ECIJA

NOTA INFORMATIVA

Novedades en obligaciones de NIS 2

Al día siguiente de la plena aplicación de NIS 2, la Comisión Europea ha publicado un Reglamento de Ejecución en el que se definen cuestiones relativas a la clasificación de incidentes de seguridad y medidas de seguridad referidas a la gestión de riesgos.

Lo que necesitas saber

- El Reglamento de Ejecución define cuestiones relativas a la clasificación de incidentes de seguridad y medidas de seguridad referidas a la gestión de riesgos.

- Este reglamento define su alcance para varios proveedores de servicios, incluyendo servicios de confianza, computación en nube, centros de datos, redes de distribución de contenidos, servicios gestionados, mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales.

- Se definen los criterios para determinar qué se entenderá por incidente significativo y recurrente.

- Se incluyen medidas de seguridad detalladas para la gestión del riesgo, como la política de seguridad y de gestión de riesgos de seguridad, la política de continuidad de negocio y gestión de crisis, y la política de criptografía.

El viernes 18 de octubre, siendo el primer día de aplicación efectiva de la Directiva 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (en adelante, "***Directiva NIS 2***"), se publicó por parte de la Comisión Europea, un Reglamento de Ejecución para detallar cuestiones específicas relativas a la consideración de los incidentes de seguridad y medidas concretas para ser aplicadas por los sujetos obligados.

1. Aplicación del Reglamento de Ejecución

Concretamente, dicho Reglamento de Ejecución define su alcance para:

- Proveedores de servicios de DNS.
- Registros de nombres de dominio de primer nivel.
- Proveedores de servicios de computación en nube.
- Proveedores de servicios de centros de datos.
- Proveedores de redes de distribución de contenidos.
- Proveedores de servicios gestionados.
- Proveedores de servicios gestionados de seguridad.
- Proveedores de mercados en línea.
- Motores de búsqueda en línea y de plataformas de servicios de redes sociales.
- Proveedores de servicios de confianza.

Así las cosas, el Reglamento de Ejecución desarrolla los artículos 21.2 (medidas de ciberseguridad para gestión del riesgo) y 23.3 de la Directiva NIS 2 (obligaciones de reporte) constando de un documento principal y un anexo al mismo.

No obstante, lo anterior, debido a la falta de una concreción mayor de las medidas de la Directiva NIS 2, **este Reglamento de Ejecución puede servir como guía, para otros sujetos obligados**.

El Reglamento de Ejecución se publicará en el Diario Oficial oportunamente y entrará en vigor veinte días después.

2. Incidentes significativos y recurrentes

En el documento principal **se definen los criterios para determinar qué se entenderá por incidente significativo y recurrente**, igualmente determina en su artículo primero que las entidades mentadas anteriormente deberán implementar medidas de gestión de los riesgos de la ciberseguridad según viene definido en el Anexo.

En este sentido, **se entenderá como incidente significativo** cuando uno o más de estos criterios sean cumplidos:

- El incidente ha causado o puede causar un perjuicio económico superior a 500 000 euros o al 5 % del volumen de negocios anual total (la cantidad que sea menor).
- El incidente ha causado o puede causar la exfiltración de secretos comerciales.
- El incidente ha causado o puede causar la muerte de personas.

- El incidente ha causado o puede causar daños considerables a la salud de personas.
- Se ha producido un acceso exitoso, presuntamente malintencionado y no autorizado a la red y a los sistemas de información, capaz de causar graves perturbaciones operativas.
- Se trata de un incidente recurrente.
- El incidente cumple uno o varios de los criterios establecidos en los artículos 5 a 14.

No se considerarán incidentes significativos las interrupciones programadas del servicio ni las consecuencias previstas de las operaciones de mantenimiento programado realizadas por las entidades pertinentes o en su nombre.

Con respecto a los incidentes recurrentes, se considerarán colectivamente como un incidente significativo cuando cumplan todos los criterios siguientes:

- Que hayan ocurrido al menos dos veces en un plazo de 6 meses.
- Que tengan la misma causa raíz aparente.
- Que cumplan colectivamente los criterios establecidos en la letra a) del apartado 1 del artículo 3.

3. Medidas de seguridad para la gestión del riesgo

Como ya se ha indicado, en el Anexo del Reglamento de Ejecución **se procede a incluir las medidas de seguridad para la gestión del riesgo** de manera más detallada y específica que en la generalidad que quedan descritas en la Directiva NIS 2.

3.1. Política de seguridad y de gestión de riesgos de seguridad

Por ello, **se atiende en primer lugar al contenido que se ha incluir en la política de seguridad de las redes y los sistemas de información**. En este apartado se incluye la necesidad de establecer los objetivos de seguridad de este documento en concordancia con los comprendidos en la estrategia empresarial de la entidad. Asimismo, se determina la necesidad de revisar y aprobar la política al menos una vez al año, o en su caso, cuando concurran incidentes significativos.

Entre los puntos que se han incluir en dicha política, cabe destacar:

- La inclusión un **compromiso de mejora continua** de la seguridad de la red y de los sistemas de información.
- La inclusión de un **compromiso de proporcionar los recursos adecuados necesarios para su aplicación**, incluidos el personal, los recursos financieros, los procesos, las herramientas y las tecnologías necesarios.
- La **comunicación a los empleados pertinentes y a las partes externas** interesadas y el reconocimiento por ellos.
- La **enumeración de la documentación** que debe conservarse y el **plazo de conservación** de esta.
- La **enumeración de las políticas temáticas** específicas.

- **La inclusión de indicadores y medidas para supervisar su aplicación** y el estado actual del nivel de madurez de las entidades pertinentes en materia de seguridad de las redes y de la información.
- **La inserción de la fecha de aprobación formal** por los órganos de dirección de las entidades pertinentes.

Además, se requiere que los roles de seguridad queden asignados, revisándose dichas funciones y responsabilidades periódicamente. A ello, se debe incluir que el propio anexo **determina de forma expresa la necesidad de contar con una política de control de accesos que permita gestionar las cuentas privilegiadas de los roles específicos de forma adecuada**, implementando medidas de seguridad reforzadas como autenticación multifactor (MFA) y autorización, así como permitir el uso exclusivo para tareas de administración del sistema.

Adicionalmente, se incluye la **necesidad de documentar un plan de tratamiento de riesgos y los riesgos residuales que debe ser aprobado por la alta dirección**. Asimismo, recoge la necesidad de **realizar una revisión periódica del plan**, así como de la política, de cara a realizar un control monitorizado sobre el cumplimiento y el estado de la ciberseguridad. Con carácter excepcional, se contempla igualmente, la necesidad de realizar revisiones de la política y del plan cuando ocurran incidentes importantes

En este sentido, el documento **contempla la revisión de la gestión de la seguridad anual por personal independientes con competencias apropiadas, y sus resultados deben ser reportados a la dirección**.

Se debe establecer una política que defina roles y responsabilidades para la detección, análisis, contención, respuesta, recuperación y notificación de incidentes y que sea coherente con los planes de continuidad de negocio. Por ello, las entidades deben:

- Implementar procedimientos y herramientas para **monitorear, registrar y custodiar la información referida a actividades en sus sistemas** con el fin de detectar eventos que puedan considerarse incidentes.
- **Implementar mecanismos simples** para que empleados, proveedores y clientes reporten eventos sospechosos.
- **Realizar evaluaciones de los eventos detectados para determinar si constituyen incidentes**, aplicando criterios predefinidos.
- Implementar **procedimientos para contener, erradicar y recuperar los sistemas afectados por incidentes.** Por lo que se requiere documentar un procedimiento que permita la resiliencia de los servicios, incluyendo la revisión de este con carácter periódico.
- **Realizar revisiones detalladas después de que los sistemas se hayan recuperado después de sufrir incidentes**, con el fin de poder identificar el origen del incidente y poder documentar aspectos aprendidos como consecuencia de los mismos.

3.2. Política de continuidad de negocio y gestión de crisis

Vinculado con el punto anterior, el Anexo desglosa igualmente los requisitos básicos que deben cubrir tanto el plan de continuidad de negocio, como los procesos de la gestión de crisis.

Como ya recoge la normativa, las entidades **han de implementar y mantener un plan de continuidad de negocio**, plan que tiene como finalidad recuperar/restablecer las operaciones y servicio después de sufrir un incidente. Para poder desarrollar un plan adecuado, además de partir de la política de seguridad de las redes y los sistemas de información, y en particular, de los resultados del análisis de riesgos e impacto empresarial, **estos planes de continuidad de negocio han de recoger los procedimientos de recuperación de operaciones de forma detallada, así como la asignación de los responsables que asumen esta obligación por rol**.

Asimismo, se menciona la necesidad de **contar con copias de seguridad**, garantizando un nivel adecuado de redundancia, incluyendo los plazos de conservación necesarios de dichas copias de seguridad. En este sentido, se expresa la necesidad **de realizar pruebas de cara a garantizar la efectividad de las copias de seguridad** realizadas con el fin de proporcionar la recuperación del servicio de forma adecuada.

Por otro lado, las entidades deben contar con un **proceso de gestión de crisis** que, además de ser revisado periódicamente, ha de contener por lo menos:

- **Funciones y responsabilidades del personal** (así como de proveedores y prestadores de servicios, en su caso) junto con la asignación de las respectivas funciones en situaciones de crisis.
- **Medios de comunicación adecuados entre las partes y las autoridades competentes pertinentes**. En estos medios se tendrán en cuenta tanto aquellas comunicaciones obligatorias, (por ejemplo, ante incidentes), como comunicaciones no obligatorias.
- Medidas adecuadas para garantizar **el mantenimiento de la seguridad en situaciones de crisis.**

3.3. Política de seguridad de la cadena de suministro

Se ha de establecer un **criterio de selección de proveedores**, incluyéndose entre otros aspectos, las prácticas de ciberseguridad y **procedimientos de desarrollo de la seguridad, gestión de vulnerabilidades, clasificación de los riesgos, y el nivel del servicio**, con el fin de mitigar los riesgos detectados para la seguridad de las redes y los sistemas de información.

En este sentido, **la entidad ha de establecer criterios para seleccionar y contratar a los proveedores y prestadores de servicios, incluyendo requisitos de seguridad para los productos y servicios TIC críticos**, asegurando que los proveedores cumplan con los mismos y valorando la capacidad que tienen los proveedores de cumplir, así como la seguridad de los productos o servicios. En esta valoración, se aplicará el principio de

"ciberseguridad desde el diseño", asegurando pruebas de seguridad en cada fase del desarrollo y de la relación contractual con dicho proveedor.
Igualmente, se atiende a la necesidad de **controlar y realizar revisiones periódicas de las prácticas de ciberseguridad de los proveedores**, con seguimiento de incidentes relacionados con los productos y servicios TIC que proveen.

3.4. Política de criptografía

En este sentido y atendiendo a la protección de la confidencialidad, veracidad e integridad de la información, se incluye la necesidad de **implementar una política y procedimientos relacionados** con la criptografía, incluyendo la gestión adecuada de las claves criptográficas y la selección de algoritmos seguros. Dicha política deberá tener en cuenta la clasificación de activos, así como el tipo y calidad de medidas criptográficas necesarias para proteger dichos activos.

3.5. Ciclo de vida de la seguridad de redes

La entidad establecerá y aplicará **procesos para gestionar los riesgos derivados de la adquisición de servicios de TIC o productos de TIC para componentes que sean críticos** para la seguridad de las redes y sistemas de información de las entidades pertinentes, sobre la base de la evaluación de riesgos realizada de conformidad a la política de gestión de riesgos. Estos procesos, que deberán de incluir **análisis vinculados con la gestión y evaluación de la seguridad en las fases de diseño, y de entornos de desarrollo**, incluyendo procesos de pruebas de seguridad durante el ciclo de vida, han de ser revisados forma periódica.

En ese sentido, dichos procesos, incluirán:

- **Requisitos de seguridad aplicables a los servicios/productos TIC** y garantía de que cumplen con los mismos.
- Requisitos relativos a las **actualizaciones de seguridad a lo largo de toda la vida útil de los servicios/productos TIC** (incluso atendiendo a la sustitución una vez finalizado el período de prueba).
- Descripción de los **componentes de hardware y software** utilizados.
- Descripción de las **funciones de ciberseguridad implementadas**.
- Implementar **metodología por escrito** de cara a validar que los servicios/productos TIC cumplen los requisitos de seguridad establecidos.

Asimismo, **se implementarán procedimientos de cara a gestionar cambios en los sistemas,** así como de correcciones necesarias a realizar en estos. Estas medidas además de someterse a pruebas periódicas de cara a valorar el alcance, y la adecuación de los procesos, deberán de ser revisadas con carácter periódico planificado o cuando se produzcan incidentes significativos o cambios importantes en las operaciones o los riesgos.

3.6. Higiene cibernética y concienciación

Las entidades deben **ofrecer programas de sensibilización en ciberseguridad para empleados, proveedores y clientes.** Estos programas deben informar sobre las amenazas relevantes y medidas básicas de higiene cibernética.
En los distintos programas de concienciación a empleados, y otro personal que se vea envuelto en los sistemas de la entidad**, se refuerza la importancia de que aquellos empleados con roles clave en seguridad, reciban formación continua en ciberseguridad**, incluyendo la gestión segura de dispositivos y la respuesta a incidentes.

En este sentido, cabe mencionar que el propio anexo, hace hincapié en la necesidad de garantizar que el personal interno y externo comprendan y cumplan con sus responsabilidades de seguridad, teniendo en cuenta el rol que ocupa cada una de las partes implicadas. También deben verificar antecedentes y competencias clave antes de contratar personal en roles críticos, incluso después de la finalización del contrato de un empleado.

3.7. Control de accesos

Las entidades, establecerán, **documentarán y aplicarán políticas de control de acceso lógico y físico que deberán de ser revisadas de forma periódica y cuando se produzcan incidentes significativos o cambios** importantes en las operaciones o los riesgos. Dicha política recogerá:

- **El acceso de las personas**, (visitantes, externos, proveedores y prestadores de servicios).
- El acceso y la necesidad de garantizar la concesión del acceso a los usuarios autenticados.
- La **gestión de los derechos de acceso a los sistemas** de red y mantener dichos registros.
- La inclusión de **políticas de gestión de cuentas privilegiadas y cuentas de administración** del sistema, incluyendo tanto la identificación, autenticación (con multifactor inclusive), así como el resto de los puntos recogidos en el punto 3.1, con respecto a la creación de cuentas privilegiadas.

3.8. Gestión de activos

Las **entidades determinarán los niveles de clasificación de todos los activos**, incluida la información, en el ámbito de sus redes y sistemas de información para el nivel de protección requerido, teniendo en cuenta confidencialidad, integridad, autenticidad y disponibilidad, para indicar la protección requerida en función de su sensibilidad, criticidad, riesgo y valor empresarial. Ello tendrá en cuenta tanto la gestión de riesgos, como la política de plan de continuidad de negocio establecido. Esta clasificación deberá de ser revisada, y en su caso, actualizada periódicamente.

Asimismo, **las entidades deberán de implementar una política de uso de activos que sea conforme a la política de seguridad** y en la que la misma cubra la seguridad de los

activos durante todo su ciclo de vida, incluido su adquisición, uso, almacenamiento, comunicación y supresión de conformidad al nivel de seguridad.

3.9. Seguridad física y ambiental

Con respecto a las medidas para prevenir pérdida daño o compromiso de la red o de los sistemas de información o interrupción a su operación debida a fallos e interrupciones se propone aplicar las siguientes medidas:

- **Proteger las instalaciones de los cortes de electricidad y otras interrupciones** en la electricidad, las telecomunicaciones, el suministro de agua, el gas, el alcantarillado, la ventilación y el aire acondicionado.
- **Proteger, redundar y supervisar los servicios de apoyo** anteriormente mencionados definiendo y controlando con umbrales de control.
- Celebrar **contratos para el suministro de emergencia** con los servicios correspondientes.
- **Garantizar la eficacia continua, supervisar, mantener y probar el suministro de la red** y los sistemas de información necesarios para el funcionamiento del servicio ofrecido, en particular la electricidad, el control de la temperatura y la humedad, las telecomunicaciones y la conexión a Internet.

Igualmente, en esta misma línea se deberán implantar:

- Medidas de **protección y control contra las amenazas físicas y medioambientales.**
- **Vigilar los parámetros medioambientales e informar al personal competente**, interno o externo, de los sucesos que superen los umbrales de control.

Con respecto al perímetro y a las medidas de control de acceso físico, se deberán implantar **medidas dirigidas a establecer perímetros de seguridad y proteger las zonas en las que se encuentran las redes y los sistemas de información** y otros activos asociados. Igualmente, se deberá diseñar y aplicar la seguridad física de las oficinas, salas e instalaciones supervisando continuamente las instalaciones para evitar el acceso físico no autorizado.

Área de Protección de Datos de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60