# CIBERSEGURIDAD, ASPECTO ESTRATÉGICO EN LA TRANSFORMACIÓN DIGITAL

ÓSCAR FERNÁNDEZ FERNÁNDEZ
SIC - Ciberseguridad
ASOCIACIÓN NUCLEAR ASCÓ-VANDELLÓS II

Cada vez es más evidente que hemos asimilado la ciberseguridad como una parte importante de nuestra vida personal y laboral. Si nos hubiesen dicho hace un año que nos llevaríamos las manos a la cabeza al saber que a los más pequeños de la casa se les dará clase con herramientas de videoconferencia inseguras, muchos no daríamos crédito.

En el artículo *Ciberseguridad a largo plazo* publicado en el número 400 de *Nuclear España*, hablamos de cómo una industria madura y orientada a la seguridad como es la nuclear, está especialmente alerta de los sucesos que se conocen como "cisnes negros". Podemos considerar la pandemia COVID-19 como el último de ellos, un suceso que se creía poco probable que superase los criterios de riesgo iniciales, pero que conlleva y conllevará un gran impacto a nivel global. Si bien es cierto que las centrales españolas ya contemplaban este tipo de situaciones, las medidas de confinamiento han necesitado que los profesionales nucleares hayan puesto todos sus recursos y conocimientos en la labor de mitigar el impacto tanto a las personas como en la operación segura de la instalación. No solo medidas clásicas de naturaleza física, por primera vez, hemos tenido que abordar un conjunto de actuaciones de carácter digital, orientadas a facilitar el acceso seguro en remoto a la información de la organización, y también redoblar esfuerzos en la protección de la isla interior, todo ello siguiendo nuestro modelo de ciberseguridad desde el diseño y defensa en profundidad.

Cuando utilizamos las tecnologías de la información para mitigar el impacto de estos "cisnes negros" que transforman el paradigma, qué duda cabe que para que esa transformación sea factible, la ciberseguridad es un aspecto estratégico fundamental. Este concepto fue el eje de la charla *Ciberseguridad, aspecto estratégico en la transformación digital* que se ofreció en la Jornada Técnica 2019 de la SNE, considerando los aspectos más importantes de ciberseguridad a tener en cuenta al abordar proyectos de digitalización en centrales nucleares, tanto para los que estamos en las plantas como para los proveedores de tecnología. El objetivo de la charla no fue entrar en aspectos técnicos, o discernir si es necesario digitalizar o no, ni qué estructuras, sistemas y componentes deben digitalizarse o qué sistemas de protección digital pueden incluirse en las plantas. El objetivo es remarcar que, para mantener la misión de operar nuestras plantas de forma segura y por supuesto a largo plazo, los nuevos proyectos de digitalización, han de llevar implícita la ciberseguridad.

Es fundamental. Y hay que analizarla al igual que la seguridad nuclear, la protección radiológica y en definitiva todos los aspectos "analógicos" de la seguridad, ya que un ciberataque a un elemento digital puede tener las mismas consecuencias que un sabotaje físico.

Hemos de partir de la base que las plantas están diseñadas de forma analógica. Es un diseño de los años 60. Y los análisis de seguridad tuvieron en cuenta los riesgos físicos y del proceso, pero no los riesgos digitales. Para paliar esto, ANAV y en general el sector nuclear lleva ya 10 años trabajando en los programas de ciberseguridad, tiempo en el que se han conseguido fundamentalmente dos cosas: la primera, obvia, incrementar el nivel de seguridad (o disminuir el nivel de riesgo) ante las ciberamenazas de nuestros componentes digitales, que como decíamos no fueron tenidas en cuenta en fase de diseño. Y la segunda, también muy importante, disponer de un marco normativo que nos ampare en todo lo relativo al cumplimiento legal, incluyendo auditorías y respuesta a incidentes como infraestructura crítica.

## DIGITALIZAR ES "SOLO" UN CAMBIO…

Nuestro negocio es especial. No podemos cambiar fácilmente todo un tren de un sistema por otro con tecnología digital más moderna y más eficiente. Estamos fuertemente regulados y por ello los cambios están acotados bajo unas normas muy estrictas.

Lo que sí que es cierto es que el mercado etiqueta la transformación digital al nivel de Revolución Industrial. Nos inundan con eslóganes como Industria 4.0 y demás grandes iconos. Parece como que si no digitalizas tu empresa estás desfasado. Hemos de ser conscientes de que probablemente, el mercado va a querer estirarnos más de lo que necesitamos, tengámoslo en cuenta, es su negocio. Pero el nuestro es ser fieles a nuestra visión y ser conservadores, mejorando la estructura sin perder el norte. Como dice el gran gurú de la ciberseguridad Patrick Miller, "*antes de poner una alarma, cierras las ventanas*".

Una de las primeras "ventanas" que tenemos que cerrar es conseguir que todos tengamos claro que hay que tener en cuenta la ciberseguridad en el día a día. Esto es un cambio difícil de implantar, incluso a los propios profesionales relacionados directamente en aspectos de ciberseguridad les cuesta, en algunas ocasiones. Todos aceptaremos bien un cambio "a digital" que nos proporciona beneficios inmediatos y fáciles de obtener, pero si ese cambio "a digital" lleva asociadas consideraciones molestas como tener que recordar contraseñas, retrasos en el diseño porque hay que implementar controles de seguridad que antes no se incluían, inconvenientes operativos, como por ejemplo tener que pasar por el puesto de verificación de virus al hacer un trabajo con un USB u otros trabajos adicionales, al final, la ciberseguridad se convierte en la cara menos amable de la digitalización.

Hay que asumir esto. A la gente al principio le va a costar, va a ser reticente a realizar todo este trabajo extra que, además, no muestra retorno claro de la inversión. Pero es necesario hacerlo, ya que ANAV ha sido nombrada Operador Esencial desde la publicación del Real Decreto que transpone la directiva europea NIS, con las implicaciones que eso conlleva. La ciberseguridad ha venido para quedarse y ya no es un tema opcional, porque nos jugamos mucho, como en todos los aspectos de nuestro negocio.

## ANALÓGICO ES MÁS SEGURO…

Aunque esta frase se suele escuchar a menudo, vamos a analizarla de forma objetiva:

Lo que parece claro es que un fallo en un sistema digital tiene los mismos impactos que el mismo fallo en su homólogo analógico. Que deje de operar, que cause daños, que provoque el fallo de otro equipo, que cause daños en la imagen pública… Otra cosa que comparten, es que tienen la misma naturaleza de amenazas, como son errores humanos, acciones maliciosas, desastres naturales, etc.

En cambio, lo que tiene un sistema digital que no tiene uno analógico es un conjunto nuevo de vulnerabilidades. Son aquellas que aprovechan lo que llamamos comúnmente "ciberataques". Fallos sin parchear, conexiones desprotegidas, *passwords* débiles y todo eso que los de ciberseguridad estamos continuamente machacando hasta hacernos pesados.

¿Entonces cuál es más seguro, el sistema analógico o el digital? Lo será aquel en el que se gestione su seguridad con más eficacia. Si se aportan los recursos necesarios para proteger un activo digital, y no para proteger uno analógico, será más seguro el digital, y viceversa, por supuesto. En nuestras centrales tenemos algo diferenciador. Por un lado, el 95 % de los activos de una planta tipo es analógico, y por otro lado, ese 5 % de los activos que son digitales se concentran en su gran mayoría en sistemas *No Importantes para la Seguridad*. Por eso en las nucleares ocurre la "paradoja analógica nuclear", por la que el diseño clásico analógico de las nucleares nos da una ventaja en cuanto a ciberseguridad frente a plantas más modernas, haciéndonos ideales para cubrir la demanda en un futuro cargado de riesgos digitales. Pero no hay que confundir diseño analógico con obsoleto. Como ejemplo, muchos fabricantes vuelven a introducir elementos analógicos en los catálogos, porque así lo demanda el negocio (Figura 1).

Por tanto, este aspecto diferenciador no hemos de perderlo. Es muy importante mantener el "core" de los sistemas importantes para la seguridad, lo que consideramos "protección", en su diseño analógico siempre que sea posible.

Ahora bien, ¿qué ocurre con los nuevos proyectos que sí incluyen activos digitales? Hemos de dotar de los recursos adicionales necesarios para proteger los activos digitales

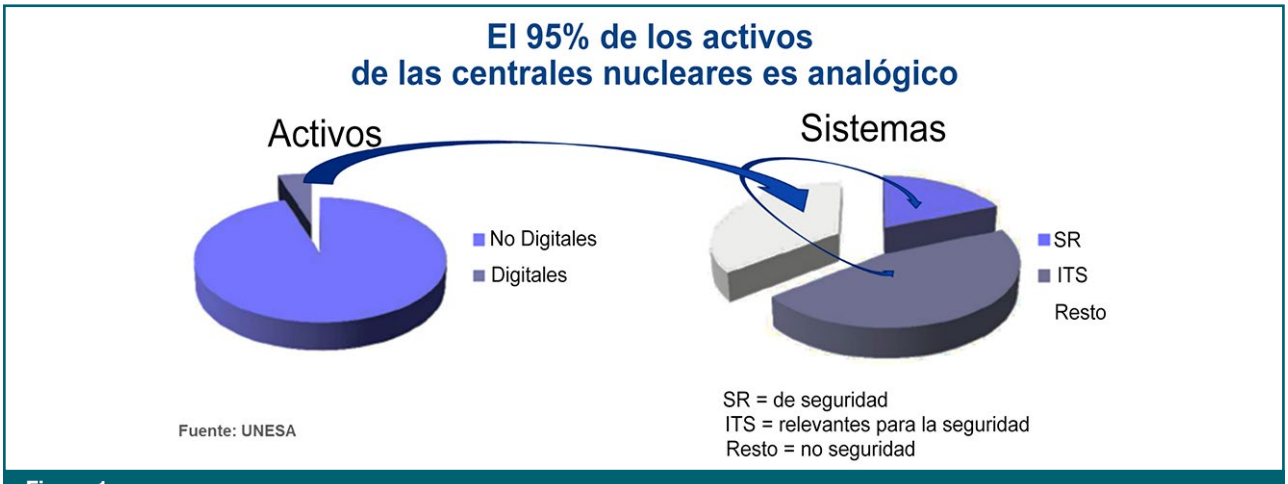


**Figura 1.**

con el mismo nivel que los analógicos, pero ¿podemos tener una seguridad digital nuclear a un nivel equivalente a la del resto de aspectos de la seguridad de una planta?

La respuesta es sí. No vamos a entrar en el detalle, pero el programa de ciberseguridad de las centrales nucleares españolas se basa en la normativa americana. Esta se fundamenta en la segmentación de redes por aislamiento y la defensa en profundidad, por el cual se plantea una estrategia defensiva a diferentes niveles y con controles estrictos en cada uno de ellos de forma incremental.

## CIBERSEGURIDAD DESDE EL DISEÑO

Para que un proyecto de digitalización tenga éxito es esencial diseñar bajo los criterios de ciberseguridad. Lo que conocemos como ciberseguridad por defecto. A cualquier activo digital de ANAV, le aplica el programa de ciberseguridad. Desde un PLC a un PC del departamento de Recursos Humanos, pasando por un multímetro digital o un USB, todos. Por este motivo, la ciberseguridad debe integrarse a nivel global, de manera que la ciberseguridad se considere un criterio de diseño, y no como un impedimento.

En las centrales españolas existe un aislamiento digital completo entre sistemas de seguridad nuclear y seguridad física, de los sistemas de monitorización y control, tal como exigió el CSN en 2012. Este diseño base ya nos cubre una buena parte de las vulnerabilidades digitales. Pero tenemos que ser escrupulosos en los diseños concretos de cada sistema, de cada activo y de cada comunicación del ámbito digital, sin olvidar el resto de controles que le aplican.

En el ámbito de los sistemas de monitorización y control, tenemos mucho más volumen de activos digitales a proteger. Un eficaz método para ello es incluir entre las protecciones una segunda frontera unidireccional también entre estos sistemas de monitorización y control y las redes corporativas de gestión.

Y, finalmente, el programa de ciberseguridad regula también el diseño de los activos de gestión corporativa, enfatizando por supuesto la protección de datos de carácter personal y la frontera con internet, con la premisa de no utilizar servicios en la nube que necesitemos en caso de aislarnos de internet manteniendo las funciones principales (Figura 2).

Parece entonces que la base es buena, pues tenemos un programa de ciberseguridad integrado a todos los niveles de la organización, el personal lo conoce y dará todo lo mejor que tiene para hacerlo lo mejor posible, tenemos el dinero suficiente, el apoyo de la dirección, incluso tenemos algo que es muy difícil de conseguir, y es que el personal de IT y el de OT trabajen en equipo y con el mismo objetivo. ¿Qué falta entonces para que un proyecto de digitalización salga bien?

Aquí es donde entran varios factores y que no siempre van a depender de nosotros. Ocurre que muchas veces estamos en manos de nuestra cadena de suministro, de nuestros proveedores.

Con la ciberseguridad, y en especial con la ciberseguridad industrial, ocurre con frecuencia que los fabricantes ven un filón lucrativo importante en colaborar con nosotros. Porque las empresas normalmente no se han preocupado hasta hace muy poco por la ciberseguridad. Frecuentemente, la ciberseguridad se oferta aparte y muchas empresas dejan eso de la *ciber* para más adelante. El problema viene cuando llegan los incidentes o las exigencias normativas, pues se ha visto que esto es contraproducente a la larga. Lo que se conoce como los costes de no securizar, que pueden ser mayores que los de securizar.

Entonces la solución efectiva es consultar a los fabricantes, que vienen a ayudar a solventar este problema, pero a un coste económico importante y esto pasa normalmente por falta de conocimiento por nuestra parte. No ocurre lo mismo en todos los ámbitos. Cuando compramos un coche, sabemos que las opciones de seguridad vial vienen de serie, no hay que elegir nada opcional en equipamiento de seguridad. Y no solo en los vehículos de gama alta. En cambio, muchos conocidos proveedores de equipamiento y servicios a centrales nucleares. Solo ofrecen algo de ciberseguridad como servicios de consultoría, y no queda claro que la ciberseguridad vaya a ser un elemento de serie. Parece más bien que será un equipamiento opcional, y que nos va a costar, además, un importe elevado. Otro problema grave, es que no nos dejan a gestionar esa ciberseguridad de forma autónoma bajo riesgo de pérdida de soporte ante incidentes, por lo que el coste del mantenimiento es aún mayor.

Como resumen, a la hora de diseñar hay que añadir el criterio de la ciberseguridad por defecto, sí, pero también es

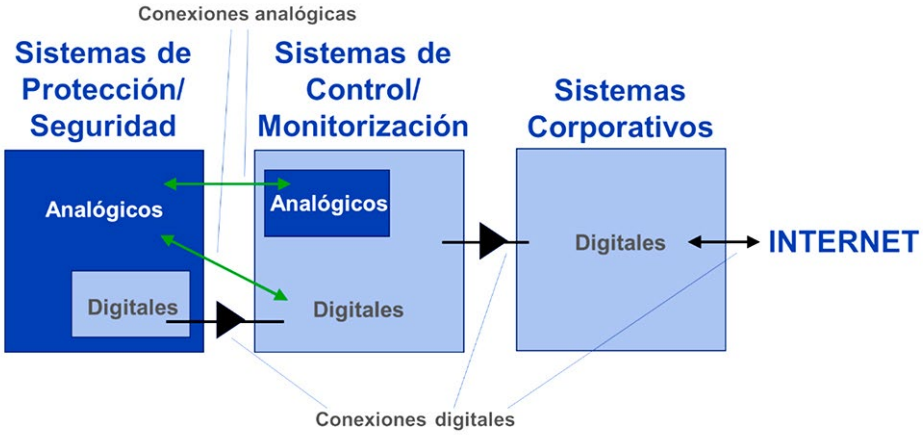


**Figura 2.**

importante saber encontrar al proveedor que nos incluya la ciberseguridad de serie, como en los coches. Los proveedores saben que esto está pasando y están trabajando en esta línea. Pero hay que hacer fuerza aquí, y es importante que nosotros vayamos a hablar con un fabricante sabiendo de lo que estamos hablando en materia de ciberseguridad, para que no nos vendan cajas negras y cumplamos con nuestro programa de ciberseguridad de forma eficiente.

## MANTENIMIENTO DE LA CIBERSEGURIDAD

Una vez tenemos un sistema diseñado e implantado con criterios de ciberseguridad, el sistema realiza su función sin problemas y tiene sus controles de ciberseguridad. Es seguro hoy, pero ¿mañana seguirá siéndolo? Todos sabemos que no, que es necesario un mantenimiento de la ciberseguridad. Igual que hay que engrasar una válvula, hay que actualizar parches de un *software*, y al igual que hay una regla de mantenimiento, hay unas políticas de ciberseguridad que dan unas periodicidades en las que hacer actuaciones en este sentido.

Para que este trabajo sea eficiente, y no trabajar de más, pero tampoco dejarnos cosas en el tintero que hagan que el sistema no cumpla con los controles de ciberseguridad aplicables, es muy importante el trabajo conjunto, creando grupos de trabajo entre los responsables del mantenimiento del sistema, los responsables del diseño y el personal de ciberseguridad corporativa de ANAV.

Cuando se implanta un nuevo sistema o activos digitales, es fundamental generar sus procedimientos de mantenimiento en paralelo, los cuales han de incluir las operativas y actuaciones necesarias para cubrir los controles de ciberseguridad (rondas de revisión para la mitigación de *insiders*, extracción de *logs* y ficheros de configuración, revisión de integridad de los datos, etc…). Del mismo modo, cuando se modifica un activo digital, se han de revisar también los aspectos que apliquen en su mantenimiento de la ciberseguridad.

La experiencia nos muestra una curva de aceptación del cambio muy acentuada, ya que para incorporar la ciberseguridad al mantenimiento de los sistemas es necesario cambiar muchos procedimientos y operativas. Hay muchas inercias y formas de hacer consolidadas y, por supuesto, hay que formar al personal encargado de realizar estas nuevas tareas. Aquí no es como en el diseño, que tarda más o menos, cuesta más o menos la ingeniería, pero el proyecto sale y listo. En cambio, al que mantiene el sistema le estamos poniendo trabajo extra para siempre. Todo este trabajo extra es necesario y la organización debe asumirlo.

Las tareas de mantenimiento de la ciberseguridad dan como resultado un conjunto de datos. Estos se tienen que analizar, aquí no acaba la cosa, hay que analizarlos a nivel de ciberseguridad, con multitud de herramientas, para conseguir dar cumplimiento a todos los controles de ciberseguridad aplicables. Las evidencias que nos muestran que estamos cumpliendo los controles (Figura 3).

En definitiva, aunando esfuerzos conseguimos generar los diseños adecuados que faciliten la ejecución de las tareas precisas de mantenimiento, (no trabajar de más), de forma que se cumplan los controles de ciberseguridad y el sistema quede preparado para asumir una auditoría de ciberseguridad completa y tenga herramientas para la detección y respuesta ante incidentes.

## RESPUESTA A INCIDENTES Y PROFESIONALES NUCLEARES CREATIVOS

Cuando un organismo regulador nos exige ciberseguridad, lo que no está pidiendo fundamentalmente son dos cosas: La primera, que tengamos una metodología, un plan de ciberseguridad integrado en todos los aspectos de la organización y, la segunda, que tengamos mecanismos para detectar, responder y reportar los incidentes de ciberseguridad.

El más fácil es el último. Reportamos con un formato según la casuística del incidente, unos interlocutores, etc. Mucho

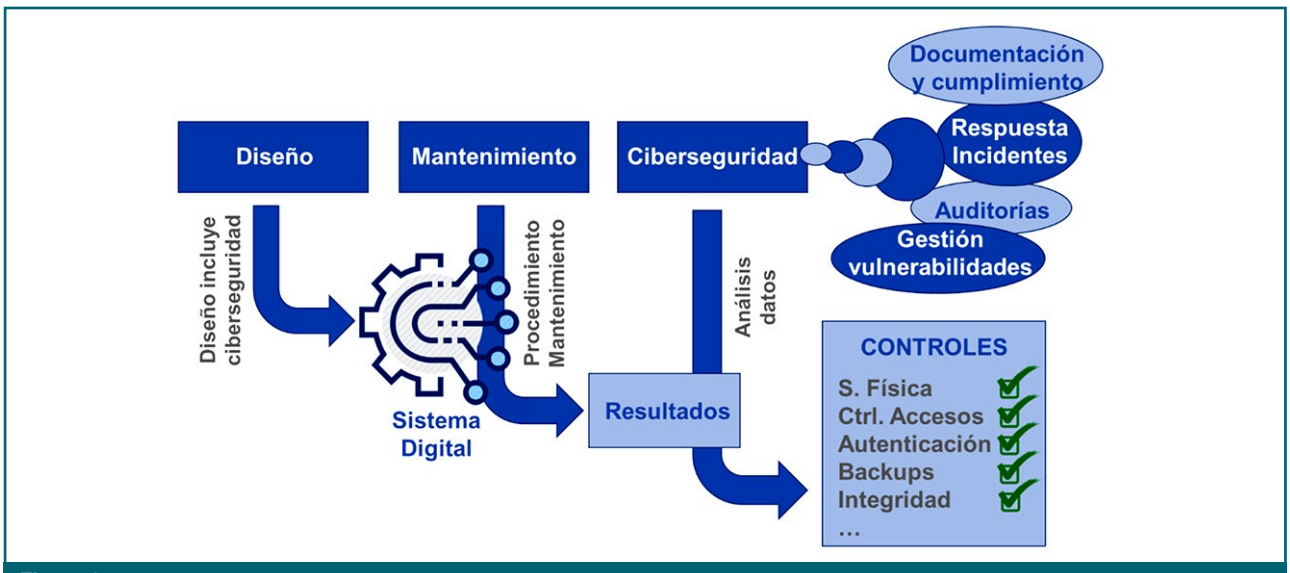


**Figura 3.**

más difícil es Detectar, pues necesitamos herramientas para ello. Necesitamos disponer de los datos y analizarlos ya sea con las incipientes herramientas automáticas como las basadas en correlación o el más moderno *machine learning*, o ya sean procedimientos más manuales, pero necesitamos tener esta información. En cualquier caso, es una tarea difícil, pues los malos van a intentar no dejar rastro.

Y, por último, lo que es tanto o más complicado es Responder. Una vez vemos el problema que me está generando un incidente y lo he reportado, ¿qué hago para que el impacto sea mínimo?

Es complicado porque el abanico de casuísticas diferentes es muy amplio. La realidad es que el número de incidentes de seguridad debido al *hacking* se incrementa de forma exponencial.

Entonces, ¿cómo podemos protegernos de estos incidentes? No hay más salida que seguir trabajando nuestro programa de ciberseguridad, ser escrupulosos con los controles de ciberseguridad desde el diseño al mantenimiento, auditorías, gestión de vulnerabilidades, etc. Pero el gran problema de la ciberseguridad es que no es posible procedimentar las actuaciones de defensa en todos los casos. Es cierto que hay procedimientos de contingencia, de recuperación de desastres, continuidad del negocio, cadenas de custodia y más buenas prácticas que vienen de la seguridad clásica, pero no es posible escribir un procedimiento para todas las casuísticas, básicamente porque no se conocen las nuevas armas que utilizarán los malos para atacarnos, ni se conocen los fallos de los sistemas que están aún por descubrir, los famosos 0-day (Figura 4).


**Foto 4.**

También es cierto que existe iteligencia artificial y que cada vez tomará más relevancia (defensa adaptativa, *Global Treath Intelligence*, etc.) que debería hacer eso por nosotros, pero hasta que todo esto sea automático y el personal de *ciber* ya no haga falta, se necesita realizar una serie de trabajos cuya naturaleza no suele darse en la industria nuclear. Para responder a un incidente, en ocasiones hay que pensar como los malos, utilizar el pensamiento lateral y a su vez mantener los valores que se necesitan para trabajar en la industria nuclear integridad, actitud cuestionadora, trabajo en equipo, decisiones conservadoras, etc. Hay que ser capaz de encontrar solución a problemas desconocidos, pero también otros enfoques a problemas conocidos.

Tal como dijo Einstein "*No podemos resolver problemas pensando de la misma manera que cuando los creamos*".