MYRIAD CONTIGO:

Obligación Patronal de Mitigar Riesgos en Planes de Retiro

Mayo 2021

En el mes de abril, luego de así requerirlo la Oficina de Responsabilidad Gubernamental de los Estados Unidos, el Departamento del Trabajo federal (en adelante DOL, por sus siglas en inglés) confirmó que, en planes de beneficios para empleados, la parte fiduciaria tiene la obligación de administrar los riesgos asociados a la seguridad cibernética de esos planes patrocinados por el patrono. Ello, en un esfuerzo por mitigar los riesgos inherentes a la acumulación global de sobre un trillón de dólares que recogen los 401(k) y otros planes de retiro.

Las guías del DOL confirman la responsabilidad del fiduciario de mitigar estos riesgos y las mismas constan de tres áreas principales: la contratación del proveedor de servicios, las mejores prácticas en la seguridad cibernética y la seguridad cuando los participantes manejan sus cuentas en línea. Si bien estas guías fueron publicadas a modo de sugerencia y no como un requisito, es razonable presumir que el DOL considerará el cumplimiento de estas guías como la expectativa o estándar mínimo de cumplimiento del fiduciario para con su responsabilidad.

Previo a la contratación de un proveedor de servicios, el DOL sugiere evaluarle mediante preguntas sobre sus estándares en la seguridad de información, sus políticas de auditoría y los resultados, cómo validan sus prácticas, el nivel de seguridad implementado y logrado, así como la divulgación de posibles brechas de seguridad. Por su parte, el contrato de servicios debe requerir al proveedor que realice auditorías anuales por un tercero, identificar la rapidez con que se informará al fiduciario sobre cualquier brecha y especificar que el proveedor deberá cumplir con toda legislación aplicable a asuntos de privacidad, confidencialidad o seguridad y a la información personal de los participantes.

El DOL ha identificado las mejores prácticas de seguridad cibernética para los encargados de informática y fiduciarios, entre ellas: contar con un programa formal y bien documentado de seguridad cibernética; crear un programa prudente de evaluación anual de riesgo; contratar a terceros para realizar una auditoría anual de los controles de seguridad; definir y asignar con claridad los roles y responsabilidades de cada participante de la seguridad de la información; garantizar procedimientos firmes de control de acceso; evaluar el uso de la nube informática por parte del proveedor de servicios; realizar adiestramientos anuales de concienciación sobre seguridad cibernética; implementar un programa seguro del ciclo de vida del desarrollo de sistemas (SDLC, por sus siglas en inglés); implementar un programa de resiliencia empresarial dirigido a la continuidad de las operaciones, la recuperación de un desastre y la respuesta a incidentes; codificar datos sensitivos; implementar controles técnicos sólidos para, a su vez, implementar las mejores prácticas de seguridad; y ser responsivo a brechas o incidentes de seguridad cibernética.

El componente final de las guías del DOL va dirigido a los pasos que los participantes y beneficiarios pueden tomar para mitigar potenciales riesgos a la seguridad cibernética. Estos pasos pueden incluir el acceso o vigilancia regular de sus cuentas, el uso de contraseñas adecuadas con múltiples elementos (combinación de letras, números y símbolos), mantener actualizada la información de contacto e inscribirse para recibir notificaciones sobre cualquier actividad o cambio en las cuentas.

Para nosotros en Myriad, es importante mantenerte informado sobre los últimos cambios o requerimientos del DOL o de cualquier legislación estatal o federal. ¡Cuenta con nosotros!