Cyber resiliencia en el sector asegurador

Daniel Hernández Arroyo // Director, Cyber Risk Advisory. Deloitte

Resiliencia en el sector asegurador

Comenzaremos por ubicar dos términos que, aunque son considerados básicos en materia de seguridad de la información, ayudarán a centrar el foco en este artículo: **ciberseguridad y ciberresiliencia**.

Por un lado, ciberseguridad, concepto definido como el conjunto de medidas de prevención y contención establecidas en una Organización para la protección ante una amenaza en los sistemas, equipos, aplicaciones, redes o información de esta.

En la actualidad los sistemas de información se han convertido en uno de los activos de mayor valor en las Organizaciones y el mayor foco para el ataque en los ciberdelincuentes. En este contexto, los atacantes buscarán el daño en los sistemas ante cualquiera de los tres pilares de la información:

- **Confidencialidad:** entendida en el ámbito de la ciberseguridad, como la protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros, así como de la configuración incluida en los dispositivos tecnológicos involucrados.
- **Integridad:** referido a la correctitud y completitud de los datos en un sistema de información. Cuando los contenidos o configuraciones de estos se modifican, la integridad de los datos almacenados puede perderse de diferentes maneras.
- **Disponibilidad:** La disponibilidad es la proporción de tiempo que un sistema está en condiciones de funcionamiento. Al mismo tiempo es un protocolo de diseño e implementación que asegura un cierto grado absoluto de continuidad operacional durante un período de medición dado.

En este entorno y, para minimizar los posibles impactos de un incidente de seguridad, aparece nuestro otro termino citado, **ciberresiliencia**, concepto el cual define la capacidad de las Organizaciones para hacer frente a la respuesta y recuperación de los incidentes ocurridos a través de las actividades de gestión y seguimiento.

Identificado el contexto del que hablaremos, el **objetivo del presente documento** es **analizar** tanto el estado actual de las **capacidades de ciberresiliencia** que las Organizaciones del **sector asegurador** disponen, como de aquellas capacidades que, considerando su nivel de amenaza, sería recomendable que dispusieran para su protección.

¿Cómo deberían afrontar la preparación y respuesta de incidentes de seguridad las empresas del sector seguros?

Las nuevas amenazas asociadas a los entornos tecnológicos (*ransomware*, explotación de vulnerabilidades, *phishing*, robo de información, etc.) son los nuevos retos a los que las Organizaciones deben hacer frente en el proceso de la digitalización actual.

Con el propósito de minimizar el riesgo de estas amenazas en las Organizaciones, es necesario establecer procedimientos, medidas y acciones para la respuesta a incidentes de seguridad y establecer por tanto el modelo de gobierno (roles, comités, *reporting*, etc.) asociado a estas actividades.

Para saber **cómo, cuándo y porqué** actuar en el momento de la crisis o incidente, se han identificado diferentes actividades de preparación previa que las Organizaciones deberán trabajar para dotarse de las capacidades idóneas de cara a una correcta gestión de incidentes de seguridad en la fase de respuesta:

- **Modelo de gobierno para la respuesta ante incidentes:** enfocado en la identificación y formalización de los roles y responsabilidades asociadas a las actividades de respuesta ante incidentes, así como en la definición de los comités y flujos de comunicación necesarios para la gestión en el momento del incidente.
- **Desarrollo y procedimiento de respuesta ante incidentes** para el análisis y adaptación en la Organización de actividades de mitigación y control durante el momento del incidente. Este procedimiento incluirá las actividades asocia-

das a cada una de las fases de la respuesta del incidente, así como las acciones necesarias de cara al cierre y aprendizaje del incidente.

- **Análisis de riesgos** que incluya la matriz de riesgos para analizar las diferentes probabilidades de que se produzca un incidente de seguridad y la posible formalización de playbooks específicos de actuación ante estos riesgos.
- **Medidas de seguridad implementadas** para la mitigación y contención de los impactos asociados al incidente de seguridad.
- **Simulaciones y *cyberwargaming*** para el entrenamiento y uso de las capacidades anteriores e identificar posibles *gaps* en el momento de respuesta.

Estas actividades ayudarán a las Organizaciones a estar preparadas en el momento en que ocurra el incidente, minimizando los impactos asociados.

Por desgracia, la implementación de estas capacidades previas no implica que las Organizaciones no puedan tener incidentes de seguridad, por lo que es necesario **saber y poder responder ante estos**. Por ello, una vez implementados estos pasos previos, es necesario estipular diferentes **fases** de cara al **triaje y gestión** del propio incidente una vez que ya se ha producido, así como tener las capacidades necesarias para la respuesta ante el incidente, ya sea de manera interna y externa.

- **En primer lugar, será necesario realizar una fase de análisis** donde el objetivo es entender el alcance del incidente, su naturaleza y su criticidad. Con los resultados obtenidos se procurará la elaboración de un plan efectivo de contención, erradicación y recuperación.
- **Paralelamente se deberán realizar las labores de contención** con el fin de evitar que el incidente se propague de forma descontrolada, llevando a cabo acciones que permitan mitigar el impacto simultáneamente con otras acciones de análisis o erradicación. Para garantizar una contención adecuada a la casuística del incidente y sus impactos, es necesario haber realizado previamente una exhaustiva labor de análisis del incidente, que podrá evitar posibles efectos indeseados o de rebote.
- **Realizadas las labores de contención y controlado el alcance del incidente, es necesario iniciar las actividades de erradicación** para eliminar el vector de entrada y sus efectos asociados y poder reestablecer los servicios a su estado habitual. La adecuada erradicación del incidente dependerá de un correcto análisis e identificación previos y será en general más sencilla cuanto mejor sea su contención.
- **Por último, es necesario volver a la normalidad gracias a las actividades de recuperación** una vez que la Organización haya contenido y erradicado el incidente. En esta fase es muy importante asegurar que la erradicación se ha ejecutado con éxito, y estar preparado para dar solución de manera más eficaz ante un mismo incidente.

Visión actual para la gestión del riesgo

La **gestión del riesgo** en materia de ciberseguridad en una Organización es difícil de abordar y en la cual los productos de ciberseguro deberán seguir jugando un papel fundamental. Si bien no resulta sencillo cuantificar los posibles impactos derivados de un incidente, el poder contar con un equipo de respuesta eficaz que permita asegurar una rápida contención de la amenaza se presenta como un elemento clave a la hora de asumir riesgos y asegurar activos clave de una Organización, puesto que más allá del potencial impacto que subyazca de todo ataque, se podrá situar una contraparte eficaz que mitigue (en la medida de lo posible) dicho impacto. Estamos hablando obviamente de los **equipos de Respuesta a Incidentes de alto rendimiento**, sobre el cual existen una serie de particularidades en su composición que merece la pena considerar.

Comencemos por el principio; complementando el concepto de **ciberseguridad** citado anteriormente, este podría ser interpretado como una conjunción de tres elementos fundamentales: **Protección, Detección y Respuesta**. Pese a que este enfoque se acerca a un concepto axiomático, no parece que esté siendo suficientemente ágil nuestra aproximación al mismo si nos fijamos en las implementaciones reales de productos y servicios bajo un enfoque integrado.

De la misma manera, existe una aproximación que indica que **la seguridad no es un producto sino un proceso**. Sin duda, debemos reevaluar continuamente la postura de seguridad ante un panorama de amenazas siempre cambiante.

Si pasamos a un **punto de vista táctico**, la ciberseguridad puede interpretarse tanto como un producto como un proceso, no dejando de ser una conjunción de personas, procesos, tecnología e información. La

variable de cada dominio sería la proporcionalidad de cada uno de estos factores:

- Los sistemas de **Protección** se apoyan fundamentalmente en tecnología, con cierto nivel de apoyo por parte de personas y procesos.
- La **Detección** requiere proporciones más o menos iguales de personas, procesos y tecnología.
- La **Respuesta** tiene un alto componente de personas, con una asistencia crítica de proceso y tecnología.

> La Respuesta a Incidentes requiere de personas, puesto que la inteligencia humana que debe aplicarse resulta ser el factor diferencial

Cuando afrontas multitud de incidentes llegas a sacar una serie de conclusiones relevantes, y una de ellas es que, hoy en día, intentar **automatizar de forma íntegra las actuaciones de Respuesta** es algo complicado y poco eficaz.

La red interna de cada Organización es diferente. Cada incidente, pese a tener nexos comunes en formato de campañas de ataque tiene una afección diferente. Los entornos de seguridad de cada organización son diferentes, así como la idiosincrasia de cada cual. Todas las Organizaciones son diferentes, y las consideraciones políticas y económicas suelen ser más importantes que las técnicas. La **Respuesta a Incidentes requiere de personas**, puesto que la inteligencia humana que debe aplicarse resulta ser el factor diferencial.

Esto lo podemos interpretar como algo relativamente nuevo para la industria de la ciberseguridad, y debe traducirse en una percepción diferente de los servicios de Respuesta. Si prestamos atención a cómo se ha percibido la industria de ciberseguridad, uno de los problemas de los que adolece es aquel denominado como ***"Market lemons"***. Este es un término prestado de *slung* económico el cual hace una analogía refiriéndose a un mercado en el que los compradores no pueden diferenciar entre los productos de calidad de otros que no lo son. En estos mercados, los productos mediocres desplazan a los productos de calidad puesto que el precio es el factor de decisión, ya que no existe una forma efectiva de comprobar la calidad del producto (como por ejemplo antivirus, FW, IDSs, etc.)

Una vez más la respuesta a incidentes se presenta como una práctica diferente, y es sensible (y mucho) al factor humano. Los mejores "productos" serán por tanto aquellos que cuenten con el mejor equipo humano, puesto que los compradores aquí sí podrán percibir la calidad en la interactuación con el producto. Bajo este enfoque, cobra aquí especial relevancia la premisa propuesta en su día por Lorrie Faith Cranor de que *"los diseñadores de sistemas deberían diseñar sus sistemas para apoyar a los humanos en el proceso, con objeto de maximizar sus posibilidades de realizar con éxito sus funciones críticas para la seguridad"*.

La lectura que puede extraerse de todo este enfoque determinará por tanto que **el equipo humano que ofrezca esa ansiada Respuesta a Incidentes será el mayor valor del proceso,** y que toda aseguradora que pretenda defender su **apetito al riesgo** deberá de tener en consideración dicha casuística con el fin de abordar esta aventura con la mayor de las probabilidades de éxito. Nunca habrá una certeza de riesgo pseudo cero, pero sí la de abordar una contingencia bajo el mejor enfoque y con el mejor equipo.

Reflexiones finales

Paulatinamente, la estabilidad y prosperidad de nuestra sociedad tiene un mayor grado de dependencia de la seguridad y confiabilidad del ciberespacio, cualidades que pueden verse comprometidas por causas técnicas o agresiones deliberadas como las que hemos vivido estos días.

Todo sabemos que no hay seguridad al cien por cien, pero sí es posible hacer que sea un poco más seguro. Para ello, la anticipación es clave; hay que ir por delante de los ciberataques: ser capaces de detectarlos y prevenirlos. Esto requiere continuidad y constancia en la vigilancia y, llegado el caso, efectividad en la respuesta.

La lectura de las pautas anteriores no hace sino transmitir el mensaje de la clara necesidad de poner remedio a las carencias de las compañías aseguradoras en materia de ciberseguridad. El culpable nunca es la víctima (nuestros clientes), pero no puede obviarse que el hecho de no seguir unas adecuadas medidas y buenas prácticas puede tener como consecuencia que algunas de ellas –que tratan y almacenan

en sus sistemas con información muy sensible para ellas mismas, sus empleados y sus clientes– se hayan visto comprometidas.

El esfuerzo actual que se está realizando por los reguladores para armonizar normativas y concienciar sobre la verdadera relevancia que tienen los riesgos cibernéticos en las empresas aseguradoras motiva a que se realicen mayores esfuerzos por mejorar la preparación y flexibilidad de respuesta ante ataques informáticos. Así, una mayor concienciación, junto con los recientes cambios regulatorios, han propiciado que las compañías del sector seguros hayan ido realizando un mayor esfuerzo inversor en actividades de protección de su información y sus sistemas. Este aspecto, las hace, a su vez, más resistentes frente a ataques informáticos y más rápidas para recuperarse de su operatividad en caso de incidente.

En la UE, distintas normativas generales (GDPR, Directiva NIS) regulan la obligatoriedad de notificar la existencia de brechas de seguridad en las organizaciones, así como su naturaleza, impacto, tipo de información afectada, etc. Esto es, las entidades aseguradoras, en caso de sufrir una brecha de seguridad, tienen la obligación de notificar dicha incidencia y, por tanto, es mucho mayor la notoriedad y alcance que puede darse al suceso. Asimismo, se contemplan sanciones para quienes no cumplan con su deber de protección de la información sensible mantenida en los sistemas corporativos, cuya sustracción o publicación pueda suponer un impacto negativo en la sociedad en general.

Precisamente por regulaciones como estas, las compañías aseguradoras están viendo la necesidad de realizar un mayor esfuerzo en ciberseguridad, lo que se ha traducido no solo en mejores medidas técnicas, sino también en una mayor concienciación de sus empleados con el objetivo de evitar que el error humano pueda suponer una fuga de información o una vía de entrada para el *malware*.

Otro indicador de esta situación es la contratación por parte de sus clientes de las llamadas ciberpólizas, consistentes en un seguro cibernético contratado para cubrirse por los daños que pueda ocasionarle un ataque informático que algunas de las compañías aseguradoras ya comercializan con éxito desde hace años. La proliferación de este tipo de seguros muestra una vez más que existe una mayor concienciación y aceptación de que la seguridad informática es una necesidad real para las empresas.

La heterogeneidad y el cambiante escenario del estado de riesgo del ciberespacio suponen un desafío continuo para las compañías aseguradoras que son clientes de Deloitte en los distintos países. Ninguna organización a título individual, por sí misma, dispone de todas las capacidades necesarias para garantizar su ciberseguridad ni tampoco los estados la del ciberespacio nacional.

Por tanto, es nuestro deber como *partner* de confianza en Ciberseguridad trasladar a nuestros clientes que solo desde la mejora de las capacidades de detección y análisis de ciberamenazas, contar con diversas fuentes de ciberinteligencia, la cooperación y colaboración entre empresas del sector e incluso público–privada, la instauración de mecanismos ágiles de coordinación entre proveedores y la capacitación y especialización de los equipos humanos y tecnológicos de las propias aseguradoras y el fomento de la concienciación y educación en materia de ciberseguridad a todos los niveles: empleados, directivo, brokers, y sus propios asegurados se podrá alcanzar un nivel de seguridad acorde a un estado de riesgo conocido y controlado para atajar y minimizar el impacto de ciberataques. ●