DIARIO FINANCIERO®

Fecha: 22/04/2025 Audiencia: 48.450 Sección: ACTUALIDAD
Vpe: $6.195.918 Tirada: 16.150 Frecuencia: DIARIO
Vpe pág: $7.443.240 Difusión: 16.150
Vpe portada: $7.443.240 Ocupación: 83,24%

DF
DIARIO FINANCIERO®
DF LAB
INNOVACIÓN, STARTUPS & TECH

CAROLINA FLISFISCH
SOCIA DE CARIOLA DÍEZ PÉREZ-COTAPOS

OLIVER ORTIZ
GERENTE DE INTANGIBLES, DATA PRIVACY & TECHNOLOGY DELOITTE LEGAL

Los riesgos de coexistencia entre los cargos de las leyes de protección de datos y ciberseguridad

POR MARCO ZECCHETTO

■ Expertos advierten que no existe un mecanismo para armonizar estos puestos -que podrían tener diferencias para gestionar riesgos e interpretar incidentes- y llaman a resolverlo con políticas internas.

Con la aprobación de la Ley de Protección y Tratamiento de Datos Personales (que entrará en vigor en diciembre 2026) y la Ley Marco de Ciberseguridad (vigente desde 1 de enero) se crean dos nuevos cargos: el delegado de protección de datos (DPO, en inglés) y el delegado de ciberseguridad, obligatorio para las firmas que califiquen como operadores de importancia vital (OIV).

Según expertos consultados, estos roles podrían entrar en conflicto con un puesto ya existente: el director de seguridad de la información (CISO, en inglés), si no se definen claramente sus funciones o si una empresa decide fusionar los cargos, lo que deberá resolverse dentro de las compañías, porque no hay mecanismos regulatorios de armonización.

La abogada y socia de Cariola Díez Pérez-Cotapos, Carolina Flisfisch, comentó que el delegado de protección de datos se encargará de informar, supervisar y asesorar el cumplimiento de la normativa y de las políticas internas de la organización y actuará como un punto de contacto entre los titulares de los datos y la futura Agencia de Protección de Datos Personales.

Según Flisfisch, la ley no impide al DPO desempeñar otras funciones, pero aclara que aunque asuma otras, "debe ser independiente", porque la mezcla de tareas podría generar "incompatibilidades" si una empresa decide integrar ambos roles en un solo puesto.

"Una misma persona eventualmente podría ejercer un cargo de CISO y delegado de protección de datos. El CISO es quien define qué herramienta de seguridad se va a utilizar. Si este decide, por ejemplo, qué tecnología se va a usar para procesar ciertos datos o incluso la finalidad de uso de estos, dónde se van a almacenar, ahí estaría interviniendo en los fines y medios, entonces como DPO no tendría la independencia necesaria", afirmó la abogada.

En tanto, el gerente de Intangibles, Data Privacy & Technology de Deloitte Legal, Oliver Ortiz, advirtió que los nuevos cargos presentan desafíos en la gestión de riesgos ante incidentes, como ciberamenazas.

Señaló que podría existir un conflicto en la "determinación de la gravedad y el impacto de una brecha". Mientras el CISO se va a enfocar en la continuidad operativa, el DPO en cómo el incidente afecta los derechos de los titulares de datos personales.

"Puede que el CISO diga que un incidente es de alta gravedad y que el DPO señale que es de baja gravedad. Ahí podría existir cierto roce en la gestión de los riesgos", afirmó Ortiz.

Explicó, por ejemplo, que, ante un eventual incidente de ciberseguridad, como un *ransomware* (secuestro de datos) que comprometa los sistemas de un operador de importancia vital y al mismo tiempo pudiera filtrar datos personales de clientes, se requeriría de una acción coordinada para reportar a ambas agencias -de Protección de Datos Personales y Agencia Nacional de Ciberseguridad (ANCI)-, pero si surgen diferencias entre los cargos y demoras, esto podría exponer a la empresa desde daño reputacional hasta infracciones por incumplimiento.

"Si el CISO dice 'tenemos que reportar ahora porque tenemos un plazo de 48 horas', es muy probable que el DPO diga 'primero necesito saber no solamente que hubo una brecha, sino cuáles son los datos, sus categorías y volumen, y quiénes son esos titulares para poder hacer un reporte más correcto'. Pueden quedar en una encrucijada e incluso generarse una infracción por no cumplir con el deber de reportar", añadió.

Ortiz también se refirió al delegado de ciberseguridad, un nuevo rol de "perfil normativo" que actuará como contraparte de la ANCI y será responsable de informar incidentes a las autoridades y a los directores y principales ejecutivos de la organización privada. Si bien no menciona riesgos, explicó que deberá trabajar con el CISO, que tiene un rol "fundamentalmente técnico", a cargo de la gestión estratégica y operativa de seguridad de la información.

"Desde un punto de vista de la responsabilidad proactiva que mandatan las normas internacionales en la materia, la función del delegado (de ciberseguridad) debería ir más allá de lo comunicacional y acompañar al CISO", dijo el ejecutivo.

Ortiz comentó que la ley no establece límites normativos o de conflictos de intereses si una empresa decide que el CISO sea también el delegado de ciberseguridad.

Resolver las diferencias

Flisfisch comentó que hoy no hay mecanismos normativos para armonizar funciones o evitar eventuales roces o conflictos de interés entre el delegado de protección de datos y el CISO, por lo que la definición y separación de roles queda bajo criterio de las políticas internas que definan las compañías.

También enfatizó en la necesidad de que las empresas aborden ambas normativas de forma "integral" para evitar ineficiencias ante aspectos técnicos, legales y de seguridad, ya que esto "influye de manera relevante en su negocio y por lo tanto tienen que abordar todos estos aspectos en forma transversal".

Por otro lado, Ortiz dijo que para evitar diferencias entre el DPO y el director de seguridad de la información a la hora de definir la gravedad de un incidente, "quien esté arriba de ellos va a tener que establecer cómo se gestionan estos riesgos, qué recursos destina para cubrirlos, y cuál tiene mayor preponderancia".