Herminio del Campo
Director general del Centro de Cooperación Interbancaria

Antonio Ramos
CEO de LEET Security

"El objetivo de Pinakes es aligerar la auditoría de los proveedores del sector financiero"

El Centro de Cooperación Interbancaria y LEET Security acaban de anunciar la puesta en marcha del proyecto Pinakes. Se trata de un servicio destinado a las entidades financieras para facilitar la auditoría de ciberseguridad de todos sus proveedores, tal como les obliga la nueva normativa EBA. Pero este marco de referencia no solo beneficia a las entidades, sino también a los propios proveedores. Herminio del Campo y Antonio Ramos, que han coordinado este proyecto, nos explican sus principales claves.

Por Enrique González

¿Qué actividad desarrolla el Centro de Cooperación Interbancaria, especialmente en lo referido a riesgos y seguridad de las entidades?

Herminio del Campo (HC): El Centro de Cooperación Interbancaria es una asociación sin ánimo de lucro que aglutina a las entidades de depósito que operan en España. Está formado por bancos, cajas de ahorros y cooperativas de crédito. Somos una asociación que trabaja en modo colaborativo, no competitivo.

Nuestros fines son servir de foro para el diálogo y la innovación interbancarios, desarrollar ideas de interés para el sector y ejercer de vehículo para el desarrollo y funcionamiento de los proyectos que las entidades consideren necesarios.

La actividad se vertebra en cuatro grandes áreas: Riesgos, Seguridad y prevención del fraude, Estándares y operaciones y Regulación. Es en la segunda de ellas, a través de la Comisión de Seguridad y Fraude, desde donde se ha abordado esta iniciativa.

Acaban de anunciar la puesta en marcha del proyecto Pinakes. ¿Cuál es el origen de esta iniciativa?

Antonio Ramos (AR): Las primeras conversaciones fueron a finales de 2019. A partir de ahí, constituimos un grupo de trabajo del Centro de Cooperación Interbancaria y durante 2020 trabajamos en la definición del servicio, la preparación del marco contractual, de las relaciones, de las herramientas que hacen falta, etcétera.

El origen del proyecto está en la normativa de la Autoridad Bancaria Europea [EBA, por sus siglas en inglés] que obliga a las entidades financieras a supervisar la seguridad de sus proveedores. Las entidades se han dado cuenta de que, con sus propios medios, solo pueden llegar a un grupo muy reducido de proveedores críticos y buscan una forma más eficiente de dar cumplimiento a ese requisito.

Pinakes será también mejor para los proveedores porque, al fin y al cabo, hablamos de un proceso que aligera muchísimo las necesidades de *due dilligence*. Básicamente porque, en lugar de tener un proceso de este tipo en la parte de ciberseguridad por cada entidad, pasan a tener uno solo.

A grandes rasgos, ¿en qué consiste este proyecto?

HC: Como decíamos, uno de los requisitos de la regulación de la EBA es verificar los niveles de ciberseguridad de los proveedores. Una de las opciones que ofrece la normativa es que las entidades hagan esta verificación mediante una calificación de un tercero externo, y ahí es donde encaja Pinakes.

En el servicio intervienen cuatro actores: el propio *hub*, las entidades adheridas, los proveedores y los evaluadores. Estos últimos son empresas de auditoría que cumplen unos requisitos y que están homologadas por el propio Pinakes.

El flujo del proceso comienza cuando la entidad financiera va a contratar un servicio con un proveedor. En ese caso, una de las opciones que tiene la entidad para verificar la seguridad de su proveedor es pedirle su calificación en el *hub*. Es el propio proveedor el que, una vez consultado a Pinakes qué evaluadores están homologados, elige y contrata a aquel que es de su elección en una relación bilateral ajena al *hub*.

La empresa elige al auditor que quiera y tendrían un contrato al margen del *hub*. En el momento en el que haya finalizado la auditoría, el propio proveedor presentará el resultado y, con ello, se le otorga una calificación.

Dicha calificación la publicamos en la plataforma que da soporte a todo el servicio y estaría a disposición de todas las entidades adheridas, de manera que pueden saber qué proveedores tienen determinada calificación para un servicio concreto. Es decir, el proveedor no tiene que volver a pasar por el proceso de calificación en caso de que otra entidad financiera adherida a este servicio quiera contratar el servicio auditado.

¿Qué criterios tiene que cumplir un evaluador para formar parte de Pinakes?

AR: Básicamente, hemos hecho un esquema de homologación equiparable al que ha propuesto la Comisión Europea para la certificación de seguridad en *cloud* o al que pide la autoridad de Luxemburgo para la certificación de protección de datos. Es un marco que coge lo mejor de los dos mundos, que es, por un lado el ISAE 3000, que es un estándar que permite emitir los informes de tipo SOC 2; y por otro lado, la ISO 17065, que permite la certificación de producto y es la que utiliza el Esquema Nacional de Seguridad como marco de referencia. Juntando esos dos mundos, hemos creado un marco de condiciones que tienen que cumplir los evaluadores, que abarca competencias, responsabilidad sobre los informes emitidos, independencia respecto de los clientes, capacitación del personal que realiza las funciones, permitir la supervisión por parte del *hub* y de las entidades financieras, así como el supervisor, etcétera.

Estamos viendo que las entidades que estarán dentro de este esquema son las auditoras que conocemos típicamente, como las Big Four más todas las que están haciendo en España informes de tipo SOC 2.

Aparte de eso, también como LEET Security, optaremos a esa homologación por tener la condición de certificadora 17065 y además estar reconocida por ENISA para aspectos de seguridad.

¿Cuál será el papel de LEET Security una vez puesto en marcha el proyecto?

AR: Este es un tema que hemos revisado con mucho cuidado por temas de competencia. Por un lado, LEET Security es la licenciataria de la metodología de evaluación, lo que conlleva una serie de trabajos relacionados con el mantenimiento y la evolución del referencial. Y por otro, actuaremos como evaluador homologado en las mismas condiciones que el resto. A partir de ahí, somos uno más en la ecuación.

> "Pinakes proporciona la evaluación más completa posible de todos los aspectos de ciberseguridad de los proveedores de entidades financieras"

Además de formar parte de Pinakes, ¿las entidades financieras llevarán a cabo otro tipo de contrataciones o evaluaciones con terceros para mantener cierta independencia del proyecto?

AR: Hay que tener en cuenta que el servicio de Pinakes sirve para la evaluación de aspectos de ciberseguridad. Pero cuando una entidad hace un proceso de *due dilligence*, tiene que incluir otros aspectos en la ecuación, no solo ciberseguridad. Lo que busca el *hub* es aligerar esa parte del proceso, pero las entidades financieras tendrán su toma de decisión y su proceso de *due dilligence* que deberá ser más completo.

Herminio del Campo.

Además pueden existir aspectos concretos que la entidad quiera revisar de manera puntual. Por ejemplo, hemos visto entidades que requieren a sus proveedores que tengan unas VPN configuradas a través de unos dispositivos de una marca y manera concretas para una determinada interconexión.

No obstante, la adhesión de las entidades Pinakes se hace para aceptar la evaluación que salga de Pinakes, con independencia de que luego puedan hacer auditorías adicionales.

¿Qué van a evaluar de un proveedor?

AR: Nos hemos basado en el marco que teníamos ya en LEET Security, que llevamos probando cinco años, y hemos añadido los requisitos de todas las entidades para construir un referencial más completo. Se van a evaluar desde aspectos genéricos, como pueda ser el sistema de gestión que tenga implementado el proveedor, pasando por aspectos de operación de seguridad, seguridad personal, seguridad de las instalaciones, protección frente a *malware*, continuidad y contingencia, desarrollos seguros, gestión de incidencias, criptografía, monitorización... Es decir, la evaluación más completa posible de todos los aspectos de seguridad.

Siguiendo la filosofía de la calificación, hemos establecido para la evaluación 14 dominios, 76 secciones y en torno a 350 capacidades distintas de seguridad. Lo que se evalúa son cada una de esas 350 capacidades y en esos resultados se basa Pinakes para construir la calificación final. No todas las capacidades aplicarán en todos los casos, obviamente; por ejemplo, si se trata de un servicio que no conlleva desarrollo, pues el desarrollo no se evalúa.

Si hubiera un incidente de ciberseguridad con alguno de los proveedores adscritos a Pinakes, ¿qué papel desempeñaría el *hub*?

AR: Las propias entidades financieras nos han pedido que pudiera haber un punto único de información para simplificar el acceso al estado más actualizado posible de un incidente. Pinakes no pretende actuar ni como CERT ni como mecanismo de coordinación a respuesta de emergencias, pero queremos es simplificar el acceso a la información. Lo que nos dicen las entidades es que han tenido situaciones en el pasado donde un proveedor que daba servicio a 25 entidades ha tenido un incidente. Qué ocurre, que hay 25 personas llamando al responsable de ese proveedor para preguntarle cómo está el incidente y al final no da abasto para atender al teléfono. Por eso buscamos un punto donde podamos tener un report actualizado de cómo está ese incidente y luego ya habrá que llamarle y preguntarle dudas puntuales. Pero no hará falta llamarle simplemente para que nos dé un status; para eso se pueden conectar a la web y ver cómo está la situación. Así descargamos un poco al proveedor y le dejamos centrarse en resolver el incidente, que es lo verdaderamente importante de estas situaciones.

Antonio Ramos.

HC: Seremos cuidadosos en ese aspecto porque hay proveedores con cláusulas de confidencialidad firmadas con sus propios clientes y ahí no podemos entrar.

¿Cuál será la vigencia de las calificaciones?

HC: La calificación tiene una vigencia temporal de un año y aparejado a la calificación están los servicios de coordinación de la información y de monitorización de incidentes.

AR: Durante la vigencia de la duración del contrato de la calificación habrá por parte de Pinakes una supervisión del nivel de seguridad digital. Está basada en los típicos raiting de IP de huella en Internet del proveedor, y lo que se va a hacer es una vigilancia, una monitorización exhaustiva de cada uno de los proveedores que estén formando parte de Pinakes para que, si se produce una modificación significativa de su nivel de calificación, el equipo de gestión Pinakes se pueda poner en contacto con él para preguntarle qué está pasando. Porque lo que se busca no es solo la calificación inicial, sino también la supervisión y la vigilancia, que es otro de los requisitos de la EBA. ■