

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
School of Professional & Executive Development

TPRM en el sector financiero

por

Marc Gracia i Riera

Trabajado realizado en parte con los conocimientos adquiridos en el máster de

CYBERSECURITY MANAGMENT

Tutor: Jordi Arumí
Directora: Txell Pineda i Teixidó

Barcelona. Verano 2023

Abstract

In the financial sector, third party risk management has become an essential practice to ensure the stability, security and continuity of financial operations. This strategy has become even more crucial in a globalised and highly competitive business environment, where organisations rely heavily on a network of suppliers to provide critical services and solutions.

Supplier risk management involves identifying, assessing and mitigating potential threats and issues that could arise in the supplier relationship. These risks can range from compliance and cyber security issues to operational and financial issues. A failure in any of these areas could have a significant impact on the reputation of the financial institution, its position in the market and, ultimately, on the trust of its customers.

In this context, the present project focuses on addressing the challenges related to the procurement of new services and the monitoring of critical suppliers. The project aims to establish a rigorous supplier evaluation process that allows for a more informed and accurate selection when procuring new services. This involves a thorough analysis of the potential risks that each supplier could present, as well as the definition of clear compliance and security criteria.

In addition, the project focuses on the continuous monitoring of critical suppliers. This constant monitoring enables any emerging signs of risk to be detected and proactively addressed, thus avoiding disruptions in the provision of services. Through the implementation of performance metrics and the regular review of contractual agreements, the project aims to ensure that suppliers meet the required standards and are prepared to deal with potential contingencies.

In short, in an increasingly complex and challenging financial environment, supplier risk management is a key pillar for stability and operational excellence. The project presented here is geared towards minimising risks when procuring new services and monitoring critical suppliers, thus contributing to the security, reliability and long-term success of the financial institution in question.

Resum

En el sector financer, la gestió del risc dels proveïdors s'ha convertit en una pràctica essencial per garantir l'estabilitat, la seguretat i la continuïtat de les operacions financeres. Aquesta estratègia s'ha tornat encara més crucial en un entorn empresarial globalitzat i altament competitiu, on les organitzacions depenen en gran mesura d'una xarxa de proveïdors per proporcionar serveis i solucions crítics.

La gestió del risc dels proveïdors implica identificar, avaluar i mitigar les possibles amenaces i els problemes que puguin sorgir en la relació amb els proveïdors. Aquests riscos poden anar des de problemes de conformitat i ciberseguretat fins a qüestions operatives i financeres. Un error en qualsevol d'aquests aspectes podria tenir un impacte significatiu en la reputació de la institució financera, la seva posició al mercat i, en última instància, en la confiança dels seus clients.

En aquest context, aquest projecte se centra a abordar els reptes relacionats amb la contractació de nous serveis i la supervisió dels proveïdors crítics. El projecte pretén establir un rigorós procés d'avaluació de proveïdors que permeti una selecció més informada i precisa a l'hora d'adquirir nous serveis. Això implica una anàlisi exhaustiva dels riscos potencials que podria presentar cada proveïdor, així com la definició de criteris clars de compliment i seguretat.

A més, el projecte se centra en la supervisió continuada dels proveïdors crítics. Aquest seguiment constant permet detectar qualsevol senyal de risc emergent i abordar-lo de forma proactiva, evitant així interrupcions en la prestació de serveis. Mitjançant laplicació de paràmetres de rendiment i la revisió periòdica dels acords contractuals, el projecte pretén garantir que els proveïdors compleixin les normes exigides i estiguin preparats per fer front a possibles contingències.

En resum, en un entorn financer cada cop més complex i difícil, la gestió del risc dels proveïdors s'erigeix en un pilar fonamental per a l'estabilitat i l'excel·lència operativa. El projecte que aquí es presenta està orientat a minimitzar els riscos a l'hora de contractar nous serveis i supervisar els proveïdors crítics, contribuint així a la seguretat, fiabilitat i èxit a llarg termini de la institució financera en qüestió.

Resumen

En el sector financiero, la gestión del riesgo de los proveedores se ha convertido en una práctica esencial para garantizar la estabilidad, seguridad y continuidad de las operaciones financieras. Esta estrategia se ha vuelto aún más crucial en un entorno empresarial globalizado y altamente competitivo, en el que las organizaciones dependen en gran medida de una red de proveedores para proporcionar servicios y soluciones críticos.

La gestión del riesgo de los proveedores implica identificar, evaluar y mitigar las posibles amenazas y problemas que puedan surgir en la relación con los proveedores. Estos riesgos pueden ir desde problemas de conformidad y ciberseguridad hasta cuestiones operativas y financieras. Un fallo en cualquiera de estos aspectos podría tener un impacto significativo en la reputación de la institución financiera, su posición en el mercado y, en última instancia, en la confianza de sus clientes.

En este contexto, el presente proyecto se centra en abordar los retos relacionados con la contratación de nuevos servicios y la supervisión de los proveedores críticos. El proyecto pretende establecer un proceso riguroso de evaluación de proveedores que permita una selección más informada y precisa a la hora de adquirir nuevos servicios. Esto implica un análisis exhaustivo de los riesgos potenciales que podría presentar cada proveedor, así como la definición de criterios claros de cumplimiento y seguridad.

Además, el proyecto se centra en la supervisión continua de los proveedores críticos. Este seguimiento constante permite detectar cualquier señal de riesgo emergente y abordarla de forma proactiva, evitando así interrupciones en la prestación de servicios. Mediante la aplicación de parámetros de rendimiento y la revisión periódica de los acuerdos contractuales, el proyecto pretende garantizar que los proveedores cumplan las normas exigidas y estén preparados para hacer frente a posibles contingencias.

En resumen, en un entorno financiero cada vez más complejo y difícil, la gestión del riesgo de los proveedores se erige en un pilar fundamental para la estabilidad y la excelencia operativa. El proyecto que aquí se presenta está orientado a minimizar los riesgos a la hora de contratar nuevos servicios y supervisar a los proveedores críticos, contribuyendo así a la seguridad, fiabilidad y éxito a largo plazo de la institución financiera en cuestión.

Contents

1 Introducción **7**
1.1 Motivación 7
1.2 Objetivos y alcance 7
1.3 Plan de trabajo 8
1.3.1 Diagrama de Gantt 9
1.4 Desviaciones del plan original e incidencias 9

2 Descripción del proyecto **11**
2.1 Metodología de trabajo 11
2.2 Fases y desarrollo del proyecto 12
2.2.1 Revisión de nuevos proveedores 12
2.2.2 Monitorización continua de proveedores críticos 18
2.2.3 Detección y gestión de los riesgos hallados 21

3 Resultados **23**
3.1 Revisión de nuevos proveedores 23
3.2 Monitorización continua de proveedores críticos 26

4 Conclusiones **27**

5 Trabajo a Futuro **29**

1 Introducción

1.1 Motivación

En mi función de consultor, he tenido el privilegio de embarcarme en un proyecto de vital importancia para el sector financiero, centrado en la optimización y mejora del modelo de gestión de riesgos de proveedores externos (TPRM) de un cliente líder del sector. La motivación de esta colaboración es la clara preocupación del cliente por reforzar su enfoque de la gestión del riesgo de proveedores, al tiempo que trata de racionalizar la identificación de riesgos y mejorar la eficacia en la evaluación de nuevos proveedores.

El cliente reconoció la necesidad de ir más allá de su enfoque anterior y abordar los retos de la gestión del riesgo de los proveedores de una manera más eficaz y eficiente. En este contexto, mi participación como consultor se basa en la capacidad de aplicar sólidos conocimientos de gestión de riesgos y colaborar junto a otros consultores internacionales, así mismo adaptar el proyecto a las necesidades del cliente.

Uno de los aspectos clave de este proyecto es la identificación y mitigación más precisas de los riesgos. Se ha trabajado en la aplicación de criterios de evaluación más rigurosos y en la integración de tecnologías avanzadas para la supervisión constante de los proveedores críticos. Esto permite la detección precoz de señales de riesgo y la adopción de medidas proactivas para evitar posibles perturbaciones en las operaciones financieras.

También se ha dado prioridad a la revisión rápida de nuevos proveedores. Mediante la redefinición de procesos y la eliminación de tareas redundantes, se ha acelerado el proceso de evaluación y aprobación de nuevos proveedores sin comprometer la necesaria exhaustividad de la gestión de riesgos.

En resumen, mi papel como consultor en este proyecto ha sido decisivo para mejorar el modelo de TPRM del cliente en el sector financiero. La atención se ha centrado en optimizar la detección de riesgos y agilizar la revisión de nuevos proveedores, todo ello con el apoyo de una combinación de experiencia en gestión de riesgos y la aplicación de soluciones y nuevas herramientas tecnológicas. La colaboración entre el cliente y mi función de consultor demuestra un compromiso compartido con la excelencia operativa y la mitigación eficaz del riesgo en un entorno empresarial en constante cambio.

1.2 Objetivos y alcance

- **Objetivos:**
  Al implantar un modelo de gestión de riesgos de proveedores, nuestro principal objetivo es revisar los nuevos servicios contratados por la compañía desde la perspectiva de la seguridad de la información y la continuidad de negocio. Aunque esta revisión

es crucial, es importante señalar que, aunque no genere ingresos directos, garantiza que los servicios contratados son seguros y contribuyen a la generación de ingresos.

Nuestro trabajo puede a veces ralentizar la contratación de servicios que son importantes para la generación de ingresos, ya que nos aseguramos de que no haya riesgos que comprometan los datos o interrumpan las operaciones antes de que estos servicios entren en producción. Así que uno de nuestros objetivos clave al implantar este nuevo modelo de gestión de riesgos de terceros ha sido minimizar el tiempo de revisión sin sacrificar la exhaustividad.

- **Alcance:**
  Este modelo se centra en la revisión de nuevos servicios y la monitorización continua de proveedores críticos. Al definir el alcance de las revisiones, las basamos en los estándares de seguridad y continuidad de negocio que son importantes para el cliente, y que son mencionados más adelante. También tenemos en cuenta el nivel de riesgo inherente a cada servicio, evitando exigir el mismo nivel de madurez a todos los proveedores.

1.3 Plan de trabajo

Para el presente proyecto, se estableció un cronograma operativo de seis meses, abarcando desde enero hasta julio. Durante este período, se llevaron a cabo de forma simultánea dos áreas fundamentales de acción. En primer lugar, se procedió a la implementación del renovado proceso de evaluación de nuevos servicios contratados, y en segundo lugar, se efectuó la puesta en marcha del nuevo procedimiento de supervisión continua dirigido a los proveedores de carácter crítico.

1.3.1 Diagrama de Gantt



Figure 1: Diagrama de Gantt

1.4 Desviaciones del plan original e incidencias

A lo largo del proyecto, se suscitaron discrepancias con respecto a ciertos materiales proporcionados por la consultora externa, lo que desembocó en la imposibilidad de mantener la coherencia con el cronograma originalmente planificado para el proyecto.

En consecuencia, en lo que concierne a la tarea integral de implementación del novedoso proceso de evaluación de nuevos proveedores, se vio necesario posponerla hasta finales de septiembre. Esto se debió al hecho de que aún no se había recibido el cuestionario de seguridad definitivo que debía ser completado por los proveedores. No obstante, pese a este inconveniente, pudimos llevar a cabo la introducción de nuevas metodologías.

Adicionalmente, nos encontramos con una dificultad al intentar poner en marcha el flamante procedimiento de monitorización continua y pasiva mediante la herramienta Securi-

tyScoreCard (explicada más adelante), debido a un problema relacionado con las licencias. Esta circunstancia ha resultado en un retraso en su resolución, programada ahora para finales de septiembre.

2 Descripción del proyecto

2.1 Metodología de trabajo

La metodología empleada en este proyecto fue fundamental para lograr resultados precisos en la gestión de riesgos de proveedores. Inicialmente, se consideró esencial sentar bases sólidas antes de emprender cualquier acción. Esto implicaba comprender las inquietudes principales del cliente, ya que sus perspectivas resultaban cruciales para guiar nuestros esfuerzos.

Particularmente, el cliente demostró un marcado interés en abordar la taxonomía de las principales amenazas presentes en la cadena de suministro, tal como lo establece el marco de referencia del NIST. Estas amenazas se centran en la seguridad física, la presencia de malware, la ingeniería social y las vulnerabilidades de software. Nuestra estrategia se enfocó en mitigar riesgos al alinear cuidadosamente nuestras acciones con estas áreas críticas.

Además, se reconoció la importancia de respaldar nuestro trabajo con sólidos estándares en seguridad de la información y continuidad del negocio. En este sentido, utilizamos múltiples marcos reconocidos, tales como ISO 27001, ISO 22301 y DORA. ISO 27001 provee directrices completas para la gestión de la seguridad de la información, mientras que ISO 22301 se enfoca en garantizar la continuidad del negocio en situaciones adversas. Por su parte, DORA se centra en la resiliencia operativa digital en el sector financiero. En un primer momento se consideró también tener en cuenta COBIT 19, pero finalmente se acordó con el cliente en que para abarcar la seguridad de la información nos apoyaríamos únicamente en ISO 27001.

Al construir los cuestionarios de seguridad, que los proveedores completarían durante la revisión de nuevos servicios, nos basamos en estos estándares. Esto nos permitió diseñar cuestionarios exhaustivos y relevantes que evaularían riesgos en línea con los criterios de seguridad y continuidad del negocio.

A lo largo del proyecto, evaluamos cuidadosamente diferentes herramientas para la monitorización continua de proveedores críticos. Específicamente, analizamos las capacidades de Bitsight y SecurityScoreCard. Bitsight ofrece una visión holística de la ciberseguridad de los proveedores, mientras que SecurityScoreCard se enfoca en supervisar la postura de seguridad. Tras colaborar con el cliente, tomamos la decisión de cambiar a SecurityScoreCard como la herramienta preferida para esta tarea.

Para llevar a cabo este ambicioso proyecto, nos embarcaríamos en una colaboración estrecha y coordinada. Esta sinergia implicaría una estrecha cooperación con una consultora externa especializada en ciberseguridad y riesgos de proveedores. Además, contaríamos con la participación activa y comprometida de los empleados clave de la sede central del

cliente, quienes se encuentran ubicados en un país distinto al nuestro.

La consultora externa se integraría como un componente esencial en el equipo de trabajo, brindando experiencia específica en ciberseguridad y proveedores. Su conocimiento profundo y experiencia en estrategias de gestión de riesgos sería fundamental para orientar el proceso de implementación, asegurando que las acciones y decisiones adoptadas estén en línea con las mejores prácticas y estándares de la industria.

Por otro lado, la colaboración con los empleados de la sede central del cliente, situada en un país extranjero, sería una parte vital del proyecto. Trabajaríamos en conjunto con estos profesionales, aprovechando su conocimiento interno de la empresa y su visión contextual para garantizar la efectividad y la alineación de nuestras estrategias, además de así poder adaptar los consejos dados por la consultora externa al cliente.

2.2 Fases y desarrollo del proyecto

En el anterior punto, hemos establecido los cimientos de nuestro proyecto. Nuestra prioridad sigue siendo abordar las inquietudes del cliente relacionadas con las amenazas en la cadena de suministro, y aprovechar los estándares y herramientas acordados previamente con el cliente.

En esta sección, presentaremos de manera detallada el desarrollo del proyecto. Dividiremos esta sección en dos enfoques principales: la revisión de nuevos proveedores y la monitorización continua de los proveedores críticos. Para ambas áreas, detallaremos exhaustivamente cada fase, desde el inicio del proceso de revisión de los servicios hasta su conclusión y aprobación definitiva.

2.2.1 Revisión de nuevos proveedores

Antes de explicar cómo desarrollamos la implementación de la nueva metodología hay que recordar cuáles son los dos objetivos fundamentales de esta sección:

- **Detección de riesgos.** Si bien es innegable que esta sección contempla dos objetivos de vital importancia, el propósito distintivo radica en este objetivo. La finalidad de esta nueva implementación es lograr la identificación exhaustiva de una plétora de riesgos potenciales. La capacidad de descubrir eventuales riesgos antes de que el servicio entre en producción permite anticiparnos a posibles incidentes tales como fuga de datos, intrusiones, menoscabo de la reputación, entre otros.

- **Reducción del tiempo de revisión.** ¿Cuál es la connotación implícita en la disminución del tiempo de revisión? Tal y como ha sido expuesto con anterioridad,

nuestra intervención en el proceso de compras, orientada a la evaluación de la seguridad del servicio, conlleva la posibilidad de extender el intervalo requerido para formalizar la contratación y establecer la ejecución plena del servicio. Esta eventualidad podría incidir en la rentabilidad empresarial en función del tipo de servicio considerado.

Al iniciar la implementación de la nueva metodología para la revisión de proveedores, no partíamos desde una posición nula. En ese contexto, ¿desde qué punto exactamente comenzábamos?

Previo al inicio de la revisión del servicio desde la perspectiva de los sistemas del proveedor, resultaba imperativo contar con una comprensión cabal del flujo de información de los datos entre el proveedor y el cliente. ¿Qué implica tener una comprensión clara de este flujo de datos? Básicamente, significa estar en capacidad de responder las siguientes preguntas:

- ¿El proveedor actúa como encargado o responsable de los datos?
- ¿Qué categorías de datos (personales y/o empresariales) tiene previsto manipular el proveedor?
- ¿Se contemplan datos sensibles, como información médica, en el tratamiento?
- ¿El proveedor dispondrá de acceso físico a las instalaciones del cliente?
- ¿El proveedor tendrá acceso lógico a los sistemas del cliente?
- ¿Se procederá al envío de datos hacia los sistemas del proveedor? En caso afirmativo, ¿a través de qué vías (correo electrónico, servicio web, sFTP)?
- ¿El proveedor almacenará los datos en un centro de datos privado o en una infraestructura de nube pública?
- ¿Se hace uso de alguna herramienta alojada en la nube pública para el procesamiento de los datos?
- ¿Es factible acceder a los datos de responsabilidad del cliente a través de Internet, como por ejemplo, mediante un sitio web de dominio público?

Antes de derivar estas preguntas a la persona apropiada, ¿podemos, en principio, obtener respuestas a algunas de estas preguntas con el respaldo de documentación adicional? Para iniciar la evaluación del nuevo servicio entrante, se nos proporcionan dos documentos adicionales por parte del equipo de compras: el *Service Risk Assessment* y la oferta del servicio presentada por el propio proveedor. El *Service Risk Assessment* es un informe elaborado en colaboración entre el equipo interno de ciberseguridad del cliente y el equipo de consultores, y se completa bajo la supervisión del responsable del área de negocios pertinente. Estos documentos proporcionan una perspectiva integral y desde una posición jerárquica superior del servicio, abordando cuestiones como su contenido, el área de ne-

gocio responsable, el flujo de datos y la tipología de datos involucrados.

Sin embargo, el aspecto más crucial del *Service Risk Assessment* radica en su función como herramienta de cálculo, dado que, según los parámetros proporcionados por el responsable del área de negocio, nos brinda un nivel de riesgo inherente específico (Muy bajo, Bajo, Medio, Alto y Muy Alto). Este elemento se convierte en un punto de referencia esencial para nuestra revisión, especialmente en lo que respecta a la implementación del nuevo modelo.

En caso de que no podemos proporcionar respuestas a todas estas preguntas por nuestra cuenta, las remitimos al responsable del área de negocio correspondiente o a la persona de contacto del proveedor.

Una vez tenemos un control completo del flujo de datos, evaluamos el nivel de seguridad de los sistemas del proveedor. ¿Cómo lo llevamos a cabo? Realizamos un cuestionario que contiene una serie de preguntas alineadas con los requisitos de seguridad extraídos de la norma ISO 27001. El proveedor completa este cuestionario y lo adjuntamos al contrato marco como evidencia, junto con las cláusulas de seguridad y los anexos de seguridad pertinentes. Además, es importante destacar que la complejidad del cuestionario de seguridad depende del nivel de riesgo inherente determinado en el *Service Risk Assessment*.

Una vez que recibimos el cuestionario de seguridad debidamente cumplimentado por parte del proveedor, lo revisamos minuciosamente y tomamos las medidas necesarias en relación a aquellos puntos que consideramos críticos y cuyo incumplimiento podría representar un riesgo para el cliente, debiendo abordarlos de inmediato o acordando una fecha con el de resolución con el proveedor.

Hasta este punto, concluimos el proceso actual de revisión de nuevos servicios. Con el nuevo modelo, nuestra meta es mejorar este proceso al centrarnos en los dos objetivos principales: la detección de riesgos y la reducción del tiempo de revisión.

- **Detección de riesgos**
  Cuando concebimos este nuevo modelo, identificamos la oportunidad de abarcar áreas adicionales para una detección más exhaustiva de riesgos. ¿Dónde se centra esta ampliación? Se focaliza en el intercambio de datos entre todas las partes involucradas y en los sistemas del proveedor.

  En relación al flujo de datos entre el proveedor y el cliente, notamos que ya teníamos una cobertura significativa. No obstante, decidimos dar un paso más allá al comenzar a investigar las subcontrataciones realizadas por el proveedor para la prestación de servicios al cliente. Esta iniciativa nos permite obtener una visión integral y crear una base de datos interna que documenta las subcontrataciones de todos los provee-

dores para cada uno de los servicios. Además, agregamos el valor de comprender qué funciones desempeñan y qué partes del servicio ofrecen al cliente. Con esta base de datos, estamos en posición de tomar medidas como la suspensión de comunicaciones con el proveedor en caso de que uno de sus proveedores subcontratados experimente algún incidente de ciberseguridad.

Dentro del objetivo de la detección de riesgos, se incluye la revisión y mejora del cuestionario "Service Risk Assessment" (SRA) y del cuestionario de seguridad que el proveedor debe completar. El desarrollo de estos cuestionarios estaban en manos de una consultora contratada por el cliente. Realizamos una serie de reuniones con esta consultora para expresar nuestras preocupaciones, y así mirar de diseñar los documentos conjuntamente, que se resumen en:
- El nuevo documento debe incorporar todas las preguntas necesarias para comprender el flujo de los datos y el estado de los sistemas del proveedor.
- Mejorar el cálculo del riesgo inherente.
- Mapear el cuestionario con los requisitos de la ISO 27001 y DORA.
- Unificar el cuestionario de seguridad en uno solo, con su complejidad variando según el nivel de riesgo inherente determinado en el SRA.
- Adaptar la complejidad del nuevo cuestionario de seguridad en función de si el servicio es en la nube o no, y de su modelo de servicio (SaaS, PaaS y IaaS).

La consultora contratada por el cliente abordó la idea de unificar el SRA y el cuestionario de seguridad para el proveedor en uno solo, para facilitar su desarrollo y comprensión.

Una mejora muy significativa, aplicada por nosotros en el nuevo SRA es que nos permite de una manera clara la activación del equipo de continuidad de negocio para darnos soporte en casos críticos. En cliente están todos los procesos de negocio de cada área de negocio registrados y almacenados por el equipo de continuidad de negocio. Entonces, vimos que era una buena idea hacer que el responsable del área de negocio indicara con qué proceso de negocio estaría vinculado el nuevo servicio que se quiere contratar, entonces si vemos que es un proceso crítico para continuidad de negocio y el proveedor es indispensable para este proceso, activamos al equipo de continuidad de negocio para que realice la revisión junto a nosotros.

Además, para ayudarnos a la detección de posibles riesgos en los nuevos servicios entrantes nos apoyamos en nuevas herramientas, sobretodo para hacer una revisión más exhaustiva a aquellos servicios con un riesgo inherente más elevado. Estas herramientas son:
- **Wappalyzer:** Es una herramienta de análisis de tecnología web que te permite descubrir las tecnologías utilizadas en un sitio web en particular. Esto incluye lenguajes de programación, sistemas de gestión de contenido (CMS), frameworks, bibliotecas JavaScript, herramientas de análisis, y más. Nos permite identificar si el proveedor está usando tecnología obsoleta o desactualizada que pueda ser vulnerable.

- **Qualys SSL Labs:** Es una herramienta de análisis que evalúa la seguridad de un sitio web en relación con su implementación de protocolos SSL/TLS. SSL/TLS son protocolos de seguridad que garantizan la comunicación segura entre un navegador y un servidor web. Esto, sobretodo nos permite saber si el proveedor en su página web permite el uso de los protocolos TLS 1.0 y 1.1, así les podemos pedir que lo actualicen.
- **GDPR Enforcement Tracker:** Es una herramienta en línea que rastrea y proporciona información sobre las multas y sanciones impuestas a empresas y organizaciones por incumplimiento del Reglamento General de Protección de Datos (GDPR) de la Unión Europea. Con esta herramienta podemos avisar al responsable del área de negocio que quiere contratar el servicio que el proveedor incumple reiteradamente GDPR.

Finalmente, una de las mejoras que planeamos implementar con este nuevo modelo es la incorporación de la herramienta "SecurityScoreCard". Esta herramienta nos permite obtener una puntuación de seguridad del proveedor de manera instantánea. Planeamos utilizar esta herramienta como soporte para aquellos servicios con un nivel de riesgo inherente alto o muy alto.

- **Reducción del tiempo de revisión**
  Como mencionamos previamente, nuestra intervención en la revisión de los nuevos servicios puede retrasar su contratación. Por lo tanto, dentro del proceso de compras, se estableció un marco temporal de un mes para otorgar nuestra aprobación al servicio.

  Cuando comenzamos este proyecto, nuestro enfoque fue el de ser capaces de detecar más riesgos sí, pero también reducir el tiempo necesario para emitir nuestra aprobación ya que vimos que para algunos proveedores sobrepasábamos el marco temporal acordado. Llevamos a cabo un análisis exhaustivo para identificar dónde se concentraba la mayor parte del tiempo de revisión en la mayoría de los servicios. Constatamos que la mayor demora se debía a la cumplimentación del cuestionario por parte del proveedor. ¿Qué causaba este retraso? Llegamos a la conclusión de que, a pesar de que anteriormente disponíamos de diferentes cuestionarios de seguridad que variaban en complejidad según el nivel de riesgo inherente, todos eran bastante complejos. Algunas compañías encontraban dificultades para completarlos, sobretodo PYMEs, y en ocasiones, debíamos reducir el número de preguntas para acomodar a ciertos proveedores. Por esta razón, uno de los objetivos que planteamos a la consultora contratada por el cliente fue el abordar este desafío.

  A pesar de que el nuevo cuestionario de seguridad puede simplificar el proceso de cumplimentación para los proveedores, buscábamos soluciones complementarias. Luego de una reunión con la nueva consultora, decidimos adoptar un enfoque diferente para los proveedores que ofrecieran servicios con un nivel de riesgo inherente

bajo y muy bajo. En estos casos, nuestra revisión se centraría en el flujo de los datos, asegurando el uso de canales de comunicación adecuados, evitando así la necesidad de enviar cuestionarios de seguridad al proveedor y reduciendo los tiempos de espera.

Además, tras una reunión adicional con la consultora, llegamos a la conclusión de que no era necesario enviar el cuestionario de seguridad a los proveedores que contaran con certificaciones como la ISO 27001 u otras similares. Sin embargo, para aceptar una certificación otorgada por el proveedor, debíamos de verificar los siguientes aspectos:

- Que el alcance de la certificación cubra el servicio proporcionado por el proveedor.
- La vigencia de la certificación.
- La certificación de la entidad evaluadora por parte de ENAC (Entidad Nacional de Acreditación).

Con estos tres puntos considerados, podemos validar la certificación y proceder a otorgar nuestra aprobación sin requerir que el proveedor complete el cuestionario de seguridad.

Flujo nuevo del proceso de revisión de servicios entrantes

Una vez que hemos planteado estas nuevas mejoras dentro del modelo de revisión de los nuevos servicios, el flujo a seguir durante la revisión de un servicio entrante es el siguiente:

1. Desde el equipo de compras, se nos notifica que una área de negocio del cliente desea contratar un proveedor para ofrecer un nuevo servicio para la compañía. El equipo de compras nos comunica el documento SRA y la oferta del servicio proporcionada por el proveedor.
2. El equipo de seguridad de la información dedicado a la gestión de riesgos en terceros (nosotros) procede a revisar la documentación facilitada. Recordemos que debemos ser capaces de responder a todas las preguntas detalladas anteriormente.
3. Si determinamos que el proveedor es esencial y está relacionado con un proceso crítico, activamos al equipo de continuidad de negocio para que realice su revisión pertinente.
4. Si no podemos responder a todas las preguntas mencionadas anteriormente o surgen dudas, contrastamos con el responsable del área de negocio y/o el contacto que tenemos del proveedor para comprender completamente el flujo de los datos. Si es necesario, programamos reuniones.
5. Solicitamos al proveedor información sobre las subcontrataciones. En el caso de que subcontrate a otras compañías para brindar el servicio, recopilamos la información necesaria y la registramos.
6. Una vez que comprendemos el flujo de los datos del servicio y sabemos dónde residen

los datos (ya sea en los sistemas del cliente o del proveedor), podemos aprobar aquellos servicios donde la información no sale de los sistemas del cliente.

7. En el caso de que los datos del cliente salgan de sus sistemas y se almacenen en los sistemas del proveedor, evaluamos el riesgo inherente resultante del documento SRA. Para los casos en los que el riesgo inherente sea bajo o muy bajo, podemos aprobar el servicio si hemos verificado que las comunicaciones entre el cliente y el proveedor son adecuadas.
8. Luego, nos centramos en otro tipo de servicios, aquellos que quizás tengan un riesgo más alto inicialmente. Solicitamos al proveedor certificaciones como la ISO 27001 u otras similares. En el caso de que las tengan, verificamos los tres puntos mencionados anteriormente y aprobamos el servicio.
9. Paralelamente al punto 8, revisamos si el proveedor ha sido penalizado por incumplimiento del GDPR utilizando la herramienta GDPR Enforcement Tracker. Además, si el proveedor cuenta con un sitio web para proporcionar el servicio, utilizamos las herramientas Wappalyzer, Qualys SSL Labs y SecurityScoreCard para realizar las revisiones correspondientes.
10. Si el proveedor no dispone de certificaciones como la ISO 27001, le proporcionamos el cuestionario de seguridad. El cuestionario de seguridad debe completarse de acuerdo con la tipología del servicio, si el proveedor utiliza servicios en la nube para ofrecer el servicio o no, y el riesgo inherente determinado por el SRA. Una vez que recibimos el cuestionario cumplimentado, lo revisamos y procedemos a aprobar el servicio.
11. Durante todo este proceso, es posible que identifiquemos riesgos que deben ser discutidos, registrados, seguidos y acordados con el proveedor o el cliente, según corresponda, una fecha de resolución para aprobar el servicio.

2.2.2 Monitorización continua de proveedores críticos

En esta sección, abordaremos la implementación de un nuevo modelo de monitorización continua de proveedores críticos. A diferencia del enfoque previo, en el que partíamos de una base sólida, en este caso, comenzamos prácticamente desde cero.

Antes de la ejecución de este proyecto, nuestra única herramienta de gestión, para la monitorización activa, consistía en un calendario anual en el que se registraban los proveedores. Cada trimestre, llevábamos a cabo una revisión de seguridad para un grupo seleccionado de proveedores. Los criterios de inclusión en este calendario se limitaban exclusivamente a aquellos proveedores considerados críticos desde la perspectiva de la continuidad del negocio, y las externalizaciones.

Anualmente, el equipo de continuidad de negocio realiza análisis de impacto en el negocio en colaboración con las distintas áreas del cliente. A partir de estos análisis, conocidos como Evaluaciones de Impacto en el Negocio (BIA por sus siglas en inglés), se extraen conclusiones para la construcción o, más precisamente, la renovación del plan de continuidad

de negocio del cliente. Nuestro interés radicaba en identificar a aquellos proveedores cruciales para la continuidad de negocio. Posteriormente, el equipo de compras del cliente nos proporcionaba información sobre los proveedores que desempeñaban un papel de externalización.

Para realizar la revisión de estos servicios únicamente enviábamos al proveedor un cuestionario de seguridad de la información, con requerimientos sacados de la ISO 27001. El cuestionario debía de ser cumplimentado y devuelto a nosotros por el proveedor.

Es relevante mencionar que ya se empleaba la herramienta Bitsight para la monitorización pasiva de proveedores. A través de esta herramienta, supervisamos a los proveedores que consideramos críticos desde el equipo de seguridad de la información encargado de evaluar nuevos proveedores. ¿Qué proveedores consideramos críticos para supervisar en Bitsight? Aquellos que gestionan grandes volúmenes de datos personales de diversos usuarios y, sobre todo, que tienen una exposición directa a Internet para brindar servicios al cliente. Por ejemplo, un proveedor que almacena datos del cliente y ofrece un sitio web accesible desde Internet para consultas realizadas por los empleados del cliente. Es importante destacar que la selección de proveedores es un proceso delicado debido a las limitaciones impuestas por el número de licencias permitidas.

¿Cuál es el procedimiento para utilizar Bitsight? Trimestralmente, nos comunicamos con los proveedores, les proporcionamos un informe con todos los hallazgos identificados por la herramienta y solicitamos a los proveedores que nos faciliten planes de acción para mitigarlos. Para ello, ofrecemos acceso gratuito a los proveedores, dentro de la herramienta, para que puedan visualizar los dominios o direcciones IP públicas afectadas y, de esta manera, corregir los hallazgos. Además, gracias al sistema de alertas de la herramienta, nos ponemos en contacto con el proveedor si vemos que la puntuación dada por la herramienta ha tenido una bajada importante repentina. El objetivo principal es fortalecer la postura de ciberseguridad de los proveedores y, en consecuencia, aumentar su madurez y seguridad en sus sistemas. Esto beneficia tanto a los proveedores como al cliente, al reforzar la ciberresiliencia de ambas partes.

A continuación, nos centraremos en las mejoras logradas con la implementación de este nuevo modelo de monitorización continua de proveedores, tanto en la monitorización activa como en la pasiva.

- **Monitorización activa de proveedores críticos**
  Como se ha indicado previamente, en el pasado, nuestra única herramienta de gestión consistía en un calendario en el que se registraban proveedores críticos para la continuidad del negocio y externalizaciones. Cuando decidimos implementar este nuevo modelo, realizamos una revisión exhaustiva de los tipos de proveedores incluidos en el calendario existente. Esta evaluación nos llevó a ampliar la lista de proveedores que requerían una revisión de seguridad más completa. Finalmente,

decidimos incorporar al calendario los siguientes tipos de proveedores:

- Proveedores críticos para la continuidad del negocio.
- Proveedores de externalizaciones.
- Proveedores que gestionan datos médicos de responsabilidad del cliente.
- Proveedores que facturan al cliente más de 300 mil euros anuales.
- Proveedores que están siendo supervisados en Bitsight.
- Proveedores responsables de aplicaciones de negocio esenciales para el cliente.

Este nuevo modelo resultó en la inclusión de cuatro categorías adicionales de proveedores, lo que nos llevó a modificar la planificación del calendario de anual a trianual. En este nuevo enfoque, se revisan cinco proveedores diferentes cada trimestre.

¿Cuál es el procedimiento para llevar a cabo esta revisión exhaustiva bajo el nuevo modelo? Para evaluar los sistemas de los proveedores, solicitamos que completen un cuestionario de seguridad de la información que ya utilizábamos, y además, hemos introducido un nuevo cuestionario específico sobre continuidad del negocio. Este último cuestionario fue elaborado por el experto en continuidad de negocio del cliente.

Además, dado que nos preocupa especialmente el flujo de datos entre el proveedor y el cliente, indagamos sobre este aspecto para garantizar que no haya habido cambios significativos desde la última revisión del servicio.

También planteamos una serie de preguntas que no están contempladas en los cuestionarios de seguridad de la información y continuidad del negocio. Estas preguntas incluyen:

- ¿El proveedor posee certificaciones ISO u otras certificaciones de seguridad o continuidad del negocio? En caso afirmativo, ¿podría proporcionarlas?

- ¿Dispone de un Plan de Continuidad del Negocio y un Plan de Recuperación ante Desastres? ¿Podría compartirlos?

- ¿Se han realizado recientemente pruebas de recuperación ante desastres? ¿El tiempo de recuperación coincidió o fue menor que el Objetivo de Tiempo de Recuperación (RTO)? ¿Los resultados de las pruebas fueron satisfactorios?

- ¿Se han llevado a cabo recientemente pruebas de penetración o auditorías (internas o externas) en los sistemas o áreas necesarios para brindar el servicio a

la entidad? ¿Se tienen previstas tales pruebas en el futuro?

– ¿Se realizan ejercicios de concienciación en materia de seguridad en la empresa? ¿Se realizan ejercicios de phishing? ¿Podría proporcionar los resultados?

Cabe destacar la importancia de la pregunta sobre el RTO, ya que cada servicio proporcionado por un proveedor está vinculado a un proceso interno de la compañía que tiene un RTO específico. Por lo tanto, preguntamos sobre las pruebas de recuperación ante desastres para verificar si el tiempo de recuperación coincide con el RTO, o mejor aún, es menor.

Además, las preguntas relacionadas con las pruebas de penetración y las auditorías se centran en determinar el nivel de madurez de los sistemas y si los hallazgos identificados se han abordado de manera oportuna.

Toda la información recopilada y las preguntas planteadas nos permiten obtener una visión más detallada del servicio. Entendemos que este enfoque exhaustivo nos permite identificar más riesgos y abordarlos de manera eficiente.

- **Monitorización pasiva de proveedores críticos**
  Al comienzo de esta sección, he presentado el funcionamiento de la supervisión pasiva de proveedores críticos. En este punto, desde la sede central del cliente, se tomó la decisión de aprovechar la reestructuración de la revisión de proveedores para migrar de la herramienta existente, es decir, dejar de utilizar Bitsight y adoptar SecurityScoreCard.

  ¿Por qué se optó por este cambio? Se fundamentó en la rapidez con la que SecurityScoreCard detecta hallazgos, su capacidad de adaptación ágil a diferentes proveedores, la eficiencia en la generación de calificaciones y, además, en su amplia cartera de proveedores en comparación con Bitsight.

  Es importante destacar que la metodología de uso de esta nueva herramienta es idéntica a la de Bitsight. La diferencia principal radica en la capacidad de añadir y eliminar proveedores para su supervisión de manera más ágil y eficiente.

2.2.3 Detección y gestión de los riesgos hallados

A pesar de que la implementación del nuevo modelo transversal para la revisión de proveedores desde una perspectiva de seguridad de la información no contemplaba originalmente un cambio en la gestión de riesgos, me gustaría brindar una breve descripción de cómo se lleva a cabo esta gestión, así como mencionar una pequeña mejora que hemos implementado.

En cualquiera de las dos secciones, ya sea en la revisión de nuevos servicios entrantes o en la monitorización continua de proveedores críticos, es posible identificar riesgos que requieren una gestión adecuada. Cuando se identifica un riesgo, se inicia una comunicación con el proveedor para determinar si disponen de un plan de acción para abordarlo. A continuación, nos ponemos en contacto con el responsable del área de negocio, quien a su vez es el encargado de la monitorización del riesgo en cuestión. Notificamos al responsable sobre el hallazgo del riesgo y, a partir de ese punto, se plantean tres posibilidades: en primer lugar, el responsable podría decidir no contratar al proveedor si considera que el riesgo es inaceptable. En segundo lugar, si el proveedor presenta un plan de acción para mitigar el riesgo, se acuerda una fecha para la implementación de las medidas con la participación del proveedor y el responsable del área de negocio. Finalmente, existe la posibilidad de que el proveedor no tenga la intención de abordar el riesgo, en cuyo caso el responsable del área de negocio debe tomar la decisión de aceptar el riesgo. Todo este proceso se gestiona mediante una herramienta competitiva del mercado conocida como Archer.

La mejora fue que decidimos incluir la fecha de mitigación acordada en el contrato en los casos en los que tanto el proveedor como nosotros, junto con el responsable del área de negocio, determinamos una fecha de mitigación. Esta inclusión en el contrato se refleja en la siguiente cláusula:

El PROVEEDOR manifiesta que no cumple actualmente con los requisitos establecidos en la sección 'X' del ANEXO 'Y', adjunto al Contrato Marco y que forma parte íntegra e inseparable del mismo. Sin perjuicio de ello, se compromete a adoptar todas las medidas que resulten necesarias. Por consiguiente, EL PROVEEDOR se obliga frente a EL CLIENTE a:

- *Cumplir con los requisitos del Anexo, en el plazo máximo de 'Z' mese a partir de la fecha de incio de la presente Adenda.*
- *Proporcionar evidencias que demuestren el cumplimiento de los requisitos exigidos para su validación por parte del CLIENTE.*

3 Resultados

En esta sección, se presentarán los resultados obtenidos a través de cada una de nuestras mejoras. Cabe destacar que no todos los objetivos son medibles de manera cuantitativa.

3.1 Revisión de nuevos proveedores

Los objetivos para esta sección eran los siguientes; detectar más posibles riesgos y el de reducir el tiempo de revisión del servicio. Entonces, nos centraremos en cómo hemos mejorado, qué ejercicios se han realizado y que resultados cuantificables hemos podido obtener.

Resultados - Detección de posibles riesgos

Para detectar un mayor número de riesgos hemos implementado todos siguientes ejercicios, explicados detalladamente arriba.

1. Pedir las subcontrataciones al proveedor
2. Mejora del cuestionario SRA.
3. Mejora del cuestionario que debe de ser cumplimentado por el proveedor.
4. Involucración inmediata del equipo de continuidad de negocio cuando se requiere.
5. Uso de herramientas como; Wappalyzer, Qualys SSL Labs y GDPR Enforcement Tracker.
6. Uso puntual de la herramienta SecurityScoreCard.

Si abordamos esta cuestión desde un enfoque lógico, consideramos cómo podríamos cuantificar estos ejercicios y evaluar si el nuevo modelo ha mejorado en la identificación de riesgos, entonces la métrica que podríamos reportar es la siguiente: el número de riesgos identificados en un período de tiempo bajo el modelo anterior y el mismo período de tiempo bajo el nuevo modelo.

Sin embargo, el desafío radica en que, en general, no es común encontrar riesgos durante las revisiones de seguridad. Por lo tanto, no disponemos de una muestra lo suficientemente grande como para generar un Indicador Clave de Desempeño (KPI) en este sentido.

Resultados - Reducción del tiempo de revisión del servicio

A diferencia de la sección anterior, en este caso, podemos identificar varios resultados que nos permiten evaluar si hemos logrado reducir el tiempo necesario para revisar los servicios. Sin embargo, es importante recordar las dos mejoras que implementamos con el objetivo de reducir dicho tiempo: primero, la exclusión de envío del cuestionario de seguridad a proveedores con un nivel de riesgo inherente bajo o muy bajo; segundo, la

omisión del envío del cuestionario de seguridad a proveedores que cuentan con certificaciones como ISO 27001 u otras similares.

Para poder demostrar que estos cambios han provocado un cambio sustancial tenemos dos resultados:

1. En el primer ejercicio, nuestro objetivo es demostrar cómo la exclusión del envío del cuestionario de seguridad a servicios con un riesgo inherente muy bajo o bajo conlleva una reducción sustancial en el tiempo necesario para validar el servicio por parte de nuestro equipo de seguridad de la información enfocado en riesgos de proveedores. Para ilustrar este punto, hemos reunido una muestra de 40 servicios, compuesta por 20 casos en los que se envió el cuestionario de seguridad al proveedor a pesar de tener un riesgo inherente bajo o muy bajo, y 20 casos en los que no se envió el cuestionario. A continuación, se presentan los resultados en la tabla siguiente en la que se muestra la fecha de inicio de revisión del servicio, la fecha de validación del servicio y la media de días laborables en los que se ha tardado en revisar el servicio *end-to-end*. Es importante destacar que estos resultados tienen una fecha "barrera", principios de mayo, momento en el que se comenzó a implementar esta iniciativa de no enviar el cuestionario a servicios con un riesgo inherente bajo o muy bajo.

Fecha inicio	Fecha validación	Media de días laborables de revisión
02/01/2023	08/02/2023	28
04/01/2023	10/02/2023	28
12/01/2023	20/02/2023	28
16/01/2023	24/03/2023	50
20/01/2023	21/03/2023	43
15/02/2023	15/03/2023	21
21/02/2023	12/04/2023	37
09/03/2023	17/04/2023	28
09/03/2023	17/04/2023	28
09/03/2023	17/04/2023	28
09/03/2023	17/04/2023	28
09/03/2023	17/04/2023	28
09/03/2023	17/04/2023	28
13/03/2023	15/05/2023	46
20/03/2023	14/04/2023	20
31/03/2023	11/04/2023	8
03/04/2023	17/04/2023	11
05/04/2023	23/05/2023	35
28/04/2023	30/05/2023	23
05/05/2023	08/05/2023	2
	Media Total	27,4

Table 1: Servicios a los cuales se le envió el cuestionario al proveedor

Fecha inicio	Fecha validación	Media de días laborables de revisión
11/05/2023	12/05/2023	2
11/05/2023	12/05/2023	2
11/05/2023	12/05/2023	2
12/05/2023	15/05/2023	2
15/05/2023	16/05/2023	2
16/05/2023	16/05/2023	1
18/05/2023	18/05/2023	1
23/05/2023	24/05/2023	2
24/05/2023	25/05/2023	2
26/05/2023	29/05/2023	2
26/05/2023	02/06/2023	6
30/05/2023	31/05/2023	2
31/05/2023	31/05/2023	1
31/05/2023	01/06/2023	2
01/06/2023	02/06/2023	2
01/06/2023	02/06/2023	2
01/06/2023	06/06/2023	4
01/06/2023	06/06/2023	4
07/06/2023	08/06/2023	2
30/05/2023	08/06/2023	8
	Media Total	2,55

Table 2: Servicios a los cuales NO se le envió el cuestionario al proveedor

Los datos indican que, cuando se enviaba el cuestionario de seguridad al proveedor, requeríamos en promedio 27,4 días laborables para proporcionar nuestra validación al servicio. Sin embargo, al optar por no enviarlo, hemos logrado reducir significativamente este período a 2,55 días laborables, lo que representa una **disminución de 24,85 días** en el tiempo de validación.

2. En el segundo ejercicio, buscamos verificar de manera similar al primer ejercicio si, efectivamente, logramos reducir el tiempo de validación del servicio al no enviar el cuestionario de seguridad a proveedores con un riesgo inherente medio, alto o muy alto que están certificados con ISO 27001 u otras certificaciones similares. Los resultados se presentan en la siguiente tabla, en este caso, hemos recopilado un total de 14 muestras, de las cuales 7 corresponden a servicios que no cuentan con ISO 27001 y las otras 7 sí la tienen.

Fecha inicio	Fecha validación	Media de días laborables de revisión
24/04/2023	19/05/2023	20
24/04/2023	19/05/2023	20
28/04/2023	08/05/2023	7
04/05/2023	16/06/2023	32
11/05/2023	16/06/2023	27
26/05/2023	04/08/2023	51
08/06/2023	26/06/2023	13
18/07/2023	28/07/2023	9
	Media Total	22,7

Table 3: Servicios a los cuales se le envió el cuestionario al proveedor

Fecha inicio	Fecha validación	Media de días laborables de revisión
05/05/2023	10/05/2023	4
26/05/2023	06/06/2023	8
07/06/2023	27/07/2023	37
19/06/2023	18/07/2023	22
19/06/2023	29/06/2023	9
02/08/2023	04/09/2023	24
02/08/2023	04/09/2023	24
	Media Total	18,8

Table 4: Servicios a los cuales NO se le envió el cuestionario al proveedor

Los datos indican que, cuando se enviaba el cuestionario de seguridad al proveedor, requeríamos en promedio 22,7 días laborables para proporcionar nuestra validación al servicio. Sin embargo, al optar por no enviarlo, hemos logrado reducir significativamente este período a 18,8 días laborables, lo que representa una **disminución de 3,9 días** en el tiempo de validación.

3.2 Monitorización continua de proveedores críticos

Al igual que sucede en nuestras revisiones de servicios recién incorporados, generalmente no identificamos riesgos durante las revisiones de proveedores críticos que están siendo monitoreados de manera pasiva mediante la herramienta SecurityScoreCard o de manera activa cuando se requiere una revisión exhaustiva de un proveedor crítico que está incluido en nuestro calendario. Esta circunstancia limita nuestra capacidad para obtener una muestra significativa que nos permita recopilar datos objetivos con el propósito de evaluar si este nuevo modelo nos permite detectar más posibles riesgos.

4 Conclusiones

En conclusión, la implementación del nuevo modelo de gestión de riesgos en proveedores desde el punto de vista de seguridad de la información y continuidad de negocio representa un avance significativo en la manera en que abordamos la evaluación y supervisión de nuestros proveedores.

En lo que respecta a los nuevos servicios entrantes, consideramos que hemos alcanzado exitosamente los dos objetivos establecidos al comienzo del proyecto. En primer lugar, hemos logrado establecer un nuevo modelo más completo para la revisión de los nuevos proveedores. Además, hemos conseguido reducir el tiempo necesario para revisar los nuevos servicios, acelerando así el proceso de adquisición.

Como hemos observado en los resultados anteriores, la decisión de no enviar el cuestionario de seguridad a proveedores que ofrecen servicios con un riesgo inherente bajo o muy bajo ha resultado en una reducción significativa en el tiempo de revisión. Por otro lado, si bien también hemos reducido el tiempo al omitir el envío del cuestionario para aquellos servicios con un riesgo inherente medio, alto o muy alto y que cuentan con certificaciones como ISO 27001 u otras similares, la diferencia no ha sido tan marcada. Esto se debe a que, para este tipo de servicios, dedicamos un tiempo considerable a comprender en profundidad el servicio y el flujo de datos, lo que implica la organización de reuniones con los responsables del área interesados en adquirir el servicio, así como con representantes del proveedor.

Es interesante notar que el tiempo requerido para proporcionar nuestra validación antes de la implementación del nuevo modelo no presentaba variaciones significativas independientemente del riesgo inherente del servicio. Esta consistencia se debe a que los proveedores con riesgo inherente bajo o muy bajo suelen ser pequeñas y medianas empresas (PYMEs) que tienen limitaciones en cuanto a personal especializado en seguridad y que a menudo enfrentaban dificultades para completar el cuestionario de seguridad de manera adecuada.

Es importante destacar que se ha dado un avance significativo en el proceso de revisión de proveedores críticos durante la fase de monitorización continua. Hemos ampliado nuestra cobertura al incluir hasta cinco categorías adicionales de proveedores a los que deseamos someter a una revisión exhaustiva. Además, hemos incorporado una cantidad sustancial de documentación relevante, datos objetivos y aplicado nuevas técnicas que nos permiten obtener una visión más detallada de la seguridad y la continuidad del negocio del proveedor. Esto nos capacita para identificar posibles riesgos de manera anticipada, mitigando así la probabilidad de que ocurran.

Este enfoque innovador se ha traducido en una mayor eficiencia en nuestros procesos de revisión de proveedores, permitiéndonos agilizar las evaluaciones iniciales y, al mismo tiempo, mejorar la exhaustividad en la detección de riesgos. Como resultado, nuestro

cliente se encuentra mejor preparado para gestionar la seguridad de la información y garantizar la continuidad de negocio, lo que a su vez fortalece su posición competitiva en el mercado. La adopción de este modelo ha demostrado ser una inversión estratégica acertada que nos proporciona una mayor visibilidad y capacidad de respuesta ante los desafíos que puedan surgir en la cadena de suministro.

5 Trabajo a Futuro

Durante la ejecución de este proyecto, hemos identificado hallazgos críticos que señalan áreas en las que el cliente no cumple completamente con las regulaciones del Reglamento de Resiliencia Operacional Digital (DORA – Digital Operational Resilience Act), que le afecta ya que es una entidad financiera. Para abordar estas deficiencias y fortalecer aún más la postura en seguridad de la información y continuidad de negocio, se han propuesto una serie de iniciativas clave que serán consideradas en el futuro:

1. **Formación en Detección de Riesgos:** Para aprovechar al máximo nuestro nuevo modelo de gestión de riesgos, es esencial capacitar al personal del área en la identificación temprana de riesgos. La formación específica en este nuevo enfoque permitirá al equipos reconocer y evaluar de manera más efectiva los posibles riesgos emergentes en la cadena de suministro. Esta capacitación garantizará que todos los implicados estén al tanto de las amenazas y desafíos actuales.

2. **Calendario de Auditorías Priorizadas:** La auditoría de proveedores críticos es fundamental para mantener la seguridad y la continuidad del negocio. Se ha propuesto establecer un calendario estratégico para llevar a cabo auditorías periódicas en los proveedores críticos. Estos proveedores deben priorizarse en función de la dependencia que el cliente tenga de ellos. Para garantizar la imparcialidad y la eficacia de estas auditorías, cliente contratará una consultora externa.

3. **Evaluación de Pruebas de Penetración (Pentest):** Dada la importancia de la seguridad de la información, es crucial relizar pruebas de penetración a nuestros proveedores críticos. Se ha propuesto llevar a cabo ejercicios periódicos de estas pruebas con un proveedor contratado por cleinte, garantizando así que se mantengan los más altos estándares de seguridad cibernética y que cualquier vulnerabilidad potencial sea identificada y corregida de manera oportuna.

4. **Planes de Continuidad del Negocio (BCP) para Proveedores Críticos:** En caso de que un proveedor crítico experimente una interrupción que afecte su capacidad para prestar servicios, es fundamental contar con planes de continuidad del negocio sólidos. Es por eso que se intentará establecer conversaciones regulares con las áreas responsables de los proveedores críticos y con una alta dependencia de ellos para negociar acuerdos que permitan una transición fluida de la operativa del primer proveedor a otro en caso de una interrupción inesperada. Estos acuerdos de contingencia serán esenciales para minimizar el impacto en nuestra cadena de suministro y garantizar la continuidad de nuestras operaciones.

En resumen, estas iniciativas representarán pasos cruciales hacia la mejora continua de nuestra estrategia de gestión de riesgos en proveedores. Al abordar la formación, las auditorías, las pruebas de penetración y los planes de continuidad del negocio de manera proactiva, fortalecemos la capacidad para identificar, mitigar y responder a los riesgos en la cadena de suministro de manera efectiva y garantizar la seguridad y continuidad de la operaciones de cliente a largo plazo.