Secure&IT by LKS Next

www.secureit.es

Centro de Ciberseguridad Industrial

Sección Española

MARCO DE CERTIFICACIÓN SEC-ICSF:2021 DE CIBERSEGURIDAD INDUSTRIAL - ENERGÍA EÓLICA -

AEE Asociación Empresarial Eólica

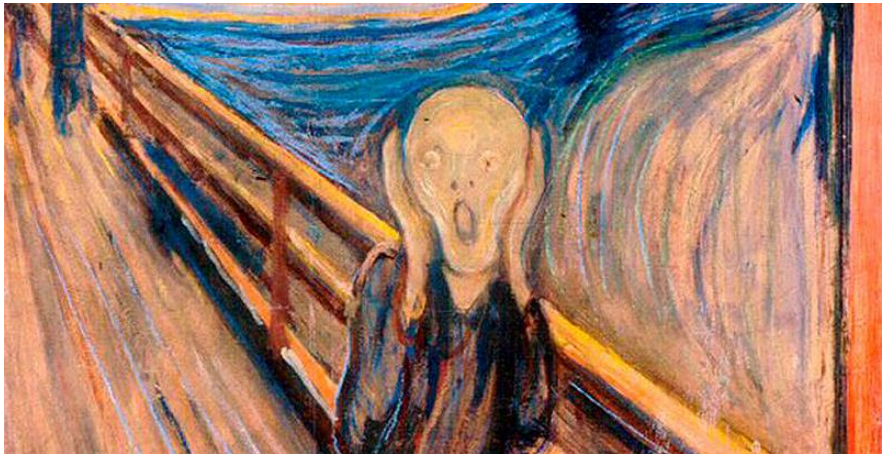
Hugo Llanos
Director Área Ciberseguridad Industrial
688 809 702 – hugo.llanos@secureit.es

Retos frente a la ciberseguridad

- Antigüedad del parque de instalaciones eólicas, sin ciberseguridad desde el diseño.
- Uso de (múltiples) protocolos industriales, generalmente no seguros.
- Importante dependencia de los accesos remotos vía inalámbrica, redes 4G, etc., especialmente en parques off-shore.
- Posibilidad de movimientos laterales hacia redes de control debido a carencias de medidas (efectivas) de seguridad.
- Aumento notable de ataques en el sector de la energía, incluyendo la eólica.
- Sin un marco de controles de seguridad de referencia.

Panorama normativo

- Contexto normativo variado: estándares (ISA/IEC 62443, NERC), requisitos específicos por propietario de las instalaciones, etc.
- Normas complejas y, en ocasiones, ambiguas
- Controles en función de determinados niveles de seguridad
- Número muy elevado de controles de seguridad
- Normas dependientes del rol en el proceso
- Procesos de certificación largos, complejos y caros



Reflexiones

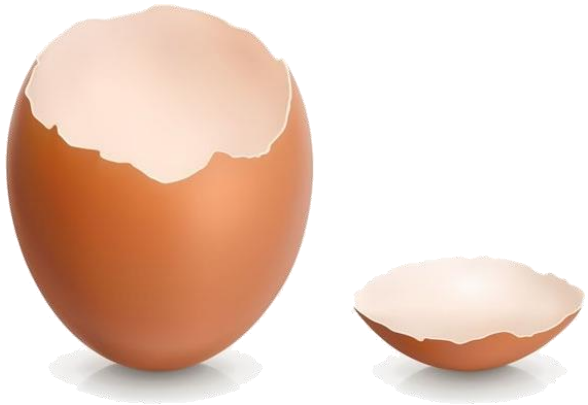
- & Los marcos actuales parecen destinados a grandes empresas con recursos disponibles para la función de ciberseguridad
- & Las empresas requieren marcos normativos alcanzables
- & Un conjunto reducido de controles eficaces reducen el riesgo en una parte muy importante
- & El estado de excelencia en ciberseguridad no evita la posibilidad de sufrir un incidente
- & Se empiezan a reclamar “garantías” en ciberseguridad, tanto en IT como en OT

La creación de una norma

¿Y por qué no definimos un conjunto de controles de ciberseguridad para el entorno industrial que se ajusten realmente a un nivel de seguridad adecuado?

¿Y por qué no los convertimos en una norma certificable por un tercero?

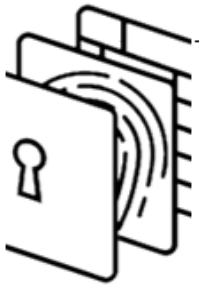
SEC-ICSF:2021



SEC-ICSF:2021 proporciona un marco normativo de ciberseguridad industrial factible, orientado a todo tipo de empresas con independencia de su actividad y tamaño, que permite alcanzar un nivel de riesgo adecuado con un número de controles mínimo, y que permite emitir una certificación por una entidad reconocida.

Principales características SEC-ICSF:2021

Seguridad para sistemas de control industrial



Marco de controles fundamentales

Reconocimiento de la adecuada aplicación de la norma

Controles industriales complementarios para ampliación de SGSI basado en 27001

SEGURIDAD DEL PROCESO INDUSTRIAL

UN ÚNICO NIVEL DE SEGURIDAD

CERTIFICACIÓN EMITIDA POR ENTIDAD RECONOCIDA

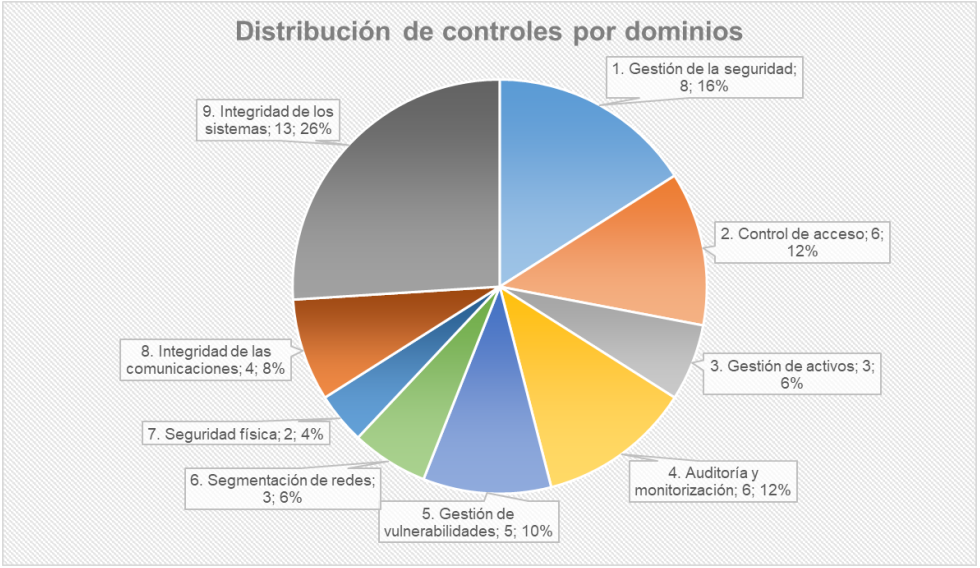
SGSI + SGCI

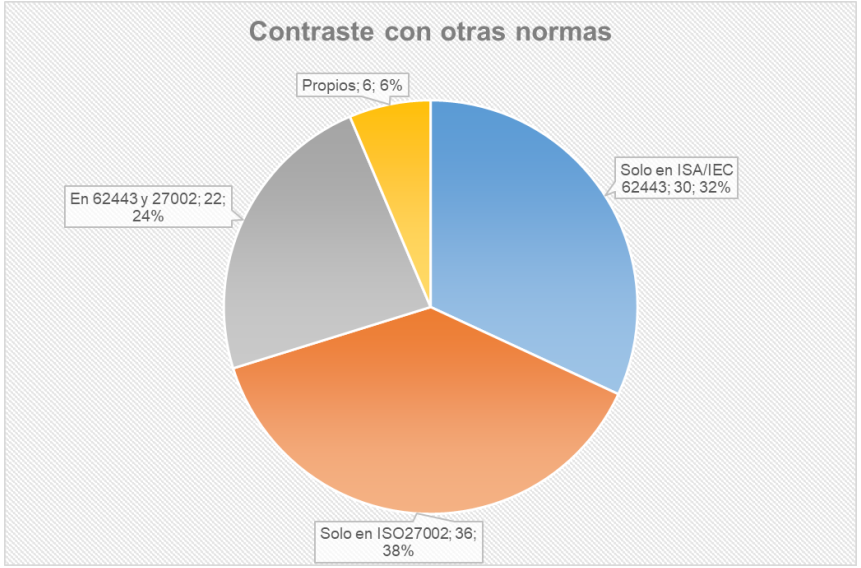
Conjunto de controles

Controles definidos en base a la experiencia de los consultores de ciberseguridad industrial de **Secure&IT**

Conjunto de **50 controles** (v1.0) divididos en 9 dominios de seguridad

Alineados con determinados SR de la 62443, ISO27002 y Centro de Ciberseguridad Industrial





Controles (I)

1. Gestión de la seguridad	Roles y responsabilidades
	Evaluación de Riesgos
	Requisitos de seguridad para nuevos sistemas
	Seguridad durante intervenciones
	Verificación de requisitos de seguridad
	Continuidad de negocio
	Indicadores de seguridad
	Formación y concienciación

2. Control de acceso	Gestión de cuentas
	Autenticación
	Contraseñas
	Protección de accesos
	Autorización
	Acceso a interfaces de administración

3. Gestión de activos	Gestión de inventario
	Sincronización horaria
	Dispositivos no autorizados

4. Auditoría y monitorización	Registros de auditoría
	Centralización de registros de auditoría
	Acceso a los registros de auditoría
	Protección de la información de auditoría
	Monitorización continua
	Gestión de incidencias

5. Gestión de vulnerabilidades	Bastionado de activos
	Identificación de vulnerabilidades
	Suscripción a feeds de seguridad
	Remediación de vulnerabilidades
	Virtual-Patching

6. Segmentación de redes	Separación de entornos IT y OT
	Segmentación de redes OT
	Protección de límites de zonas OT

7. Seguridad física	Control de acceso físico
	Soporte para entornos hostiles

8. Integridad de las comunicaciones	Integridad y confidencialidad de las comunicaciones
	Protocolos seguros
	Accesos remotos y por terceros
	Redes inalámbricas

9. Integridad de los sistemas	Protección contra código malicioso
	Privilegios de ejecución
	Comunicaciones personales
	Integridad del software y de la información
	Gestión de cambios
	Confidencialidad de la información
	Dispositivos removibles
	Intervenciones in-situ por terceros
	Gestión de recursos
	Gestión de errores
	Protección Denegación de Servicio (DoS)
	Copias de seguridad
	Criptografía

Controles críticos

Controles (II)

Cada control de seguridad se estructura de la siguiente forma:

Descripción

Definición del objetivo perseguido con la implantación del control de seguridad.

Tipo de control

Si el control se refiere a una práctica ligada al ámbito organizativo, procedimental o técnico.

Guía de implantación

Proporciona información que orienta en la puesta en marcha del control y, por lo tanto, alcanzar los objetivos perseguidos por el mismo. En este sentido es necesario detallar que, en ocasiones, es posible alcanzar un mismo objetivo de diferentes formas, por lo que lo detallado en esta norma no debe ser interpretado como la única solución posible.

Controles (II)

Información adicional

Apartado de aparición opcional en cada control de seguridad que proporciona, en el caso de que exista, información adicional de interés sobre el control de seguridad.

Se presenta a modo de orientación para la comprensión o clarificación del requisito correspondiente.

Un ejemplo

5. Gestión de vulnerabilidades: Virtual-Patching

Descripción

En aquellos sistemas o elementos en los que no sea posible llevar a cabo actualizaciones, proceder con la puesta en marcha de medidas compensatorias que disminuyan el grado de exposición en la red de los mismos. En este caso se podrá optar al despliegue de soluciones en modelos distintos como el filtrado de las comunicaciones dentro de la misma zona, subred o ámbito de operación.

Tipo de control

Técnico

Guía de implementación

Dado que en ocasiones no es posible implementar medidas de seguridad nativas en los equipos finales afectados por vulnerabilidades (pérdida de garantías con fabricantes/integradores, incompatibilidades, etc.), es necesario implementar medidas compensatorias en la red, como por ejemplo la protección de los equipos a través de cortafuegos que limiten los accesos a los equipos finales tanto en capa 4 (restricción de acceso por IP/puerto origen/destino) como en capa 7 (limitación de funcionalidades a nivel de aplicación) del modelo OSI o agrupación en segmentos de red distintos de un menor número de equipos.

Información adicional

Hay que considerar que añadir más elementos de seguridad en la red implica un aumento de las tareas de gestión relacionadas con los mismos. Esta medida debería implementarse únicamente cuando no sea viable la aplicación de medidas opcionales.

El uso de cortafuegos de manera tradicional requiere de la asignación de direccionamientos de distintas redes o subredes. La inclusión de estos equipos para proteger un número reducido de ellos podría suponer cambios de direccionamiento, algo inviable según escenarios. Por ello, se puede adoptar el uso de estos equipos en Capa 2 (interconexión de los equipos de seguridad que actúan a modo de pasarela transparente del tráfico, pero manteniendo las funcionalidades de filtrado y análisis del tráfico que los atraviesan) del modelo de referencia OSI, filtrando el tráfico en la misma red o subred.

Opciones de implantación

Dos posibilidades para la implantación:

1) Como un **marco independiente**:
   - & Adecuado para empresas que no han desplegado un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO27001
   - & Permite una gestión ordenada de la función de seguridad en el entorno industrial
   - & **¡OJO!** Importante interoperabilidad con el entorno IT

2) Como un conjunto de controles que **amplían el alcance de un SGSI** con el entorno puramente industrial (SGCI)
   - & Algunos controles del dominio 1 relacionado con la gestión de la seguridad ya estarían desplegados, solo es necesario ampliar alcance
   - & Sistema único IT+OT e integrado

Certificación Ciberseguridad de instalación eólica

Datos

- Evaluación de la ciberseguridad del parque eólico y de los sistemas de control.
- Aseguramiento de las comunicaciones entre los parques y los centros de control.
- Establecimiento de unas bases mínimas de ciberseguridad en el conjunto.

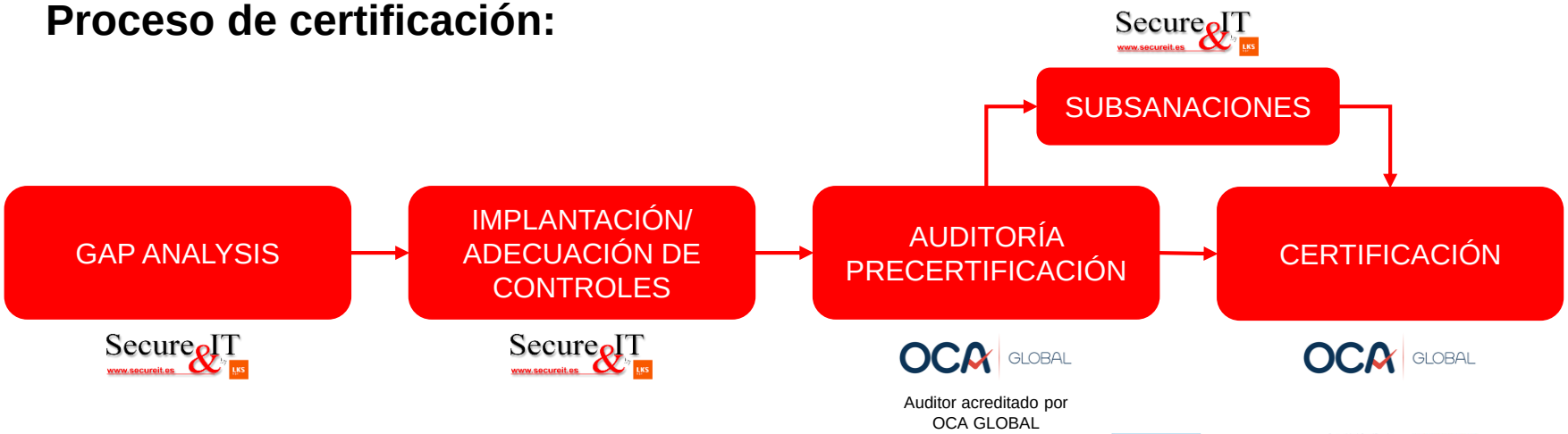
Personalización de SEC-ICSF:2021 al contexto y "lenguaje" específico del sector de la energía eólica

Certificación

SEC-ICSF:2021 es una norma privada desarrollada por **Secure&IT**, reconocida y certificable en exclusiva por la empresa OCA GLOBAL

Permite obtener una certificación a tres niveles (Alto, Medio y Bajo), en función de la puntuación total obtenida conforme al grado de implantación de cada uno de los controles de seguridad

Proceso de certificación:



OCA GLOBAL

"Posiblemente, la compañía de ensayos, inspección y certificación con **mayor crecimiento orgánico en el mundo**."

OCA Global, es una compañía de capital privado, con sede en España, que emplea a más de 2.000 personas y cuenta con más de 30 años de experiencia en la industria. Ofrece una amplia gama de servicios para todo tipo de industrias, sectores y empresas.

OCA Global está acreditada en ISO 17020, 17025 y 17021 para múltiples estándares y es reconocida mundialmente por ILAC (*International Laboratory Accreditation Cooperation*) e IAF *(International Accreditation Forum).*

La empresa fue fundada en 2010 con el objetivo de consolidarse como la organización de inspección y certificación de referencia del siglo XXI, así como una alternativa a las compañías tradicionales del sector.