TOLERANCIA AL CAMBIO

Uno de los últimos factores que hay que tener en cuenta a la hora de comprender el grado de aceptación de las empresas a la necesidad de “nadar entre tiburones” es su capacidad de adaptarse al cambio en el ámbito de las TI. Como se ha mencionado anteriormente en este informe, los criterios de buenas prácticas en materia de ciberseguridad suponen una variación con respecto a los comportamientos tradicionales que se han ido desarrollando a lo largo de décadas. Para poder modificar la mentalidad y la filosofía en el ámbito de la seguridad, es fundamental tener la capacidad de dar la bienvenida al cambio en las TI subyacentes.

Un ejemplo clave en este sentido es la transformación digital, una de las principales razones por las que las empresas se ven, de entrada, obligadas a adentrarse en aguas infestadas de tiburones. Es posible que la práctica habitual entre los profesionales de la seguridad sea la de tratar de impedir la adopción de nuevas tecnologías como social business, movilidad, Big Data/análisis de datos y la nube. Adoptarlas supone correr riesgos. No obstante, este no es el enfoque más maduro; en vez de poner trabas a la transformación digital, las empresas inteligentes deben tratar de alentar a sus usuarios, poniendo a su disposición las herramientas necesarias para adoptar la transformación digital de forma segura.

Como se indica en la Figura 4 a continuación, cuanto más madura es una organización según lo definido por el marco de este estudio, más cómoda se siente adaptándose a los cambios en las TI. En el otro extremo, las empresas menos maduras tienden a pasarlo mal con cualquier cambio en el ámbito de las TI o, cuando menos, tienen dificultades cuando se les pide que implementen otros cambios a las aplicaciones y servicios que no sean los mínimos. No obstante, a medida que vamos subiendo por la escala de madurez, va siendo más probable que la empresa se describa a sí misma como capacitada para adaptarse a dichos cambios o, incluso, "muy capacitada" para ello.

Estos hallazgos muestran que, en el contexto actual de la seguridad, una de las claves para ser una empresa exitosa y dinámica reside en adoptar un enfoque maduro sobre la seguridad y ser capaz de sacar partido a los cambios en las TI (en vez de tenerles miedo). La puerta se abre en ambas direcciones, siendo un asunto reflejo del otro. La capacidad de efectuar cambios en las TI requiere conocer en profundidad las posibles implicaciones en materia de seguridad. Al mismo tiempo, para adoptar una postura madura sobre seguridad, es fundamental tener la capacidad de implementar los cambios necesarios en las TI.

Capacidad de adaptarse al cambio según el nivel de madurez en el ámbito de la ciberseguridad

Q2. When it comes to business requests for new or enhanced applications or services, which statement best reflects your IT department`s capabilities?

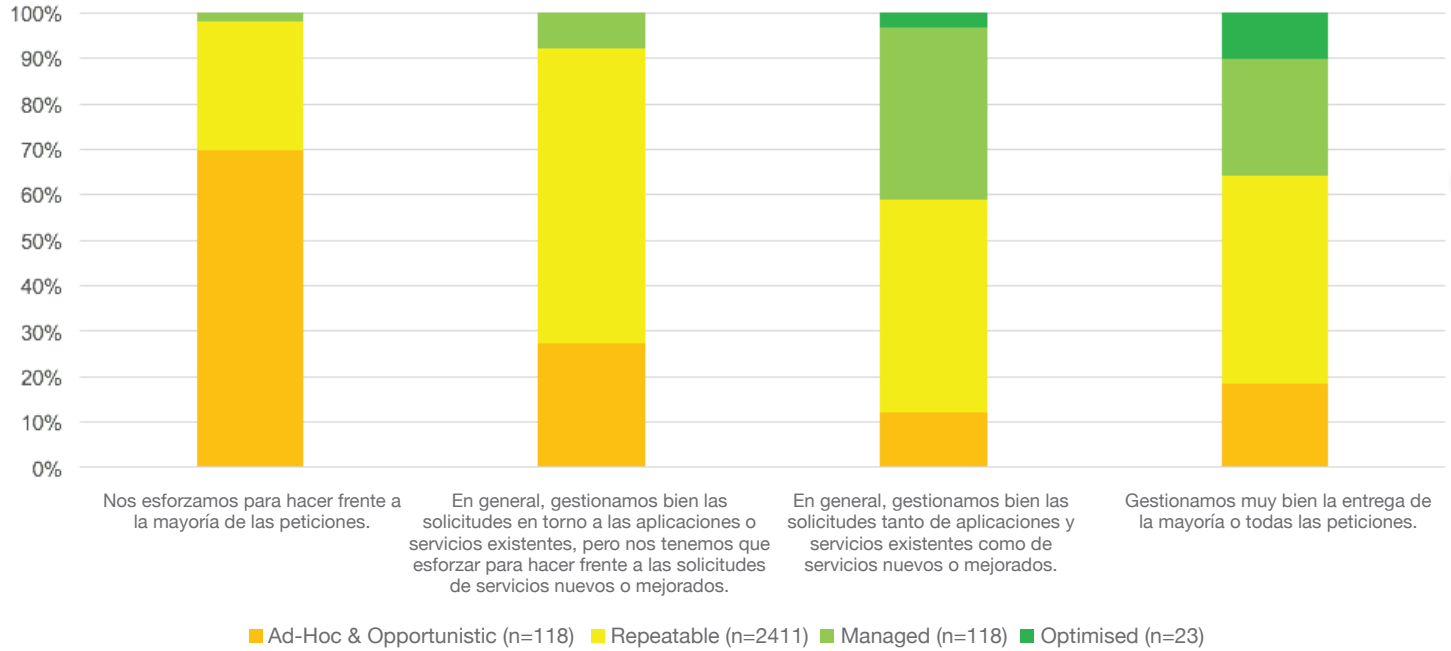

Figura 4 *Fuente: IDC, 2016*

10 RECOMENDACIONES PARA SU ORGANIZACIÓN

A continuación, se incluyen diez recomendaciones que proporcionan un marco para que su empresa mejore su nivel de madurez en el ámbito de la seguridad:

- **Compare su posición con la de empresas similares en términos de sector, tamaño y ubicación geográfica.**
- **Determine el grado de madurez de su empresa y hasta dónde está dispuesta a llegar.**
- **Determine las carencias de su enfoque actual en materia de seguridad comparándolo con el nivel al que desea llegar.**
- **Considere la posibilidad de recurrir a especialistas en seguridad externos para ayudarle a diseñar e implementar los cambios necesarios para alcanzar su objetivo.**
- **Identifique los procesos y actividades de seguridad que son vitales en comparación con aquellos que tienen poco valor y son repetitivos.**
- **Piense en qué áreas se podrían automatizar actividades de menor valor para reducir el uso de recursos.**
- **Investigue en qué casos se podría obtener una mejora de resultados trabajando con PSSG. Las actividades de menor valor pueden ser un buen punto de partida para aprovechar los modelos globales e industrializados de prestación de servicios.**
- **Sin embargo, a medida que los SSG van siendo cada vez más habituales en los negocios, piense en dónde podrían encontrarse recursos especializados que sean capaces de mejorar los resultados deseados, teniendo en cuenta no solo el coste sino también la calidad.**
- **Adopte un enfoque de seguridad basado en riesgos que abarque toda la empresa. Todos los usuarios constituyen una "amenaza interna" potencial, por lo que la cultura y la estrategia en materia de seguridad deben ser integrales.**
- **Haga partícipes a los responsables de seguridad de las nuevas iniciativas empresariales desde el principio. Si se asegura de que las nuevas iniciativas sean "seguras desde su diseño", se ahorrará problemas más adelante.**