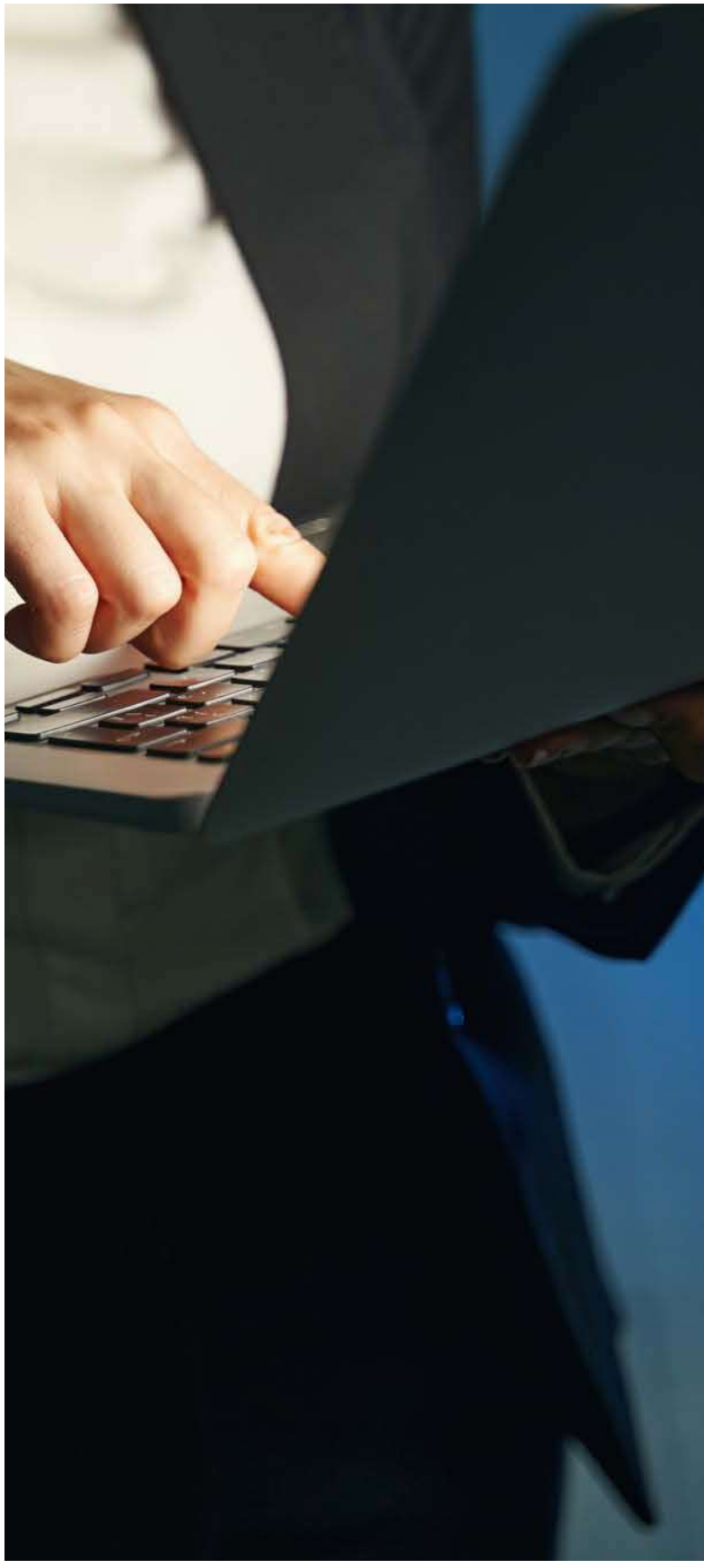


Obtener la aceptación de las partes interesadas

Cualquier esfuerzo para reorientar la TI debe ser impulsado desde arriba hacia abajo, por lo que el primer paso fue lograr su aceptación. Uno de nuestros mayores desafíos fue la financiación, lo que significó obtener la aprobación del Canciller y de la junta. **Todo el mundo sabe que las iniciativas de riesgo cibernético son una carrera armamentista contra los malos actores.** A menudo implican una competencia de contratación con empresas tecnológicas bien remuneradas que buscan analistas de seguridad del mismo grupo de talentos. Con el apoyo de la junta, pudimos obtener los fondos que necesitábamos para contratar a las personas que necesitábamos para transformar nuestra la seguridad cibernética infraestructura.

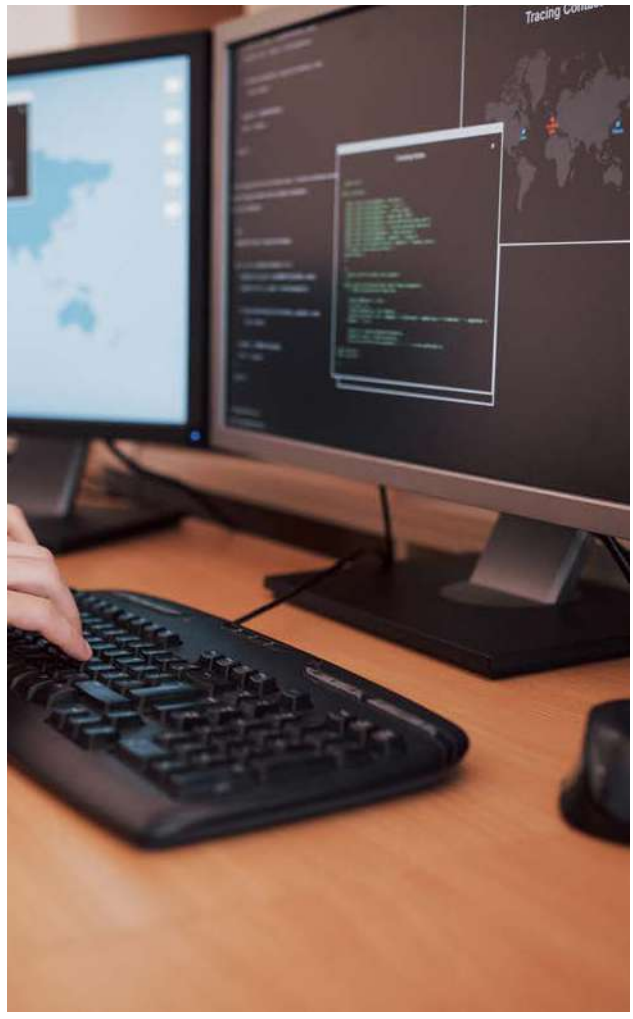
Identificar la plataforma adecuada

Para gestionar mejor el riesgo en un entorno de TI diverso y heterogéneo, nuestras herramientas, departamentos y terminales de seguridad tuvieron que unirse en una sola plataforma. En consecuencia, tuvimos que decidir cómo consolidar muchas de estas piezas de manera realista. Tuvimos que preguntarnos qué pasos se requieren para tener todo esto en una sola plataforma. **¿Cómo podríamos reducir nuestros costos generales y al mismo tiempo optimizar nuestra eficiencia? ¿Cómo podríamos medir cualitativamente y comunicar la efectividad del programa a nuestra junta directiva?**



Evaluamos múltiples soluciones para integrar las piezas en una sola plataforma. Teníamos herramientas separadas y aisladas, como detección de red, SIEM e IPS/IDS, y queríamos reunirlas todas en una consola de administración central. Necesitábamos una solución que pudiera ver toda la red y sus puntos finales pero que no volviera locos a nuestros analistas con miles de alertas diarias.

Nosotros consideramos Plataformas XDR porque nos permitieron colapsar parte de nuestro software heredado para obtener un mejor retorno de la inversión con mayor eficiencia y resultados de mayor calidad. Analizamos las plataformas XDR y Abrir XDR. Muchos Plataformas XDR eran SIEM mejorados o herramientas de punto final. Al mismo tiempo, Abrir XDR nos brindó una mayor flexibilidad para mejorar las numerosas tecnologías de nuestra pila de seguridad existente y al mismo tiempo ofrecer un conjunto completo de herramientas de seguridad de forma nativa en la plataforma.



Elegimos un Abierto Plataforma XDR de Ciber estelar. Con él, podríamos incorporar nuestras herramientas existentes mientras recopilamos y correlacionamos automáticamente todas las fuentes de nuestros firewalls, puntos finales y entornos locales y de nube. La plataforma también permitió a nuestros analistas profundizar rápidamente en los incidentes (más allá de las alertas fundamentales) para poder centrarse en la remediación. Esto redujo los costos operativos y mejoró la eficiencia, redujo el "agotamiento de alertas" de los analistas y brindó mejores resultados de gestión de riesgos para la universidad.

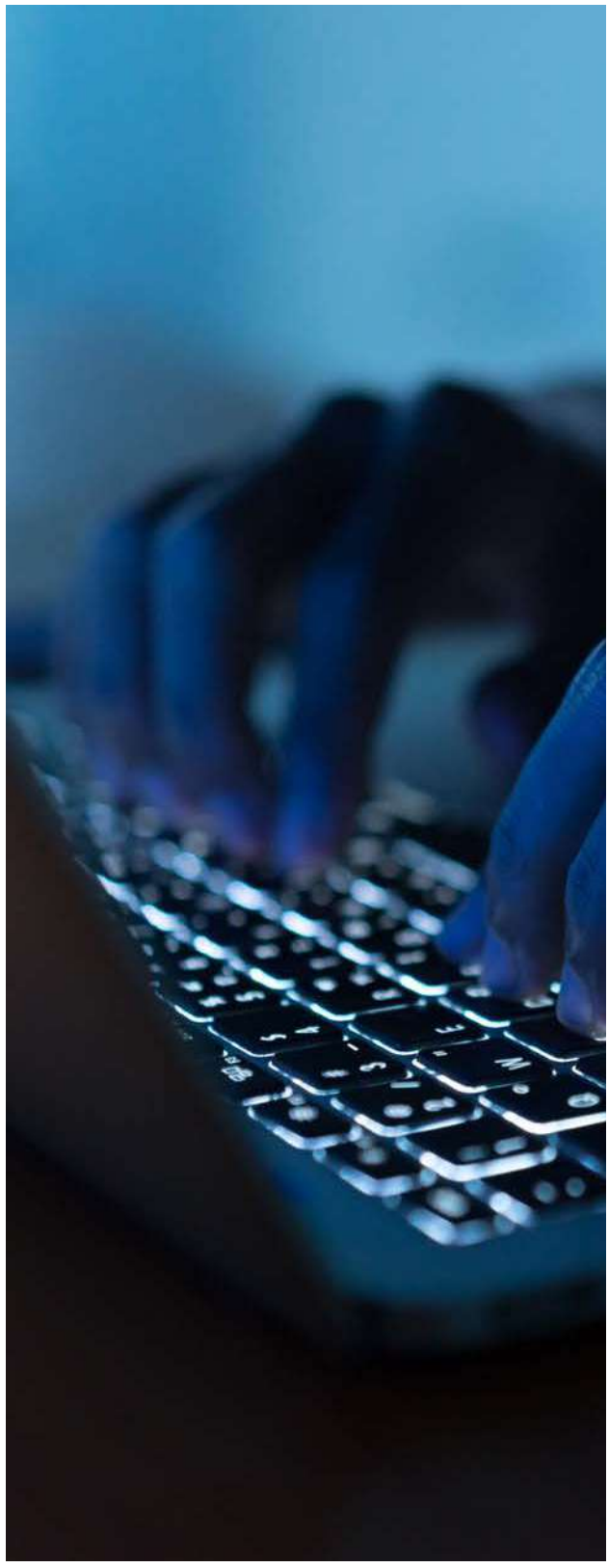
Alinearse con la junta

Una conciencia más ilustrada de la seguridad cibernética Los riesgos ayudaron a alinear nuestros equipos de TI y seguridad y aquellos en la junta directiva con respecto a la estrategia y la financiación. Nos comunicamos regularmente y con total transparencia al directorio. **Contratamos a una empresa externa para que realizara una auditoría que mostrara dónde estábamos en el frente de la ciberseguridad.** Esa auditoría externa demostró a la junta directiva que no sólo nos estábamos mirando a nosotros mismos internamente, sino que brindó una validación más objetiva de dónde estábamos y dónde necesitábamos estar.

La junta directiva estaba de acuerdo y empezó a hacernos las preguntas difíciles. Querían saber cuándo nos comunicaríamos con ellos con respecto a las actualizaciones de TI y cómo redujeron nuestra exposición al riesgo. **Comunicamos nuestro estado de seguridad y actividad con informes mensuales escritos en términos con los que los miembros de la junta podrían identificarse personalmente, mostrando la cantidad de ataques de phishing, virus o intrusiones que habíamos evitado.**

Para nosotros, desarrollar una resiliencia progresiva fue un proceso de convencer, consolidar y comunicar.

Teniendo esto en cuenta, puede impulsar una resiliencia progresiva en su propia organización de TI para gestionar mejor los riesgos de ciberseguridad.



Autor Bio: Russell Kaurloto
Fuente de información: stellarcyber.ai