CIBERSEGURIDAD A LARGO PLAZO

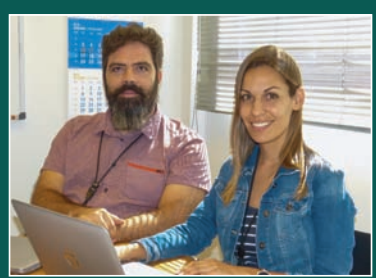
La industria nuclear ha sido históricamente un referente tecnológico. Los componentes digitales implicados en los procesos de una instalación nuclear como Vandellós II, contaron en su diseño con un nivel de seguridad intrínseco a la industria de forma que sus funciones se evalúan con criterios de seguridad nuclear y, por tanto, cumplen requisitos específicos según sean clasificados como *Clase Nuclear 1E* o *Relevantes para la Seguridad*. Indudablemente, el marco de seguridad nuclear es robusto y se sustenta en la Defensa en Profundidad por diseño, basada en la separación de sistemas de seguridad y no seguridad, la redundancia de trenes y el control de acceso.

EL CISNE NEGRO

Según el ensayista e investigador Nassim Nicholas Taleb, la industria y la sociedad en general se mueven al ritmo de lo que denomina *cisne negro* en su libro homónimo, dicho de otro modo, un suceso altamente improbable pero de gran impacto. Estos sucesos raros pero de gran transcendencia, ocurren por sorpresa y en su análisis posterior muestran que todos los datos estaban ahí, solo que arrinconados por los analistas en sus campanas de Gauss por ser de probabilidad despreciable. Los hay de naturaleza positiva como la aparición de internet, la penicilina, etc. y negativa, como las grandes guerras, atentados, desastres naturales y demás (Figura 1).

El gran *cisne negro* que supuso el punto de inflexión en la seguridad y por ende en la ciberseguridad de la historia reciente, fueron los ataques terroristas en Nueva York el 11 de septiembre de 2001. El mundo se percató de que los paradigmas de la seguridad como se conocían en ese momento estaban incompletos. A partir de entonces, la inteligencia norteamericana se dedicó a detectar nuevas amenazas que pusieran en riesgo la seguridad nacional.

Diez años después de los atentados de Nueva York, un nuevo *cisne negro* sacude de una forma terrible a la industria nuclear. El accidente de Fukushima Daiichi el 11 de marzo de 2011, pone de manifiesto la necesi-



MARIAN MORÁN

(CISO de ANAV).

Jefa de Sistemas de Información y Comunicaciones.

Ingeniera superior en Telecomunicaciones, se incorporó a ANAV en el año 2010 como ingeniera de planta en CN Ascó.

ÓSCAR FERNÁNDEZ

(CISO suplente de ANAV).

Técnico de explotación de Ciberseguridad y bases de datos.

Ingeniero técnico en Informática de Gestión. Se incorporó a ANAV en el año 2009 como técnico de explotación de bases de datos.

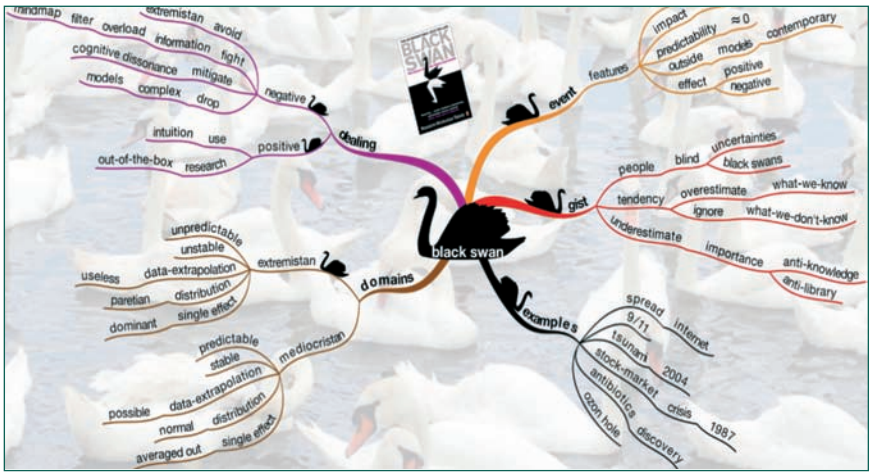


Figura 1. El cisne negro.

dad del refuerzo de ciertos sistemas de salvaguardias, añadiendo equipos portátiles de última generación, y también el refuerzo de las comunicaciones tanto internas como con el exterior. Aunque las comunicaciones de emergencia ya estaban consideradas en el Programa de Ciberseguridad, se puso gran esfuerzo en dotar a la organización de nuevas alternativas de comunicación, diseñadas de la forma más segura posible y con alto grado de disponibilidad.

CIBERSEGURIDAD NUCLEAR

Una de las áreas de actuación en la búsqueda de nuevas amenazas fue la industria nuclear. En consecuencia, la NRC ha actualizado la amenaza base de diseño en instalaciones nucleares, realizando modificaciones sustanciales en todos los ámbitos, y de forma particular, en 2007, incluye el ataque cibernético en la amenaza base de diseño en el 10 CFR 73.1. En la Figura 2, presentada por Mario R. Fernández Jr. de la NRC, se puede ver la cronología.

Dos años más tarde, en 2009, la NRC publica la 10 CFR 73.54, en la cual se exige un Plan de Ciberseguridad a las centrales nucleares estadounidenses. Se hace pública la guía para implantar la regulación de la seguridad informática para centrales nucleares RG 5.71 y se añade un conjunto de documentos del NEI específicos. Es en ese momento cuando Vandellós II y el resto de plantas españolas toman la determinación voluntaria de adoptar una metodología formal basada en la normativa americana para protegerse de las amenazas cibernéticas, y de esta forma complementar la estrategia de seguridad. Ello sin perder de vista las premisas de aislamiento y control de acceso fehaciente a los sistemas de seguridad nuclear y de seguridad física que marca el CSN en el condicionado de 2012 y en concordancia con las recomendaciones que el OIEA incluye en la revisión 5 del documento INFCIRC-225.

En la misión de operar C.N. Vandellós II de forma segura, fiable y a largo plazo, la ciberseguridad es entendida como parte de la seguridad integral de la organización y cuenta, entre los puntos clave, no solo con medidas técnicas avanzadas, si no que pretende que la ciberseguridad forme parte de la Cultura de Seguridad de la organización. Este es el motivo por el cual uno de los pilares fundamentales del Programa de Ciberseguridad es la concienciación y la formación a todos los niveles. Tal como confirma Cruz Cirauqui, director de Servicios Técnicos de ANAV, "los profesionales nucleares nos caracterizamos esencialmente por nuestro compromiso con la seguridad, así que debemos interiorizar los requisitos de ciberseguridad, hacerlos nuestros como en el pasado hemos introducido otros, e incorporarlos en la planificación de nuestros trabajos".

Paralelamente, se define un Plan de Ciberseguridad para los sistemas de información y comunicaciones corporativas (Plan ICT), que consiste en un proceso de mejora continua basado en la gestión del riesgo. El Plan ICT se integra en el Programa de Ciberseguridad general, y por tanto todos los activos digitales, tanto los relacionados con los procesos de planta (Zona OT) como los de gestión corporativa (Zona IT), cuentan con gestión de la ciberseguridad.

CIBERSEGURIDAD IT-OT

Disponemos, por tanto, de un plan para proteger todos los activos digitales de la instalación, ya sean del tipo tradicionalmente llamado Tecnologías de Información (IT), o del tipo Tecnologías de la Operación (OT). Además, hay que hacer un verdadero esfuerzo para asimilar que la tecnología se está unificando, concepto denominado *Convergencia IT-OT* o *Convergencia IP*. No hay que entender este concepto como la unión IT-OT, pues la segmentación de redes, niveles, diversidad de fabricantes y el resto de controles de ciberseguridad se deben seguir cumpliendo.

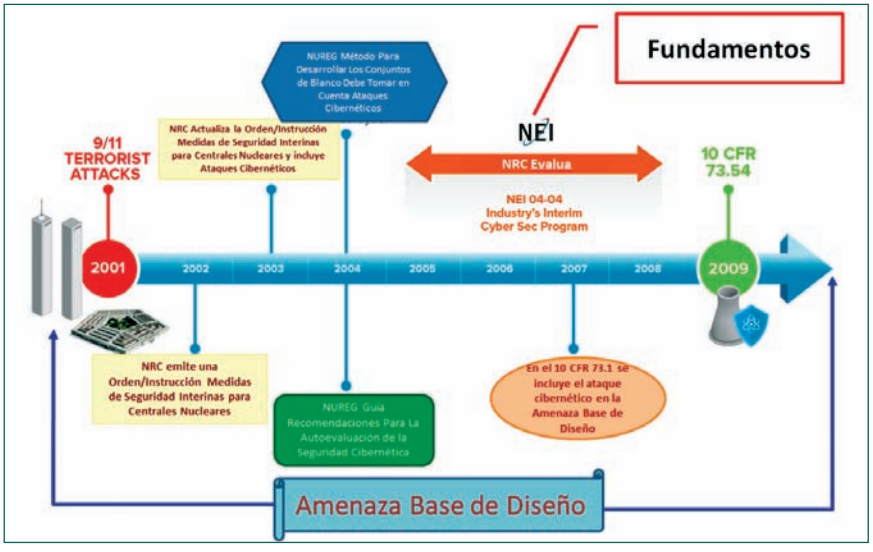


Figura 2.

Figura 3.

Esta convergencia tiene grandes dificultades, comenzando por la propia naturaleza de las prioridades de la ciberseguridad. Mientras que en el mundo IT siempre ha tenido un gran peso específico la confidencialidad, entendida como el acceso no autorizado a los sistemas, en el mundo OT prima la garantía de disponibilidad del sistema. Obsérvese el esquema del experto Joan Figueras Tugas que ilustra esta situación (Figura 3).

En sus inicios, las tecnologías IT y OT eran completamente distintas (PC de mercado vs Scada con sistemas operativos propietarios). Pero inevitablemente, la industria nos arrastra a que esas diferencias sean cada vez menores, y ya podemos encontrar sistemas OT ejecutándose en plataformas virtualizadas, o por ejemplo los ordenadores de proceso de planta, que son servidores iguales a los que encontramos en los centros de cálculo corporativos, el uso de tablets rugerizadas en lugar de PDA, *firewalls*, IPS, antivirus, etc. Por tanto, este concepto no es futuro, es presente, y ha venido para quedarse.

Efectivamente, esta corriente está siendo aprovechada por los fabricantes IT para introducirse paulatinamente en el mercado OT, acuñando eslóganes como el de *Industria 4.0* o cuarta revolución industrial.

No hay que perder de vista que el entorno nuclear precisa de una toma de decisiones conservadora y es fundamental saber discernir el alcance, pues hay puntos en los que no es óptimo abordar la convergencia. Debemos orientar los esfuerzos donde la convergencia es posible, tal como se muestra en la ilustración de Gartner (Figura 4). Algunos ejemplos son las estrategias de recuperación, configuración y registro, ciberseguridad, flujos de transferencia de datos, etc., de forma que sean disciplinas unificadas que traten ciertas actividades de forma transversal en la organización.

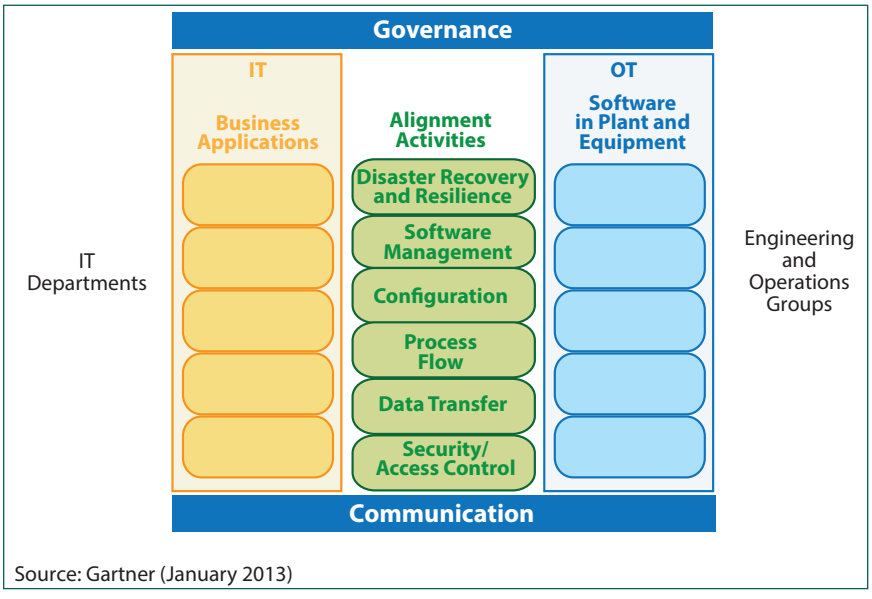


Figura 4.

A continuación se detallan unos conceptos que tarde o temprano tenemos que afrontar.

Genera respeto oír hablar de el **Internet de las cosas** o **IoT** cuando quieres proteger una instalación crítica. Pero no es descabellado conocer y valorar las ventajas que puede ofrecer una solución IT de gestión distribuida, que ya es capaz de interactuar con elementos electromecánicos, como por ejemplo, sensores, *tablets* o cámaras de vigilancia conectados a una red IP. De hecho, muchas industrias están implementando esta tecnología en un entorno OT, como es el caso de las llamadas *Smart Grid*, sin por ello quebrantar requisitos o políticas de un Plan de Seguridad, por estricto que sea, porque la tecnología se diseña y despliega de acuerdo a lo establecido en los planes.

Otro concepto es el ***Big Data***. El mundo OT dispone de historiadores con una calidad y robustez extremas para poder trabajar con los datos en tiempo real, y con una latencia muy baja, inimaginable en una red IP. La tecnología ha avanzado tanto en los últimos años, que empresas como Twitter, Instagram o Whatsapp, realizan más inserciones por segundo en sus bases de datos IT que la mayor planta del mundo introduce en su historia. Y, por supuesto, disponen de las ventajas de análisis de información de estas herramientas *Big Data* de apoyo a la toma de decisiones. No tardará en llegar el día en que esta tecnología se incorpore a los sistemas de proceso en la industria.

Pero los retos tecnológicos son solo una cara de la moneda. No menos dificultades encontramos en la convergencia entre las personas y las formas de trabajar tan diferentes que tradicionalmente tienen IT y OT.

El profesional IT, debe entender que los tiempos en OT son más lentos, los procedimientos más estrictos y profusos, y la burocracia asociada a los cambios de diseño o la configu-

Figura 5.

ración de la documentación es fundamental. Por otro lado, el personal OT, puede aprovechar la nueva tecnología para aligerar cargas de trabajo, y entender que si evoluciona la tecnología, también lo hace la forma en la que se entienden y ejecutan los procedimientos.

Debemos aprovechar lo mejor de los dos mundos, crear equipos de trabajo multidisciplinares. Como ejemplo, el equipo para la evaluación de la ciberseguridad creado en ANAV. En definitiva, como en la ilustración de Manuel Guerrero Cano (Figura 5), no es una batalla por ver quién se lleva la mayor parte del pastel, sino que el éxito radica en colaborar y buscar consensos, pues como dijo el legendario samurái Miyamoto Musashi, "existe más de un camino a la cima de la montaña".

CIBERSEGURIDAD A LARGO PLAZO

De todos estos años de trabajo en materia de ciberseguridad en Vandellós II y el resto de reactores españoles, podemos extraer una conclusión importante: el enfoque del mundo nuclear de defensa en profundidad, vectores de ataque y trabajo multidisciplinar es robusto. Y más importante aún, el hecho de que gran parte de los sistemas de protección de las plantas nucleares sean de naturaleza analógica, nos da una gran ventaja frente a otras tecnologías de producción eléctrica más modernas que cuentan en su diseño con más activos digitales en sus sistemas críticos.

Paradójicamente, ser una tecnología implantada en los años 80, hace que sea de naturaleza más cibersegura que una instalación moderna. Esta es, sin duda, una fortaleza del sector nuclear en la carrera de la transición energética frente a otras tecnologías.

Los expertos coinciden en que las centrales nucleares, operando a 60 años, representan un activo fundamental para alcanzar los actuales objetivos energéticos y medioambientales, y los aspectos de ciberseguridad refrendan sus argumentos. Pero es muy importante asumir que será necesario modernizar y digitalizar ciertos elementos en las plantas, teniendo la ciberseguridad como un pilar estratégico a largo plazo.

Para canalizar esta estrategia de ciberseguridad llega la transposición a Ley Española de la Directiva (UE) 2016/1148 de 6 de julio de 2016 del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como *Directiva NIS*. Esta puede representar un revulsivo en materia de seguridad, pues cuenta entre sus elementos clave con la creación de una ventanilla única de reporte de incidentes, no solo de ciberseguridad, sino también de aquellos del alcance de la Agencia de Protección de Datos.

Para el sector nuclear, el interlocutor de referencia será el Centro de Respuesta a Incidentes (Incibe-CERT), siendo la autoridad competente el Centro Nacional de Protección de Instalaciones Críticas (CNPIC) dependiente del Ministerio del Interior. Esto no deja de ser un impulso más a la idea de integrar los aspectos de seguridad física, ciberseguridad, seguridad de la información y seguridad industrial y a su vez hacer converger las tecnologías IT y OT.

Otro punto clave de la transposición de la NIS, es la intención por parte del Instituto Nacional de Ciberseguridad (Incibe) de aplicar un modelo común de obtención de información. Todas las infraestructuras críticas utilizarán el mismo formato, presumiblemente el ENSI_C4V y de esta forma, el Mando Conjunto de Ciberdefensa (MCCD) dispondrá de toda la información relevante de forma óptima. Para que esto sea posible, las plantas tendrán que rehacer parte de los programas de ciberseguridad, para asimilar el nuevo modelo procurando aprovechar todo lo que sea

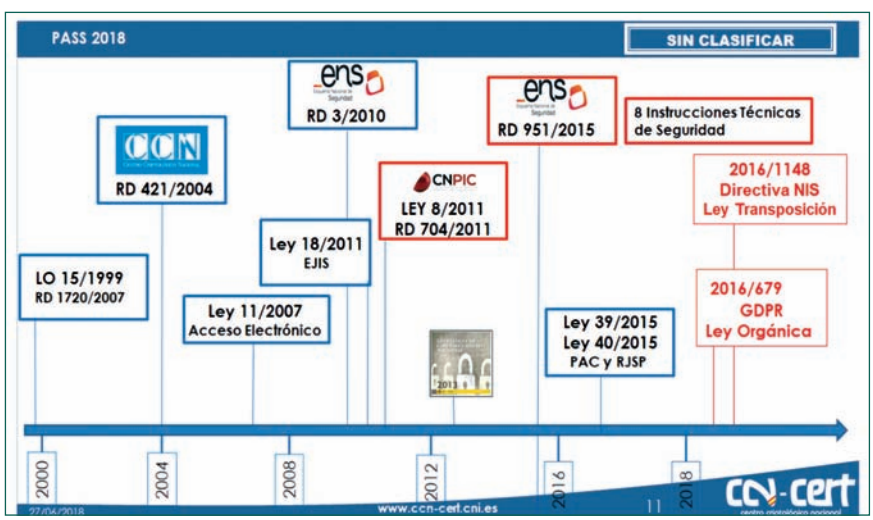


Figura 6.

de utilidad de la normativa americana y la esencia del modelo de defensa en profundidad.

No estamos en disposición de decir si esta directiva será la norma definitiva. El CSN también tiene la opción de publicar una instrucción de seguridad para regular la ciberseguridad del sector nuclear, y está en borrador el nuevo Reglamento de Seguridad Privada.

De un breve período de tiempo a esta parte, la cantidad de normativa generada en materia de ciberseguridad es abrumadora, como se observa en la infografía cedida por el Sr. Javier Candau, jefe del Departamento de Ciberseguridad del Centro Criptológico Nacional (Figura 6). Puede que la directiva NIS sea la culminación de los esfuerzos de modernización tecnológica y ciberseguridad desde 2001, sobre todo si se materializa la iniciativa propuesta desde el CCN de crear una ventanilla única para la comunicación de ciberincidentes.

CONCLUSIÓN

La ciberseguridad es un campo de la técnica inacabable, y más si cabe en una infraestructura como la de Vandellós II, donde la experiencia operativa tiene tanto peso y los incidentes en otros sectores empiezan a aumentar en frecuencia y repercusión.

Hoy en día, es muy fácil lanzar un ataque por mecanismos cibernéticos, y este puede ser perpetrado por fuerzas que ni siquiera tienen por qué estar localizadas en el mismo país. Las normativas evolucionan constantemente y no tenemos un horizonte claro que justifique el retorno de la inversión. No existen herramientas milagrosas, y no hay una única tecnología que cubra todas las necesidades de securización, ni en el mundo IT ni tampoco para el mundo OT. Mucho menos aún existe una fórmula magistral para aunar esfuerzos entre ambos mundos, esto sólo se consigue mediante colaboración y objetivos comunes.

Es por todo ello que, año a año, se incrementan los esfuerzos en materia de ciberseguridad, tanto por parte de los organismos oficiales, como de los propietarios y los profesionales nucleares. Después de ocho años de trabajo en ciberseguridad, Vandellós II ofrece una protección y una capacidad de detección de amenazas que va más allá de los requisitos legales y lo exigido por los reguladores CSN y CNPIC, lo que hace que ANAV se sienta optimista ante un futuro cada vez más exigente.

Ante este escenario de batalla continua, el enfoque nuclear de defensa en profundidad, vectores de ataque y trabajo multidisciplinar puede ser la mejor manera de abordar la ciberseguridad de nuestras instalaciones y con ello, ayudar a conseguir que las nucleares sean el baluarte que el sector energético necesita para conseguir los objetivos propuestos.

Profesionales de ANAV involucrados directamente: Cruz Cirauqui, Rafael Cao, Marian Morán, Jordi Bolaños, Antonio Pontejo, Jose Ignacio Alutiz, Josep Mirambel, Josep Dols, Ignasi Balazote, Oscar Fernández. Profesionales de empresas colaboradoras involucrado directamente: Raúl Miró, Glòria Pujol, James Álvarez, Pau Bernadó, Daniel Maestro. ■