El día 17 de octubre de 2024 está prevista la transposición en España de la Directiva (UE) 2022/2555, del Parlamento Europeo y del Consejo, por la que se exige a los Estados miembros la implementación de medidas de gestión de riegos de ciberseguridad y notificaciones en sectores críticos y se establecen normas relativas a la cooperación, el intercambio de información, la supervisión y la ejecución.

Con esta Directiva se establece un marco regulador con el objetivo de mejorar el nivel de ciberseguridad en la Unión Europea.

1. Ámbito de aplicación

La Directiva resulta de aplicación a las entidades públicas o privadas medianas (más de 50 trabajadores) y grandes (más de 250 trabajadores), que operen en los siguientes sectores, considerados como críticos:

- Energía (electricidad, calefacción y refrigeración urbanas, crudo, gas e hidrógeno)
- Transporte
- Banca e infraestructuras de los mercados financieros
- Sector sanitario
- Agua potable
- Aguas residuales
- Infraestructura digital (proveedore de servicios de datos, de computación en la nube, de redes públicas de comunicaciones electrónicas y de servicios de comunicaciones electrónicas disponibles para el público).
- Gestión de servicios de Tecnologías de la información y de las comunicaciones (TIC).
- Entidades de la Administración publica central y regional, con exclusión del poder judicial, los parlamentos y los bancos centrales.
- Espacio.
- Servicios postales y de mensajería.
- Gestión de residuos
- Fabricación, producción y distribución de sustancias y mezclas químicas.
- Producción, transformación y distribución de alimentos.
- Fabricación de productos sanitarios, informáticos, electrónicos, ópticos, eléctricos, determinada maquinaria, vehículos de motor y material de transporte.
- Proveedores de servicios digitales de mercados en línea, motores de búsqueda y plataformas de servicios de redes sociales.
- Investigación.

Sin perjuicio de lo anterior, independientemente de su tamaño, la Directiva también se aplicará a las entidades cuando:

a) los servicios son prestados por:

i) proveedores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles para el público;
ii) prestadores de servicios de confianza;
iii) registros de nombres de dominio de primer nivel y proveedores de servicios de sistema de nombres de dominio;

b) la entidad sea el único proveedor en un Estado miembro de un servicio esencial para el mantenimiento de actividades sociales o económicas críticas;

c) una perturbación del servicio prestado por la entidad pudiera tener repercusiones significativas sobre la seguridad pública, el orden público o la salud pública;

d) una perturbación del servicio prestado por la entidad pudiera inducir riesgos sistémicos significativos, en particular para los sectores en los que tal perturbación podría tener repercusiones de carácter transfronterizo;

e) la entidad sea crítica a la luz de su importancia específica a nivel nacional o regional para el sector o tipo de servicio en concreto o para otros sectores interdependientes en el Estado miembro;

f) la entidad sea una entidad de la Administración pública central o regional, si esta última presta servicios cuya perturbación podría tener un impacto significativo en actividades sociales o económicas críticas.

Los Estados miembros podrán disponer la aplicación de la Directiva a las entidades de la Administracion pública local y a los centros de enseñanza.

2. Medidas técnicas, operativas y organizativas

Las entidades incluidas dentro del ámbito de aplicación de la Directiva deben adoptar, al menos, las siguientes medidas técnicas, operativas y de organización para gestionar los riesgos que se planteen para la seguridad de los sistemas de redes y de información que utilizan en sus operaciones o en la prestación de sus servicios y prevenir o minimizar las repercusiones de los incidentes en los destinatarios de sus servicios y en otros servicios:

- Políticas de seguridad de los sistemas de información y análisis de riesgos
- Protocolos de gestión de incidentes
- Procedimientos para garantizar la continuidad de las actividades (como la gestión de copias de seguridad y la recuperación en caso de catástrofe).
- Medidas para garantizar la seguridad en la adquisición, el desarrollo y el mantenimiento de sistemas de redes y de información, incluida la gestión y divulgación de las vulnerabilidades.
- Políticas y procedimientos para evaluar la eficacia de las medidas.
- Prácticas básicas de ciberhigiene y formación en ciberseguridad
- Políticas y procedimientos relativos a la utilización de criptografía y, en su caso, de cifrado.
- Protocolos de seguridad de los recursos humanos y políticas de control de acceso y de gestión de activos.
- Soluciones de autenticación multifactorial o continua, comunicaciones de voz, vídeo y texto seguras y sistemas seguros de comunicaciones de emergencia.

3. Régimen sancionador y formación obligatoria

La Directiva establece la posibilidad de que los Estados miembros impongan multas administrativas para sancionar su incumplimiento hasta un máximo 10.000.000 € o el 2% del volumen de negocios anual total a nivel mundial de la empresa a la que pertenece la entidad esencial durante el ejercicio financiero anterior, optándose por la de mayor cuantía.

Y, por otra parte, también se establece la obligación de los Estados miembros de velar por que los órganos de dirección de las entidades aprueben las medidas que deban ser adoptadas, reciban formación obligatoria y ofrezcan periódicamente a sus empleados formaciones similares que les permitan adquirir conocimientos y destrezas suficientes para detectar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en los servicios proporcionados.

El departamento de IT de *Glezco Asesores y Consultores* pone a su disposición personal cualificado y con experiencia que ayudarán a adaptar sus sistemas a la normativa.