CISO transformado, CISO regulado

José de la Peña Muñoz
Director
jpm@codasic.com

Bajo la escrutadora mirada del auditor, el CISO es quien se encarga de que la política de seguridad de la información de la corporación se cumpla y de informar a sus mayores del estado de la ciberseguridad en cualquier dimensión, sea o no regulada.

Guiándose por su sagacidad, el sector en el que opera su entidad, su habilidad para pactar, su espíritu de servicio y la dirección de los vientos organizativos –entre otros factores–, algunos CISOs (con plan y presupuesto), han ido creciendo y estructurando su departamento para atender áreas de interés, ya en el terreno de la operación, ya en el normativo y de cumplimiento legal: seguridad de datos personales, IaM segura, gestión de incidentes, gestión de proveedores, prescripción, prevención de ciberfraude…

Algunas altos directivos se han percatado de que el CISO debe tener una posición alta en el organigrama y, en ocasiones, trato directo con el Consejero Delegado o con el Presidente. Conciben al CISO como una figura clave en la optimización y el cumplimiento. No lo consideran un "stopper", sino pieza maestra del día a día y en la conquista de la dimensión digital.

El CISO ya dejó de ser una larva para convertirse en crisálida. Falta que tras una metamorfosis completa, salga adaptado a las funciones que vayan demandado los servicios y la estandarización de procesos en la transformación digital.

CISO y CTSO

En las empresas con directivos poco leídos o presos de su propia historia, se le confunde con la función de seguridad TIC. ¡Craso error! El CIO, que debe estar en el Comité de Dirección y participar de forma destacada en las decisiones sobre seguridad de la información (entre otras), debe tener en su departamento una función de seguridad TIC (la de Chief Technology Security Officer-CTSO) a fin de que el SI tecnológico soporte la política corporativa de seguridad de la información. Sin embargo, algunos magníficos CISOs dependen hoy del CIO. La excepción es justificada en no pocos casos, especialmente en aquellos en los que el CIO está a la vanguardia del negocio.

¿Quién suple al CISO?

¿Qué figura existente podría convertir al CISO en innecesario? Creo que ninguna. Antes bien, el CIO y el CSO deben verle como un colaborador leal y con personalidad propia; el CDO como una fuente de alternativas a algunos de sus problemas; y el DPO como un experto en tratamiento de la información, en la gestión de riesgos, en la protección de datos personales y en ciberseguridad.

Certificación profesional

¿De quién debe colgar el CISO? Las regulaciones celtibéricas se decantan hoy por el CSO. Aunque depende: no es lo mismo un banco, una telco, una industria, un operador de IC, un regulado por el futuro reglamento de desarrollo de la ley de Seguridad Privada, una administración pública o una mixtura.

En mi opinión, el departamento del CSO, que debe ser el adecuado para proteger a la compañía en todo escenario (incluido el digital), no está culturalmente preparado (al menos, todavía) para liderar la metamorfosis de la transformación. Ese terreno es más propio del CIO, el CDO y el CISO. Aunque hay excelentes CISOs que cuelgan de excelentes CSO.

Con la futura transposición de la Directiva NIS se abre la oportunidad de regular de modo general la actividad de CISO, de señalar de qué debe entender y de plantear la creación de un esquema de certificación profesional voluntaria acorde con la UE.

Se verá. Mientras tanto, y como dice un amigo, el DPO debe encargarse de que la multa sea lo más baja posible, y el CISO de proteger a la entidad de los ciberataques. ¿Cuál es más rentable? ●