CC-CISO-CSO-CSTO-CTRO-DPO… ¿Alguno lo tiene claro?

José de la Peña Muñoz
Director
jpm@codasic.com

La pregunta que propone este año Securmática (¿Qué le está pasando a la ciberseguridad?) se las trae. Y la respuesta, más. Algunos sabios ventilan el asunto diciendo que lo que le sucede es que está de moda. Pero cuando les preguntas que qué entienden ellos por ciberseguridad, les tiemblan los párpados y optan por esconder su ignorancia tras el siempre socorrido: "Es un tema complejo". Y tanto.

Más allá de la definición del palabro, lo primero que procede decir es que las prácticas de la gestión de riesgos de seguridad de la información y la ciberseguridad constituyen una actividad apasionante todavía en fase de estabilización. Y en ese proceso, hay algunas interesantes bifurcaciones; una de ellas, la que separa el terreno de la seguridad tecnológica del de la seguridad de la información (CSTO-Chief Security Technology Officer y CISO-Chief Information Security Officer). Esta, por decirlo de algún modo, queda en "casa". Pero la siguiente no; a saber: la seguridad de la información y la protección de los datos de carácter personal (CISO y DPO). ¿Qué campo le corresponde a cada uno? Sobre el papel, el CISO tiene una función que englobaría la del DPO. Por otra parte, sin seguridad tecnológica no puede existir un razonable control de la seguridad de la información, incluidos los datos personales. Será apasionante observar aquí las pugnas entre tecnólogos y juristas, y de juristas con juristas (DPO/CO-Compliance Officer) y tecnólogos con tecnólogos (CTRO-Chief Technology Risk Officer/CISO/CSTO). La luz se puede hacer si incorporamos al guiso la función de prevención del fraude.

Lo impepinable es que el encargado de gestionar los riesgos de seguridad tiene que entender de la gestión de riesgos de ciberseguridad. ¿Le afecta esto al CSO (Chief Security Officer)? Sí; en la medida en que la mayoría de CSO procede de campos ajenos al escenario que hoy dibujan las TIC. El nuevo CSO que demandan las compañías debe dominar también el terreno digital. Sin ello, no podrá gestionar correctamente la seguridad de la alta dirección y del resto de estamentos y procesos de su compañía. O al menos otros estarán mejor armados para hacerlo, porque tienen a su alcance habilitarse en los quehaceres de la seguridad clásica. Y también pueden fichar especialistas.

> "El nuevo CSO que demandan las compañías debe dominar el terreno digital para poder gestionar la seguridad de los estamentos y procesos de su compañía. Si no otros actores, los más versados en la ciberseguridad, estarán mejor armados para hacerlo, porque tienen a su alcance habilitarse en los quehaceres de la seguridad clásica y también fichar especialistas".

¿Qué le pasa al CISO?

Visto que la ciberseguridad es una disciplina, y que quienes la dominan son profesionales y entienden de la materia, lo lógico es que en las compañías nombren CISO a expertos que, además de tener otras habilidades, sepan de ciberseguridad. ¿Sucede esto? Suceden otras cosas. Aquí van algunas: consideración de directivo corporativo (en el mejor de los casos) no de primer nivel; desproporción entre sus potestades y sus responsabilidades; disputas razonables con otras áreas (lo de que la ciberseguridad es cosa de todos, aunque cierto, conviene matizarlo: no es lo mismo diseñar controles, gestionar la ciberseguridad y auditar controles); indefinición de la frontera que separa su campo de actividad de la del DPO (en el supuesto de que las funciones estén separadas); pocas armas para poner fin a la habilidad que tienen otros directivos de áreas muy establecidas (personal, marketing, recursos humanos, I+D, contabilidad, jurídico, comercial…) para desentenderse del uso seguro de la información tratada en y por sus áreas; falta de recursos corporativos para controlar adecuadamente los procesos externalizados y al externalizador y su selección.

Y de la ciberinseguridad, ¿qué?

Viva está, no cabe duda, porque los delincuentes ya tienen a pleno gas las churreras para ir renovando su catálogo de productos y servicios; es decir, para ir abandonando las líneas de actividad que alcancen la línea roja de peligro e ir abriendo otras nuevas en las que el botín compense la asunción de los riesgos derivados. Y es que la actividad de la delincuencia organizada (principalmente la económica) tiene más fundamento que lo que enseñan en muchas escuelas de negocios.

Como decía, la ciberinseguridad está viva. Y la ciberseguridad, también. Se huele la cercanía de novedades. ¿Cuáles? Pues aquí dejo algunas: el rol del CISO en el modelo PIC; la reglamentación de la seguridad informática en base a la Ley de Seguridad Privada; la interpretación de los fiscales de los delitos contra los datos y sistemas informáticos, y de los delitos de acceso ilegal a sistemas e interceptación de datos; las estrategias de ataque a la rentabilidad de las acciones de la delincuencia organizada (la ciber y la que se manifiesta combinando el medio tradicional y el ciber); el juego que puede dar el recién llegado sector asegurador; las notificaciones de incidentes (sector público y privado), una encrucijada en la que no parece que la mano derecha (la legislación penal y algunas normativas sectoriales) se haya hablado con la izquierda (la legislación sobre protección de datos de carácter personal).

Mientras tanto, se seguirán haciendo cábalas acerca de cuándo estará publicado el RGPD (lo divertido será conocer la interpretación Made in Spain del texto), de cuándo tendremos Directiva NIS (su trasposición también debería ser interesante, aunque cuando acontezca quizá algunos estemos ya prejubilados o desvinculados o suspendidos o despedidos o retirados), y de si habrá en España gobierno o elecciones generales (aunque se firme un pacto). ●