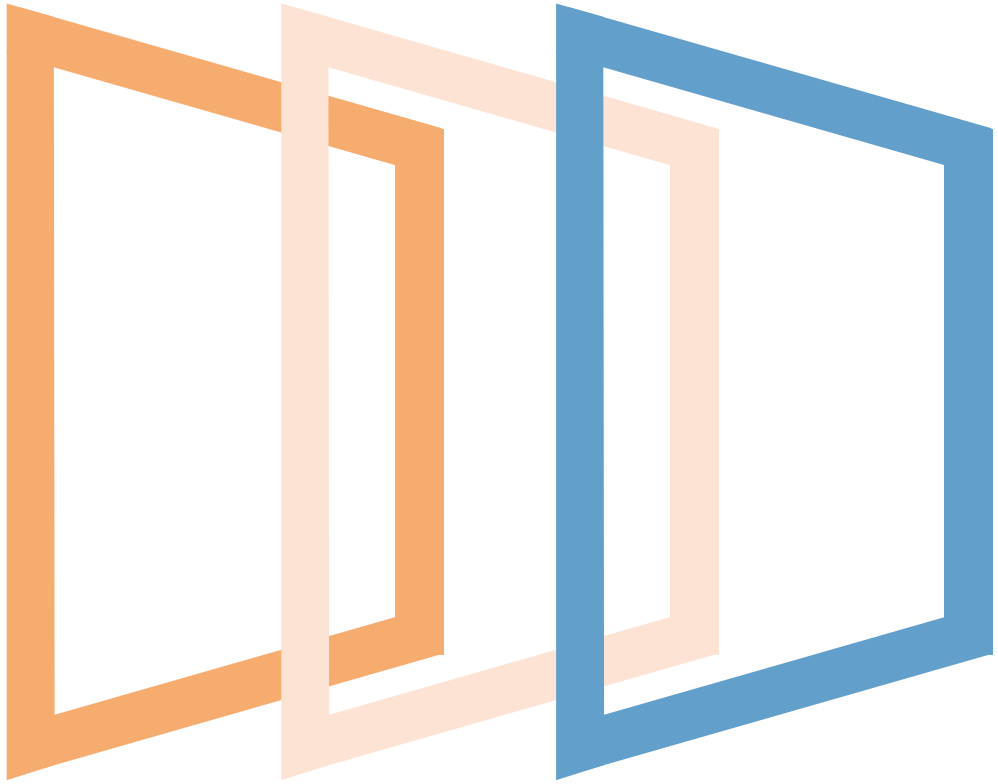
AEE
Asociación Empresarial Eólica

Implicaciones de la Directiva NIS (RD 43/2021)

Jornada Análisis Operativo Parques Eólicos

30 Septiembre 2021



Agradecimiento

Agradecemos a la Asociación Empresarial Eólica, por darnos la oportunidad de participar en la jornada de Análisis Operativo Parques Eólicos

Daniel Madrid Díaz

Resp. Global de la Práctica de Consultoría en Riesgo Tecnológico y Ciberseguridad en Minsait Business Consulting

Phone: +34 600 56 88 91

Mail: dmadrid@minsait.com

Linkedin: www.linkedin.com/in/danielmadriddiaz

¡Muchas gracias!

Minsait es uno de los players de referencia en materia de riesgo tecnológico y ciberseguridad

Más de 1.400 profesionales dedicados en exclusiva a ciberseguridad, especializados en cada una de las capacidades que componen nuestro portfolio.

Somos el partner de referencia para muchos de los fabricantes líderes de soluciones de ciberseguridad.

Además, poseemos capacidades de desarrollo propias que nos permite ofrecer soluciones diferenciales a nuestros clientes.

4 CyberDefence Centers y 9 Cyber Response Centers federados a nivel global que ofrecen capacidades escalables.

Todos nuestros procesos están certificados por los más altos estándares (ISO27001, ISO22301, ISO20000, ENS, Leet) y homologados según las mejores prácticas (CERT, TF-CSIRT, FIRST, etc.). Somos la única empresa española que intercambia ciberinteligencia con el CERT de la OTAN.

El RD 43/2021 supone el último paso de un camino que se inició hace más de diez años para proteger los servicios (e infraestructuras) esenciales frente a las amenazas de ciberseguridad

2011 Ley 8/2011 de 28 de abril de Protección de infraestructuras Críticas (**Ley PIC**)

2016 **Directiva 2016/1148**, relativa a las medidas de seguridad de las redes y sistemas de información (**Directiva NIS**)

2018 **Real Decreto-ley 12/2018** de seguridad de las redes y sistemas de información

2021 **Real Decreto 43/2021** de protección de los servicios esenciales y de los servicios digitales

El RD 43/2021 establece a los sujetos obligados requisitos en cuatro ámbitos principales

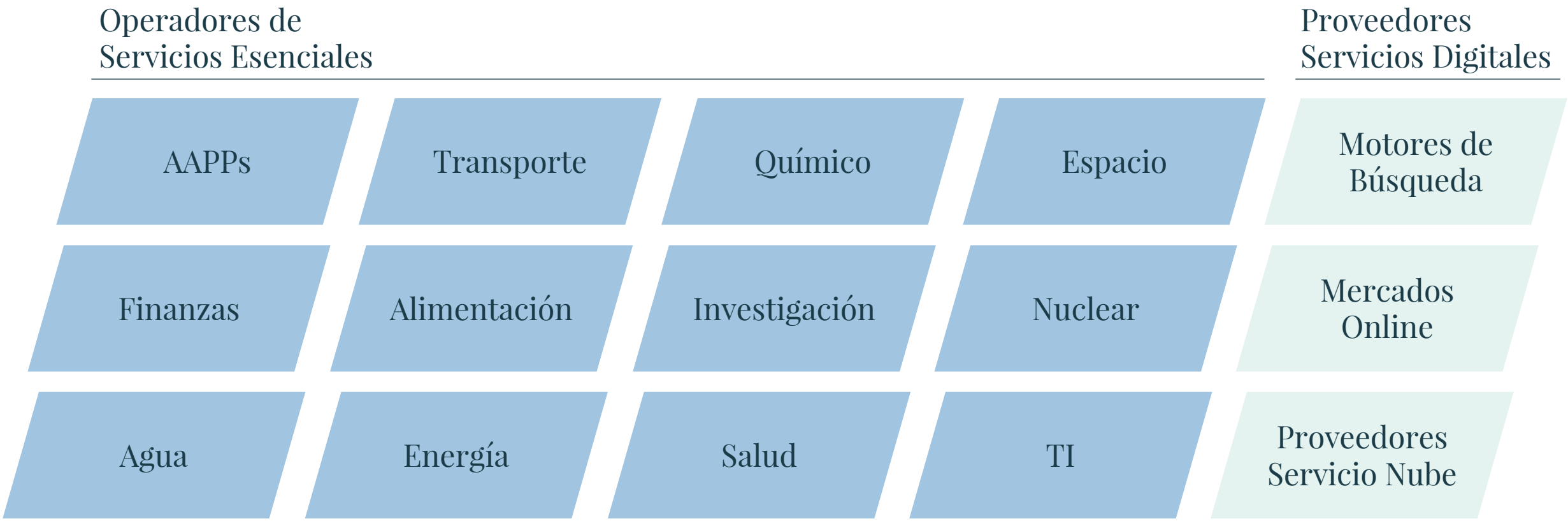
- Elaboración Marco Normativo de Ciberseguridad.
- Supervisión de la implantación de las medidas de seguridad.
- Enlace con las autoridades competentes.
- Independiente y cualficado.

- Taxonomía de Incidentes de ciberseguridad
- Guía para la determinación de umbrales de notificación
- Plataforma nacional de notificación de incidentes

- Políticas de Ciberegurdidad.
- Declaración aplicabilidad.
- Marco de Referencias Principal: ENS

- Auditoría Externa Independiente

A la hora de valorar su aplicación, los operadores de parques eólicos deben entender adecuadamente el ámbito de aplicación del RD 43/2021…



En la actualidad, los operadores de servicios esenciales son los operadores críticos ya designados de acuerdo a la Ley PIC.

… y recordar que el regulatorio es simplemente uno de los principales drivers a la hora de adoptar un modelo de ciberseguridad

A la hora de valorar el nivel de riesgo intrínseco de este tipo de instalaciones, recomendamos considerar tres variables clave

Motivación

Más allá de la amenaza del cibercrimen y los ataques de ransomware a los que está expuesta cualquier tipo de organizaciones, el sector energético puede ser potencial objetivo de otro tipo de amenazas más avanzadas de origen geopolítico.

Exposición

La juventud de este tipo de instalaciones y la complejidad del ecosistema que las conforma incrementa el nivel de exposición de las mismas frente a las amenazas cibernéticas.

Impacto

De acuerdo al Ponemon Institute, el sector energético y de utilities es, por detrás del sector financiero, el segundo sector con mayor coste económico medio por incidente de ciberseguridad, con un impacto medio por incidente de 17,2M$.

Recomendamos que la ciberseguridad debe ser considerada como un elemento más a la hora de diseñar el modelo operativo de cualquier instalación eólica

1. Ser proactivos a la hora de considerar los riesgos de ciberseguridad
2. Aplicar el principio de "Security by Design"
3. Considerar todas las palancas de ciberseguridad: personas, procesos y tecnología
4. Considerar los diferentes marcos de referencia disponibles (incluyendo la regulación)

¡Gracias!