CISO: El nuevo traje del emperador

Estamos observando normativas y regulaciones orientadas a empoderar la figura del CISO y por tanto, la función de la Ciberseguridad. Ahora bien, existen elementos fuera del ámbito de la Ciberseguridad relacionados con la madurez del gobierno corporativo o la gestión de la tecnología que deberían estar implantados para garantizar este 'empoderamiento'. Sin estos elementos, podemos correr el riesgo de hacer un nuevo traje que no cubra aspectos básicos de la Ciberseguridad ni proporcionen el soporte necesario a su función y su misión acordes a las expectativas esperadas.

Es innegable el valor de las nuevas directrices y normativas que directa o indirectamente están fortaleciendo la figura del CISO contribuyendo a que pueda cumplir su misión y función. Ahora bien, para empoderar la figura del responsable de Ciberseguridad, además de la dotación de recursos, son necesarios elementos que exigen una madurez en el gobierno corporativo y en la gestión de la tecnología.

Y esta es la cuestión que me gustaría esbozar aprovechando el relato de Andersen: ¿Cuáles son algunas de las condiciones que necesita el *nuevo* traje del CISO para que el relato tenga un final distinto al conocido en el cuento?

Para ser sucinto utilizaré el formato de preguntas que apuntan a las respuestas y en si traslucen las problemáticas que hay que resolver y que todos los responsables de Ciberseguridad conocemos pero que necesitamos recordarlas conjuntamente.

¿Existe una madurez de gobierno en tecnología para acompañar al nivel ciberseguridad necesitado?

Igualmente, no me refiero al uso intensivo y extensivo de arquitecturas, herramientas y servicios de *última generación* por parte de las áreas de tecnología para dar cobertura a las unidades de negocio. Estoy apelando a la madurez en procesos y procedimientos para tener insertados controles de ciberseguridad que **1)** garanticen una seguridad por diseño, **2)** una mitigación eficaz y eficiente de vulnerabilidades en todos los ámbitos (sistemas, desarrollo) y **3)** puestas en producción de servicios seguros. Y también apunto a una madurez de gestión y operación de la tecnología para implementar nuevas arquitecturas y medidas de Protección, Detección y Respuesta.

¿Existe una gestión formal de riesgos?

No estoy hablando de disponer de "pesadas" herramientas de análisis de riesgos de dudosa utilidad con su cohorte de consultores y mantenedores. Me estoy refiriendo a lo importante una vez que tenemos identificados los riesgos, su gestión: su presentación en Comités directivos donde se aporte el detalle de los riesgos en Ciberseguridad, se doten de recursos para su mitigación o la aceptación formal de estos con un acto implícito de asunción de responsabilidades en tales Comités. Estas *aceptaciones* formales de riesgos (que deberían ser las mínimas) incluirían recortes presupuestarios en materia de Ciberseguridad y priorizaciones de proyectos de negocio (justificables y necesarios) frente a necesidades de Ciberseguridad.

¿Existen o están implantadas las tres líneas de defensa?

Este modelo, muy simplificado distingue a tres grupos (líneas) que dentro de una organización participan en una gestión de riesgos: **1)** grupos que implantan y operan controles, **2)** un segundo grupo responsable de los controles que define y supervisa su implantación en toda la compañía y **3)** un tercer nivel que revisa todo el marco de controles de los dos primeros grupos. En un ejemplo, igualmente simplificado, tendríamos en la primera línea –entre otros– a las unidades de Tecnología, en la segunda línea a Ciberseguridad y en la tercera a Auditoría interna.

Los objetivos de este modelo son la eficacia, eficiencia, control e independencia en el aseguramiento de la Ciberseguridad. Pues bien, ¿realmente está articulado y funcionando un modelo de independencia entre Ciberseguridad y Tecnología donde esta última aplica los controles de ciberseguridad en tiempo y forma? ¿Las unidades de Auditoría de Sistemas tienen capacidad para verificar que los controles de Ciberseguridad están implantados y son eficaces y eficientes?

En mi opinión, estas áreas de *gobierno* (Tecnología, Riesgos y Control) son importantes y con estas consideraciones he querido apuntar a necesidades para que los responsables de seguridad puedan acometer eficaz y eficientemente su función en el marco de roles y responsabilidades que se le quiere atribuir (el nuevo *traje*).

¿Realmente está articulado y funcionando un modelo de independencia entre Ciberseguridad y Tecnología donde esta última aplica los controles de ciberseguridad en tiempo y forma?

Creo que, sin estas coberturas, podemos correr el riesgo de hacer un *traje* nuevo al emperador y, sin embargo, en su paseo ante su público (la cruda realidad) observemos con una simple mirada inocente que el emperador se encuentra realmente desnudo. ■

DAMIÁN RUIZ SORIANO
CISO
SINGULAR BANK