WISER

Wide-Impact cyber SEcurity Risk framework

Guía sobre la directiva europea de seguridad en redes y sistemas de información

Julio 2016

www.cyberwiser.eu | info@cyberwiser.eu | @cyberwiser

WISER es un Proyecto de innovación financiado por el programa Horizonte 2020, que desarrolla un framework de gestión de ciber riesgo con el fin de evaluar, monitorizar y minimizar riesgos. WISER desarrolla una suite de servicios para PYMES tecnológicas y para propietarios de sistemas ICT complejos e infraestructuras críticas, aplicable a múltiples industrias.

CyberWISER Light es un servicio gratuito online que comprende un cuestionario que proporciona al usuario un informe descargable sobre su perfil de ciber riesgo; y la posibilidad de hacer un test de vulnerabilidades para prevenir futuros ataques, generando de igual manera un informe que se puede descargar.

Nuevos servicios disponibles a finales de 2016:

CyberWISER-Essential: una solución llave en mano para gestión del riesgo en PYMES

CyberWISER-Plus: Una plataforma de gestión de riesgo como servicio (RMaaS) orientada a ciber sistemas de alta complejidad que requieren la implementación de controles especiales en su infraestructura ICT para ser monitorizados.

Aviso

El único propósito de esta guía es crear conciencia sobre la Directiva NIS para el sector público y privado.
Se recomienda encarecidamente a todas las organizaciones afectadas por esta directiva leer los documentos oficiales en el siguiente enlace:
http://ow.ly/pWO4302Gs10

Guía sobre la directiva europea de seguridad en redes y sistemas de información

La Directiva europea de Seguridad en Redes y Sistemas de Información (NIS) representa el primer paso en regulación sobre ciberseguridad a nivel de la Unión Europea.

La entrada en vigor de la Directiva NIS se programó para **Agosto de 2016**. Los Estados Miembros tendrán desde entonces **21 meses** para implementar esta Directiva en sus legislaciones nacionales, y 6 meses más para identificar a los operadores de servicios esenciales

El objetivo de esta Directiva es alcanzar un alto nivel de seguridad en redes y sistemas de información en la Unión Europea mediante:

» La mejora de las capacidades relativas a ciberseguridad a nivel nacional

» Un aumento de la cooperación a nivel de la Unión Europea.

» Hacer obligatoria la gestión de riesgos y la comunicación de incidentes para los operadores de servicios esenciales y los operadores de servicios digitales

1. Acciones de los Estados Miembros para incrementar y mejorar las capacidades de ciberseguridad a nivel nacional

Cada Estado Miembro adoptará una estrategia nacional a nivel de seguridad de red y sistemas de información, definiendo los objetivos estratégicos, políticas apropiadas y medidas regulatorias. Esta estrategia debería incluir:

» Objetivos estratégicos, prioridades y un marco de gobernanza.

» Identificación de medidas de preparación, respuesta y recuperación.

» Métodos de cooperación entre el sector público y el privado.

» Creación de conciencia, formación y educación.

» Planes de investigación y desarrollo relativos a la estrategia NIS.

» Plan de evaluación de riesgos.

» Lista de actores involucrados en la implementación de la estrategia

Los Estados Miembros designarán una o más autoridades nacionales competentes para la Directiva NIS, para monitorizar la aplicación de esta Directiva a nivel nacional.

Los Estados Miembros también designarán un punto de contacto único, que será el enlace que asegurará la cooperación transfronteriza con las autoridades relevantes en otros Estados Miembros y la aplicación de los mecanismos de cooperación creados por la propia Directiva.

Los Estados Miembros designarán uno o más equipos de respuesta a incidentes de seguridad en activos digitales. Estos equipos se responsabilizarán de, como mínimo:

» Monitorizar incidentes a nivel nacional.

» Proporcionar avisos tempranos, alertas, anuncios y diseminación de información a los actores relevantes sobre riesgos e incidentes.

» Responder a incidentes.

» Proporcionar un análisis de riesgos e incidentes dinámico y crear conciencia de la situación.

» Estar en contacto y participar de forma activa en la red de equipos de respuesta nacionales de los diversos Estados Miembros.

2. Acciones de los Estados Miembros para incrementar la cooperación a nivel de la Unión Europea

La Directiva NIS establece un Grupo de Cooperación, para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados Miembros y para desarrollar un clima de confianza.

También establece una red de equipos nacionales de respuesta para contribuir a la creación de un clima de confianza entre los Estados Miembros y para promocionar una cooperación operacional ágil y efectiva.

¿Qué hará el Grupo de Cooperación?

El Grupo de Cooperación comprenderá representantes de los Estados Miembros, de la Comisión Europea y de la agencia ENISA (Agencia

europea para la seguridad en redes y sistemas de información), con la Comisión Europea ejerciendo de Secretaria.

El Grupo de Cooperación trabajará en programas bienales, en cuatro áreas diferentes:

Planificación:

» Establecer un programa de trabajo 18 meses después de la entrada en vigor (Febrero de 2018).
» Preparar un programa de trabajo cada dos años de ahí en adelante.

Dirección:

» Guiar a los equipos de respuesta nacionales
» Asistir a los Estados Miembros en desarrollar las capacidades asociadas a NIS.
» Apoyar a los Estados Miembros a la hora de identificar a los operadores de servicios esenciales.
» Debatir buenas prácticas de notificación de incidentes.
» Debatir sobre estándares.
» Colaborar con cuerpos e instituciones relevantes de la Unión Europea.
» Evaluar las estrategias nacionales a nivel NIS y a los equipos de respuesta (de manera voluntaria).
» Compartir información y buenas practicas relativas a:
  » Riesgos
  » Incidentes
  » Creación de conciencia.
» Formación.
» I+D

Informar:

Cada año y medio, se emitirá un informe evaluando la experiencia adquirida con esta cooperación. El informe será enviado a la Comisión como contribución a la revisión del funcionamiento de la Directiva.

¿Qué harán los equipos de respuesta?

La red de equipos de respuesta comprenderá a representantes de cada uno de los equipos nacionales de los Estados Miembros, y al equipo de respuesta a situaciones de emergencia en activos digitales específico de los cuerpos, instituciones y agencias de la Unión Europea. La Comisión Europea participará en esta red como observador. ENISA proveerá la secretaría y apoyará activamente la cooperación entre los equipos.

Esta red realizará las siguientes tareas:

» Intercambiar información concerniente a los servicios, operaciones y cooperación de los equipos de respuesta.
» Intercambiar y analizar información relativa a incidentes (bajo demanda y de manera voluntaria)
» Identificar una respuesta coordenada al incidente (bajo demanda y voluntariamente)
» Apoyar la gestión de incidentes transfronterizos (de manera voluntaria)
» Explorar otras formas de cooperación operacional.
» Informar al Grupo de Cooperación de sus actividades y requerir asesoramiento y guía.
» Tratar sobre las lecciones aprendidas de la práctica de la NIS.
» Analizar problemas e incidentes sucedidos en la operación de cada equipo de respuesta (bajo demanda)
» Emitir guías y líneas maestras sobre cooperación operacional.

Dos años después de la entrada en vigor de la Directiva NIS, y cada 18 meses de ahí en adelante, la red de equipos de respuesta producirá un informe evaluando la experiencia adquirida gracias a la cooperación operacional, incluyendo conclusiones y recomendaciones. El informe será enviado a la Comisión como contribución a la revisión del buen funcionamiento de la Directiva.

La gestión del riesgo y la obligación de informar de incidentes ocurridos para operadores de servicios esenciales y proveedores de servicios digitales.

¿Qué son operadores de servicios esenciales, y qué se requerirá que hagan?

Los operadores de servicios esenciales son empresas privadas o entidades públicas que juegan un papel determinante para la sociedad y la economía.

Bajo la Directiva NIS, los operadores de servicios esenciales identificados tendrán que tomar medidas de seguridad apropiadas y notificar incidentes graves a la autoridad nacional relevante.

Las medidas de seguridad incluyen:

» Prevención de riesgos: Medidas técnicas y organizacionales que son proporcionadas y adecuadas al riesgo.
» Asegurar la seguridad de las redes y sistemas de información: las medidas deberían asegurar un nivel de seguridad en las redes y sistemas de información adecuado a los riesgos.

» Gestionar incidentes: Las medidas deberían minimizar el impacto de los incidentes en los sistemas IT que proporcionan los servicios esenciales.

¿Cómo identificarán los Estados Miembros a los operadores de servicios esenciales?

Cada Estado Miembro identificará las entidades que tienen que adoptar las medidas de seguridad apropiadas y notificar de incidentes significativos aplicando estos criterios:

(1) La entidad proporciona un servicio esencial para el mantenimiento y continuidad de actividades socioeconómicas críticas.

(2) La provisión de ese servicio depende de las redes y sistemas de información.

(3) Un incidente de seguridad interrumpiría de manera significativa la provisión del servicio esencial en cuestión.

¿Qué sectores cubre la Directiva?

La Directiva cubrirá los operadores en los siguientes sectores:

» Energía: electricidad, gas y combustibles.
» Transporte: aire, tren, y carreteras.
» Banca: instituciones crediticias.
» Infraestructuras y sedes de los mercados financieros
» Salud
» Agua: abastecimiento y distribución de agua potable.
» Infraestructura digital: proveedores de Internet, proveedores de servicio DNS, etc.

¿Qué tipo de incidentes tendrán que notificar los operadores de servicios esenciales?

La Directiva no define un umbral de lo que es un incidente significativo que requiere notificación a la autoridad nacional relevante. Define 3 parámetros que se deberían considerar:

» Número de usuarios afectados.
» Duración del incidente.
» Extensión geográfica de dicho incidente.

Estos parámetros pueden ser aclarados mediante guías adoptadas por las autoridades nacionales competentes actuando de manera coordinada con el Grupo de Cooperación.

¿Qué son los proveedores de servicios digitales (DSPs) y qué se requiere que hagan?

Empresas importantes que proporcional servicios digitales, nombradas por la Directiva como DSPs. Se les requerirá que adopten las medidas de seguridad adecuadas y que notifiquen incidentes sustanciales a la autoridad competente.

Las medidas de seguridad cubren lo siguiente:

Prevención de riesgos: medidas técnicas y organizacionales que son apropiadas y proporcionadas al riesgo.

Asegurar la seguridad de las redes y sistemas de información: las medidas deberían asegurar un nivel de seguridad en redes y sistemas de información adecuado a los riesgos.

Gestión de incidentes: Las medidas deberían minimizar el impacto de los incidentes en los sistemas de IT que se usan para proporcionar los servicios esenciales.

Las medidas de seguridad adoptadas por los DSPs deberían también tener en cuenta algunos factores, que serán especificados por la Comisión con más detalle en un documento con tal propósito:

» Seguridad de los sistemas e instalaciones
» Gestión de incidentes.
» Gestión de continuidad del negocio
» Monitorización, auditoria y testeo.
» Cumplimiento de estándares internacionales.

¿Qué tipo de incidentes deberán notificar los DSPs?

La Directiva no define umbrales o qué constituye un incidente sustancial que requiere notificación a la autoridad nacional relevante. Define 5 parámetros que deberían ser considerados:

» Número de usuarios afectados.
» Duración del incidente.
» Extensión geográfica
» Hasta qué punto el servicio es interrumpido o afectado.
» El impacto en actividades económicas y sociales.

Estos parámetros serán más detallados por la Comisión en documentos específicos.

¿Qué servicios digitales cubre la Directiva?

» Marketplaces online – Permite a los negocios establecer tiendas

en estos sitios online para ofrecer sus productos.

» Servicios de Cloud computing.

» Motores de búsqueda.

Todas las entidades que se ajusten a estas definiciones estarán de manera automática sujetas a los requerimientos de seguridad y notificación bajo la Directiva NIS. Micro y pequeñas empresas (según definición en la Recomendación de la Comisión Europea 2003/361/EC) no están dentro del alcance de la Directiva.

¿Cómo se logrará esto de una manera progresiva en DSPs?

La Comisión generará documentación en cuanto a la implementación en lo concerniente a los requisitos de seguridad y a la obligación de los DSPs de notificar incidentes antes de cumplirse el año de la adopción de la Directiva. Los Estados Miembros no podrán imponer requisitos de notificación y seguridad más restrictivos sobre los DSPs. Además, las autoridades competentes podrán ejercer actividades de supervisión sólo cuando tengan evidencia de que un DSP no está cumpliendo con sus obligaciones bajo la Directiva.

Enlaces útiles

Network and Information Security (NIS) Directive,

http://ow.ly/pWO4302Gs10

Digital Single Market: cyber security

http://ow.ly/Pc9l302Gs5A

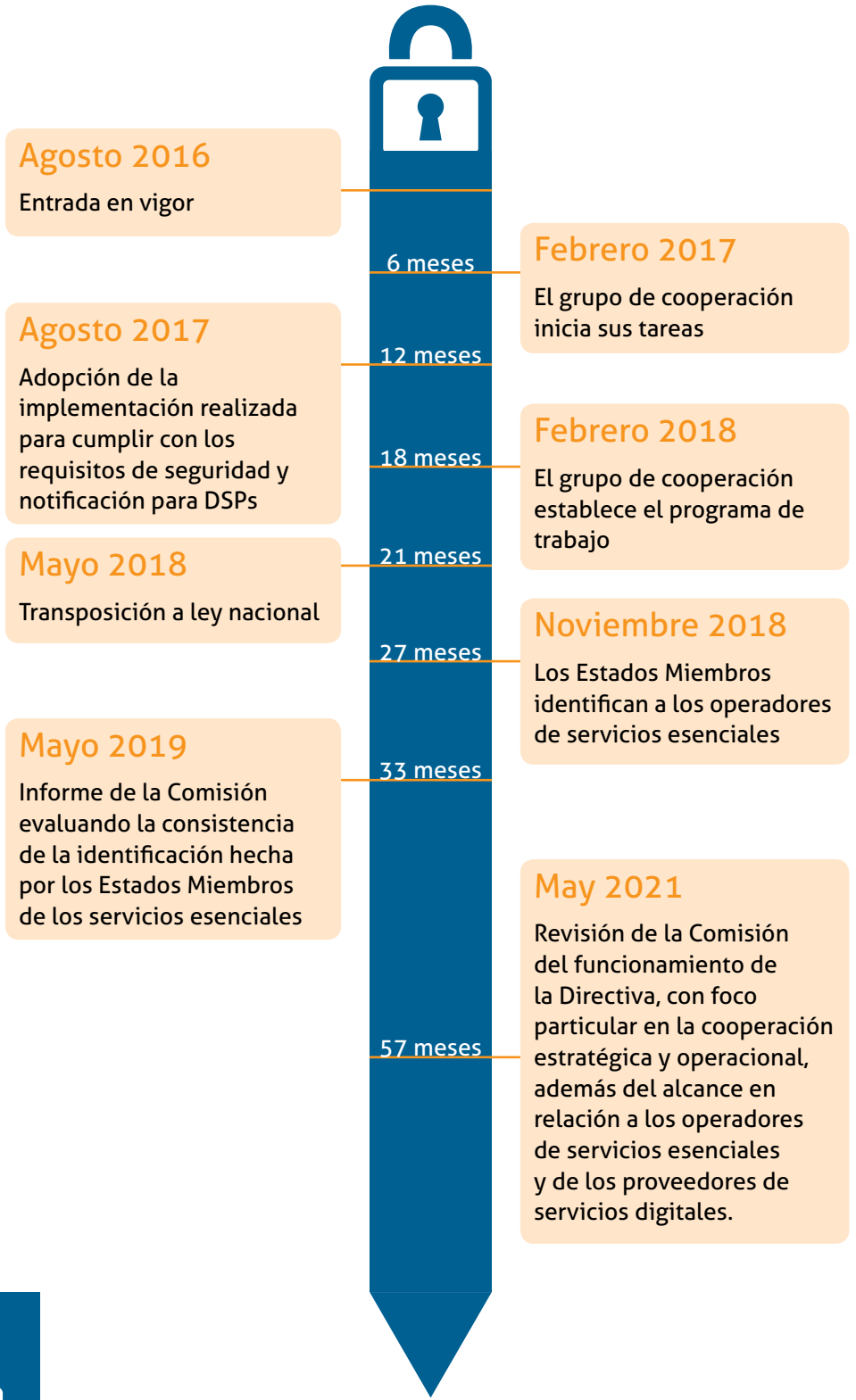
Fact Sheet on Cyber Security in EU

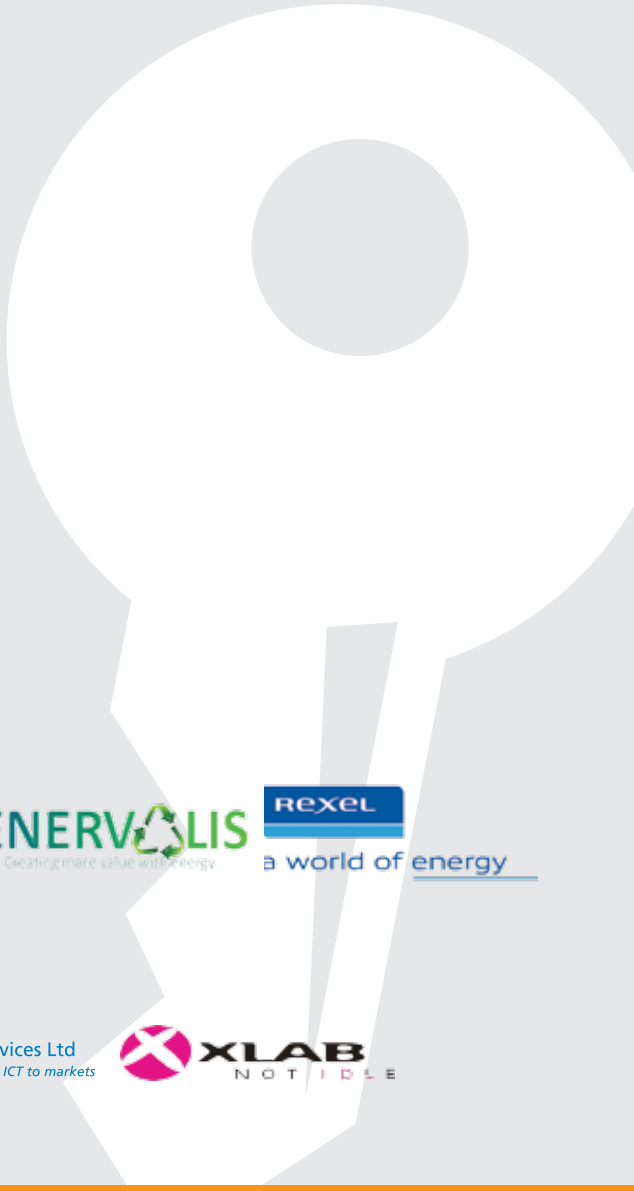
http://ow.ly/YkSJ302Gs83

EC Press Release on NIS Directive approval by EU Parliament

http://ow.ly/Z5Nk302Gsaf

¿Cuál es el calendario para la aplicación de la Directiva?





AON Atos ENERVALIS Rexel a world of energy

SINTEF Trust-IT Trust-IT Services Ltd Communicating ICT to markets XLAB NOT IDLE

Únete a la comunidad WISER para acceder gratis a CyberWISER Light

Regístrese a nuestro boletín:

Síganos en Twitter:

Conéctese en LinkedIn:

European Commission