“Este año superaremos los 1.750 incidentes de ciberseguridad en el sector energético”

Ponferrada alberga el próximo 5 de julio un evento organizado por INCIBE, CIUDEN, en colaboración con ISMS Forum, para analizar los retos de ciberseguridad en el sector energético

El Consejo de Administración del Instituto Nacional de Ciberseguridad (INCIBE), nombraba a Félix Antonio Barrio Juárez nuevo director general de la entidad hace ahora un año.

Félix Antonio Barrio Juárez es gerente de Ciberseguridad CISM por ISACA. Ha sido miembro del Board of Directors de la European Cyber Security Organization (ECSO), y presidente del Subcomité de Tecnologías de Ciberseguridad-UNE.

¿Qué objetivos pretende cubrir este evento que organiza INCIBE, CIUDEN e ISMS Forum sobre ciberseguridad en infraestructuras críticas?

En el marco de nuestra actividad festival por excelencia que es el *Cybersecurity Summer BootCamp* donde se van incorporando cada vez más países, llevamos mucho tiempo pensando en crear una actividad propia.

A tal efecto, ha surgido esta iniciativa en un sector tan estratégico y crítico como es el energético. Crítico porque es el que genera mayor número de incidentes que gestionamos, distribuyendo esos incidentes en cuanto a infraestructuras críticas respecto del resto de sectores estratégicos.

Al mismo tiempo en España, como ventana de oportunidad, tenemos mucho recorrido y hay un alto nivel de excelencia en el sector energético, tanto a nivel de profesionales, en cuanto a equipos rectores, CISO y entidades, como ISMS Forum, entidad líder en la configuración de este tipo de desarrollo de capacidades directivas.

Uno de los principales objetivos era juntar a INCIBE, con la OEA (Organización de Estados Americanos) para organizar un evento en el que ISMS Forum, con su liderazgo, podamos establecer una jornada para analizar cuáles son las coyunturas y necesidades, con propuestas

que nos ayuden a avanzar en el llamado liderazgo técnico.

La jornada tiene un programa ambicioso en una infraestructura con pruebas energéticas que reproduce una central eléctrica real en funcionamiento. Dicha infraestructura solo puede encontrarse en EE.UU., algo similar en los llamados laboratorios federales.

Al final, el objetivo que planteamos es el poder analizar cómo podemos establecer un programa que nos permita unir formación teórica y práctica en ciberseguridad industrial a la altura de estos cambios que estamos teniendo.

¿Cuáles son los retos que se plantean en política de ciberseguridad en la protección de los sectores estratégicos como el energético de un país como el nuestro?

En primer lugar, hay que mencionar que la Directiva NIS2, la cual nos va a suponer un estrés importante en cuanto al desarrollo y ejecución de las políticas de ciberseguridad en España.

El pasado 30 de marzo, el Consejo de Administración de INCIBE aprobaba la creación de ocho departamentos de ciberseguridad para diferentes sectores estratégicos, siempre el primero de ellos el de la industria energética.

Precisamente, se creó dicho departamento ante las previsiones de que este año podremos superar los 1.570 incidentes que ya gestionamos en el sector energético en el último año y que precisamente se trata también de abordar todos los retos en cuanto a la adecuación a las diferentes directivas que van a incidir en esa reconfiguración de los sistemas de respuesta a incidentes de ciberseguridad sectoriales.

Hay que recordar que este es el año de las directivas de radiofrecuencia, de la nueva directiva de Marcado C que va a afectar a la importación de cualquier producto conectado y que influirá en la

IOT industrial.

Son muchos los ámbitos normativos que requieren una revisión exhaustiva por parte de los responsables públicos y privados de un sector como es el energético. Esto tiene que provocar una involucración activa de la comunidad profesional representada por ISMS Forum, pero también de las empresas y de toda la cadena de suministro que es el eslabón más débil en relación a la respuesta a incidentes y ciberamenazas.

Desde esta perspectiva es importante este evento, que nos va a permitir reunir todos estos expertos y habilitar un espacio especialmente centrado en el análisis de estos cambios normativos.

¿Cómo encaja nuestra política de ciberseguridad en relación con la estrategia de la UE para una energía segura, competitiva y sostenible?

Todavía no sabemos cuáles van a ser las líneas finales que vamos a tener en materia de reconfiguración de la gestión de riesgos, que es la palabra clave en materia de política normativa en la regulación del sector, pero sí tenemos claro las líneas maestras.

A este respecto hay que interpretar que le dediquemos en esta jornada, y a la propuesta de ISMS Forum, la aprobación de una Declaración sobre sostenibilidad porque la resiliencia del sistema no tiene solo en cuenta el riesgo tecnológico desde el punto de vista de los parámetros que tiene la configuración de los sistemas, físicos, híbridos y digitales de ciberseguridad, sino que también tiene en cuenta la disponibilidad de un sistema que se ve condicionado por elementos de coyuntura de mercado. En este contexto, la sostenibilidad energética se ha revelado como un elemento central.

Desde esta perspectiva, debemos ser capaces de establecer estrategias a medio y largo plazo que nos permitan tener esa suficiencia para generar la energía necesaria a medida que se vaya necesitando y en el lugar que sea preciso.

En mi opinión, este tipo de principios rectores surgen y se avanzan más rápido en ellos si encontramos ese tipo de escenarios públicos y privados de reflexión y de análisis.

En esta jornada se va a firmar un Manifiesto por una Ciberseguridad Sostenible, ¿qué líneas básicas va a contener este manifiesto?

Estamos hablando de un manifiesto para la sociedad y para la economía y una iniciativa en la que nosotros como INCIBE vamos a adherirnos con entusiasmo.

En segundo lugar, la perspectiva es la de un manifiesto que pretende involucrar toda la cadena de valor y esto es muy importante permitiendo así que el proyecto tenga una dimensión mayor y global, trascendiendo así las fronteras.

Desde mi punto de vista, creo que es una propuesta audaz en tiempos de incertidumbre. Al final, este documento debe formar parte de las guías de actuación y estrategias corporativas de las empresas. También debe ser un elemento clave de nuestra Estrategia Nacional de Ciberseguridad.

Al mismo tiempo no debemos restringirnos exclusivamente a los ámbitos de la ciberseguridad, sino que también una dependencia tecnológica del concepto de gestión eficiente de la energía desde el punto de vista de la producción y del consumo. Son elementos esenciales en estos momentos.

Estoy convencido que este primer encuentro, el primero de muchos, abre una vía importante.

Una de las mesas redondas va a abordar los retos que se plantean en materia de regulación de la ciberseguridad y buenas prácticas, ¿cómo hay que entender dicho marco normativo?

En estos momentos hay dos elementos prioritarios en un contexto con tanta incertidumbre donde crear este evento es un espacio de diálogo y reflexión sobre esta problemática.

Uno de esos elementos consecuentes es el desarrollo de un marco de certificación, homologación de productos y proveedores en el ámbito de la ciberseguridad dentro del mercado interior europeo.

Ahora hay que clarificar muy bien que la infraestructura privada a través de las entidades de certificación y de homologación, establece al sistema europeo crítico.

Se trata de que todos esos sistemas se aborden en nuestro país desde una óptica que permita ayudar a toda la cadena de proveedores y clientes de la industria para que tenga un sistema de respaldo de confianza, pero también no suponga barreras para la entrada de nuevos operadores y sobre todo para pequeñas y medianas empresas.

Un dato muy importante surgió en el marco del debate que tuvo lugar el pasado mes de noviembre en el Parlamento Europeo respeto al impacto de la directiva NIS2 y que se preveía que se podría necesitar entre 150.000 y 170.000 nuevas pymes en Europa de ciberseguridad para poder dar respuesta a todas las necesidades que vamos a tener desde el punto de vista de soporte a empresas y ciudadanos en materia de ciberseguridad.

Habrá que ver cómo afecta esta situación al sector energético y cómo las regulaciones deben servir para llegar a este objetivo. Al mismo tiempo, esas regulaciones sean una palanca de apoyo y no una barrera, es decir, que sea una normativa eficaz para que ayude a la gestión eficiente de la ciberseguridad.

Es un proceso en el que ya se está trabajando y que requiere la concurrencia de las personas que trabajan en esto, de ahí que el debate de esta mesa redonda sea esencial.

Otro elemento a destacar es la definición de las metodologías de evaluación de riesgo. En este caso hay incertidumbres sobre todo en el ámbito de la 5G y que es muy importante que veamos cómo podemos avanzar deprisa para evitar los riesgos asociados a la invasión de dispositivos que estarán conectados, sobre todo del Internet de las cosas a nivel industrial y que puedan estar en riesgo de no estar a un nivel suficiente de protección en un marco en el que todo el impacto de las nuevas redes de comunicación, y en particular del 5G, van a tener importancia en nuestros sectores.

En esta mesa redonda se abordará, desde un punto de vista práctico, las regulaciones tanto en el ámbito de EE.UU. con las particularidades que tendrá el modelo europeo, como el papel que España está desarrollando.