AUDITANDO SISTEMAS INDUSTRIALES E INFRAESTRUCTURAS CRÍTICAS

Cuadernos de ISACA Madrid

Reconocimientos

El Capítulo de Madrid de ISACA (183) desea reconocer la labor de:

Coordinación

Erik de Pablo Martínez, CISA, CRISC

Editor

Ana González Monzón, CISA, CISM

Coautores

Ana González Monzón, CISA, CISM

Antonio Cazorla, CISA

Erik de Pablo, CISA, CRISC

Dr. Jose Ramon Coz, CISA, CISM, CGEIT, CRISC, COBIT

Maite Avelino, CISA, CISSP, PMP

Antonio J. Turel, CISM

Revisores expertos

Francisco Moya Villar

Raúl Aguilera

Junta Directiva del Capítulo de Madrid de ISACA (183)

Ricardo Barrasa García, CISA, CISM, Presidente

Antonio Ramos, CISM, CISA, CRISC, Vicepresidente

José Miguel Cardona, CISA, CISM, CRISC, Secretario

Joaquín Castillón, CGEIT, CISA, Tesorero

Enrique Turillo Mateos, CISM, CISA, CRISC, Vocal

Pablo Blanco Iñigo, CISA, CISM, Vocal

Erik de Pablo Martínez, CISA, CRISC, Vocal

Índice de Contenidos

1 Objetivo

Presentar y describir un modelo para auditar sistemas de control industriales y de infraestructuras críticas, mostrando la metodología que se debe seguir con la revisión del análisis de riesgos, de los modelos de control y de las pruebas periódicas que se deben hacer para su verificación, con objeto de concluir sobre la madurez del entorno.

2 Antecedentes

Una forma para explicar mejor las características peculiares de la informática en los entornos industriales es comparándola con el entorno corporativo.

2.1 La informática corporativa

La informática corporativa es un sector maduro, con prácticas, normas, marcos de control y sistemas de revisión bien establecidos. Está centrado casi exclusivamente en la información y los sistemas que soportan los procesos de gestión de las compañías y en algunas aplicaciones técnicas de nicho.

Es habitual el uso de herramientas de colaboración como correo, mensajería, voz, video, etc… todo ello sobre unas redes de comunicaciones internas y de acceso a internet. Hoy en día los protocolos de comunicaciones se han unificado sobre TCP/IP, que se comparte con la red externa de Internet.

Otro aspecto relevante es el modelo de protección de la información y de las infraestructuras, que se denomina “seguridad lógica” y que ya tiene más de 20 años de existencia sometido a mejora continua. Este modelo está basado en un diseño de “Fortaleza” (seguridad perimetral) que ha permitido a las organizaciones ofrecer servicios internos centralizados, con transparencia, integridad, disponibilidad, confidencialidad y eficiencia.

2.2 El control en tiempo real en el siglo XX

Pasemos ahora a definir un concepto de especial relevancia en los entornos industriales, el concepto de tiempo real. Éste se basa en asegurar una respuesta de un sistema a un estímulo externo en un tiempo prefijado. Debido a la gran variedad de sistemas vinculados con un entorno al que suelen “controlar”, los valores característicos del tiempo de respuesta varían igualmente.

Por ejemplo, en un avión de combate el tiempo de respuesta puede ser de pocos milisegundos, mientras que en un horno de calcinación puede ser de segundos o incluso de minutos. Igualmente, el tiempo de respuesta en un sistema de invernaderos puede llegar a ser de segundos o minutos.

En los sistemas industriales clásicos (producción por lotes, envasado de líquidos, petroquímica, industria eléctrica, etc.…) los tiempos de respuesta suelen ser entre 50 y 100 milisegundos.

Se define entonces como “sistema de control en tiempo real” aquél que relaciona sensores y actuadores físicos a través de un programa informático cuya respuesta, en cualquier caso, está asegurada en un valor característico.

El diseño de los sistemas de control en tiempo real se ha realizado tradicionalmente alrededor de un procesador dotado de un conjunto de interrupciones que, adecuadamente priorizadas, permiten asegurar la respuesta en el tiempo prefijado. Estas interrupciones estaban totalmente centradas en el sistema de control y los aspectos secundarios, como la gestión de entrada o salida de periféricos (disco, ratón, etc…), se dejaban pendientes de la disponibilidad de CPU. Por ello, en los años anteriores al 2000 se consideraba que los sistemas de “tiempo real” y los sistemas corporativos eran completamente disjuntos y no se podían conectar salvo con dispositivos intermedios bastante complejos. Incluso con estos elementos de conexión, podría decirse que eran entornos aislados.

2.3 Cuando eran zonas aisladas

La arquitectura de estos sistemas, por ejemplo, los SCADA (*Supervisory Control and Data Acquisition*), era muy simple. Básicamente era una "caja negra", propietaria del fabricante, que se conectaba con los sensores y actuadores a través de unos paneles de electrónica cableada. Esta caja negra alojaba el procesador de tiempo real y los elementos de conexión a los paneles de conexionado.

Progresivamente fueron incorporándose periféricos que agrupaban la vinculación con los sensores y actuadores y que incluían también una lógica programada. Estos dispositivos se denominan controladores programables o PLC (*Programmable Logic Controller*). Los sistemas que los usaban, que utilizaban una red de comunicaciones propietaria bastante robusta, se denominan DSS (*Distributed Control System*) y son los habituales en el entorno del año 2.000.

El equipamiento, como decimos, ha sido siempre específico del proveedor, tanto procesadores como redes de control y conexionado (Redes LCN, Modbus, Fieldbus, RS422, RS485, etc…). Los sistemas basados en dicho equipamiento pueden llegar a manejar y supervisar de forma fiable y eficiente varios miles de sensores y actuadores.

En estos sistemas se alojan modelos de control muy sofisticados, por ejemplo, los PID (control de lazo Proporcional, integrativo y derivativo), FCS (Fuzzy Control System), ECS (Expert Control & Supervision), Control avanzado multivariable etc... Permiten almacenar información histórica del comportamiento de la planta y supervisan y manejan todos los posibles estados de la planta e incluso optimizan su eficiencia. Pero la arquitectura sigue siendo la descrita hasta aquí.

En resumen, estos entornos de control industrial han sido considerados hasta hace poco tiempo como "cajas negras" que han estado aislados de la red corporativa y centrados exclusivamente en su objetivo de controlar el proceso industrial, ofreciendo en ocasiones resultados o resúmenes, pero siempre en modo "*off-line*".

2.4 La conexión e integración de zonas del siglo XXI

A principios de la década del 2000 se inició un proceso de conexión de estos entornos industriales con los entornos corporativos, con objeto de que estos sistemas ofrecieran algunos datos de forma más interactiva o en "tiempo real".

Esta conexión fue inicialmente compleja y costosa, pero permitió introducir mejoras sustanciales, como conocer "*on-line*" datos de producción, información real de existencias o enviar a planta programas de producción u órdenes logísticas (por ejemplo, para automatizar la carga de camiones con pedidos).

Estas mejoras vinieron para quedarse y el proceso ya fue imparable. Sobre esta interacción cada vez más compleja entre los entornos corporativo e industrial, se sumó la aparición de equipamiento informático suficientemente rápido como para simular el concepto de "tiempo real". Estos nuevos equipos, basados en el sistema operativo Unix y posteriormente en Windows, no tenían las características descritas para considerarse de tiempo real pero su velocidad superaba con creces las limitaciones del sistema operativo estándar. Su coste decreciente y su potencia cada vez mayor no hacían más que facilitar esta transición. En la actualidad puede decirse que la inmensa mayoría de los sistemas industriales se basa en el sistema operativo Windows.

Una de las consecuencias más notables de este proceso ha sido la incorporación del protocolo TCP/IP en las redes de control. Este hecho ha sido aceptado por los fabricantes con muchas reticencias, por las características probabilísticas de este protocolo, pero el bajo coste, la facilidad de uso y la integración perfecta con los procesadores basados en Unix o Windows ha hecho que terminara siendo un estándar también en los sistemas industriales.

En ese momento las redes de control pasan a ser, *de facto*, una pieza más de los sistemas corporativos, debido a la continuidad que permite el protocolo de comunicaciones TCP/IP. La interconexión entre los entornos corporativo e industrial se hace muy sencilla y todos los requisitos de interoperabilidad que mencionábamos antes se cumplen en su totalidad. De hecho, la arquitectura inicial es simple, un ordenador de la red industrial está conectado a través de un *router* o *switch* a la red corporativa y de hecho se plantean muy pocas restricciones de tráfico a este enlace.

Sin embargo, hay que mencionar el impacto que provoca compartir tanto el protocolo de red como la continuidad y uniformidad de la infraestructura, ya que origina la aparición en los entornos industriales de las vulnerabilidades y los riesgos de ciberseguridad.

3 El problema y los riesgos

Ahora vamos a explicar por qué la problemática de las redes industriales es diferente y, por tanto, está expuesta a riesgos y consecuencias diferentes a la de los entornos informáticos. El auditor de estos sistemas deberá tener en cuenta los aspectos que se describen a continuación a la hora de realizar su actividad.

3.1 Complejidad

Un buen punto de partida es constatar las diferencias entre la protección de las infraestructuras críticas y la ciberseguridad industrial.

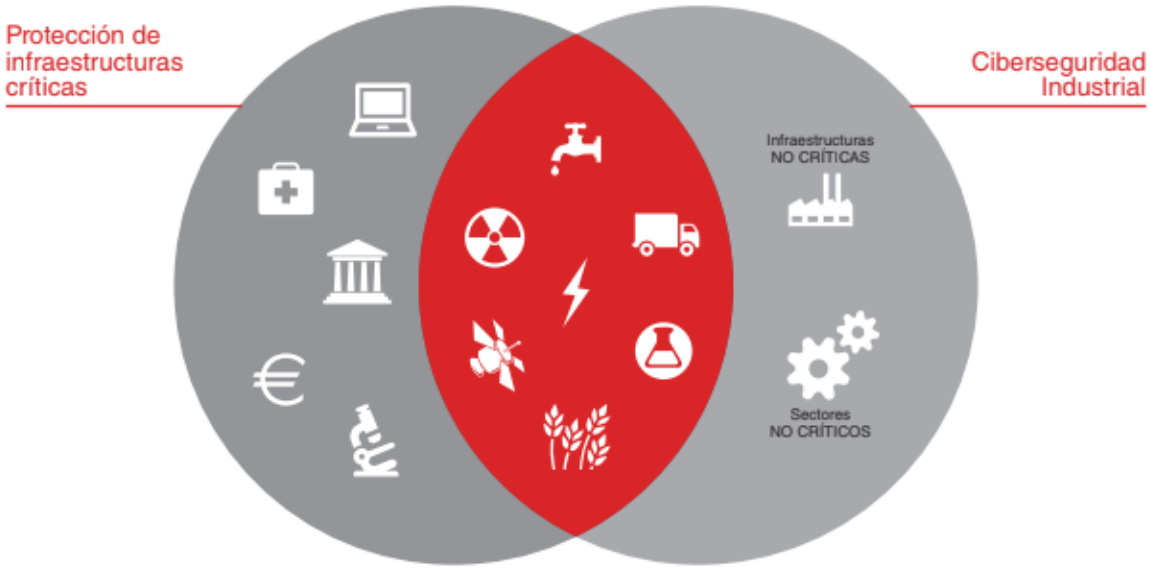

Ilustración 1 - Protección de Infraestructuras críticas y ciberseguridad industrial

(Fuente CCI)

La protección de Infraestructuras Críticas (PIC) ha adquirido gran relevancia debido a la repercusión que tendría sobre la sociedad la alteración o destrucción de las infraestructuras críticas y los servicios esenciales. Por otra parte, el ámbito de aplicación de la Ciberseguridad Industrial, dentro de los sectores industriales, es mayor que el de PIC, ya que la mayor parte de las infraestructuras industriales no son críticas, pero requieren ser protegidas de manera adecuada.

En el capítulo dedicado a la regulación se realizará una explicación detallada de la legislación específica que regula los aspectos de seguridad de las Infraestructuras críticas, por lo que no nos extenderemos ahora sobre ese aspecto. Cabe decir que la mejora de la conectividad aumenta la superficie de ataque y que, por tanto, el riesgo en el caso de una infraestructura crítica se vuelve mucho mayor.

En el caso del resto de instalaciones englobadas en lo que llamamos Ciberseguridad Industrial, hay fuertes carencias en la regulación y los aspectos de seguridad dependen de cada compañía propietaria, hecho que ha provocado que se apliquen diferentes estándares de seguridad en cada una de ellas. De esta forma podemos encontrar diferentes modelos de control de riesgos, cada uno con diferente madurez:

- Modelos Reactivos: basados en identificar el riesgo en concreto y actuar sobre él.
- Modelos Adaptativos: que abordan una gestión holística del riesgo

3.2 Diversidad de legislación

Hay un amplio número de organizaciones (NIST, JRC-EC, ISO/EIC, ENISA, CCI) que están desarrollando marcos estratégicos para la correcta gestión de la ciberseguridad y con ello la correcta gestión de riesgos en entornos industriales. En su esencia, todos tienen en común que se debe establecer un ciclo de vida equivalente al de un SGSI (Sistema de Gestión de la Seguridad de la Información) pero, específico a los Sistemas Industriales e IC. La disminución del riesgo sólo será posible a través de los ciclos aplicados año tras año, para llegar a un nivel aceptable de riesgo y finalmente considerar el riesgo residual como riesgo aceptado.

3.3 Prioridades

Hay otra consideración que diferencia de forma específica a los sistemas industriales de los entornos informáticos. En Seguridad Informática siempre hay tres principios clave a tener en cuenta en cualquier análisis: Confidencialidad, Integridad y Disponibilidad. En los sistemas Industriales hay que tener en cuenta que, a diferencia de los sistemas informáticos IT, la prioridad de estos principios es justo la inversa, ya que se trata de sistemas que funcionan en tiempo real que, por tanto, deben priorizar la Disponibilidad sobre cualquier otra consideración, seguida de la Integridad y la Confidencialidad en último lugar. El auditor de estos sistemas deberá valorar principalmente cualquier amenaza que ponga en riesgo la disponibilidad de las instalaciones que esté auditando.

3.4 Madurez

Aunque la adopción de las técnicas de conectividad ha mejorado el conocimiento y la uniformidad de las arquitecturas de los sistemas de control industrial, aún existe una carencia importante en todo lo relativo a la recogida de los datos (*logs*) que permitirían la aplicación de herramientas y técnicas existentes en los entornos informáticos. Gran parte de esta situación se debe a la existencia múltiples protocolos y formatos de datos, impuestos por los fabricantes de dispositivos.

Esta situación puede dificultar el trabajo del auditor ya que muchas de las herramientas utilizadas en los entornos IT no estarán disponibles para entornos industriales y deberá hacer uso de herramientas configuradas específicamente para ellos, con el agravante de que, como hemos visto en el párrafo anterior, el uso de estas herramientas podría afectar al funcionamiento normal de los sistemas de control industrial y poner en peligro la continuidad del servicio de la instalación auditada. Por tanto, es muy importante que el auditor y/o su equipo tengan un buen conocimiento de los entornos de proceso y los protocolos de los dispositivos de los entornos industriales.

3.5 Concienciación

En los entornos industriales puede afirmarse que es muy reciente la sensibilización hacia la ciberseguridad, y el enfoque es menos intenso que el que existe por ejemplo hacia la Seguridad física o medioambiental.

Tradicionalmente los sistemas de control han sido una pieza más del proceso industrial, en el que el objetivo primordial es la producción (continuidad). Normalmente los profesionales que atienden a estos sistemas están mucho más cercanos a las problemáticas físico-químicas y de ingeniería del proceso industrial que al mundo de la informática. Por ello, estos equipos han sido en cierta forma refractarios a las metodologías que se introdujeron a principios de la década del 2.000 (ITIL por ejemplo) y las nuevas exigencias llegan en una fase de baja madurez. Este punto es de importancia crucial y debe ser tenido muy en cuenta por los auditores.

En general, el auditor debe identificar, analizar y tratar los riesgos de la instalación industrial auditada, de acuerdo con la problemática descrita anteriormente para realizar un análisis de riesgos, para el que podrá utilizar una metodología como la descrita en la siguiente figura.

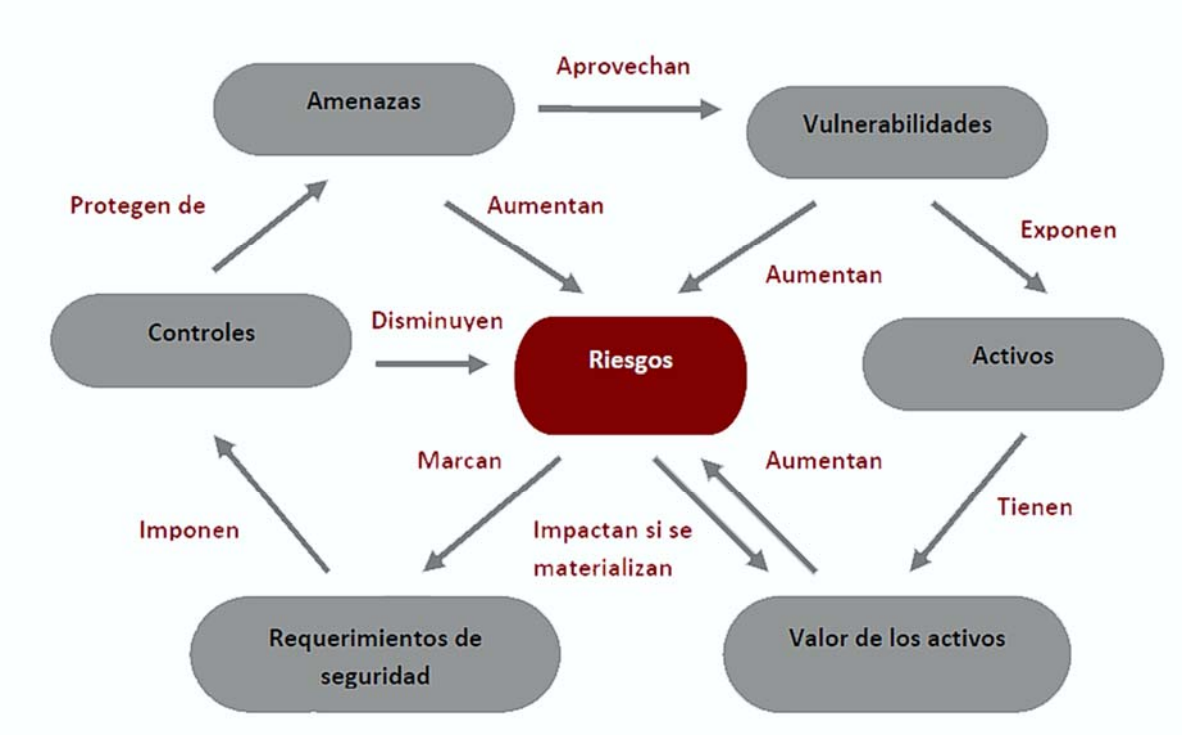

Ilustración 2 - Ciclo metodológico para el análisis de riesgos

3.6 Evolución tecnológica

La costumbre en los sistemas industriales ha sido siempre la de instalar productos de un único fabricante en una "isla", desconectada del resto de la organización, con un funcionamiento probado, continuo y sin alteraciones externas. Este modelo de "caja negra" ha estado vigente hasta hace pocos años y subyace en muchos diseños actuales.

Actualmente, en medio de la Transformación Digital Global, el sector industrial se encuentra añadiendo mayor 'inteligencia' a sus procesos, para conseguir una reducción de costes y obtener mayor efectividad productiva (beneficio económico).

A continuación, parte de los activos que deberán ser tenidos en cuenta en la gestión de riesgos:

- Archivos de proyecto.
- Lógica en ejecución en controladores y SCADA.
- Equipos, máquinas y/o instalaciones.
- Materia prima, material en proceso y/o producto terminado.
- Información del proceso y/o de la organización.
- Red y elementos de la arquitectura de comunicación.
- Medio Ambiente.
- Personal propio y/o de terceros.
- Terceras personas.

3.7 Modelos de Análisis de riesgos

Si bien cualquier modelo de análisis de riesgos es, en principio, de aplicación para cualquier entorno, la realidad es que los entornos industriales tienen sus peculiaridades.

Por ejemplo, los riesgos de baja probabilidad y alto impacto son de gran importancia, debido a los efectos multiplicadores del entorno industrial:

- efectos en el medio ambiente
- efectos en la salud de la población cercana
- posibles riesgos letales para las personas del circulo próximo
- efectos en los servicios esenciales
    - impacto en la población
    - desaprovisionamiento
    - carencias de bienes y servicios
    - efectos psicológicos en la población
- efectos reputacionales
- etc…

Por ello, aunque en los análisis de riesgos IT no suelen ser considerados, en este caso es imprescindible tenerlos en cuenta, con técnicas de análisis específicas.

Por esta razón podemos considerar dos tipos de riesgos muy diferentes:

3.7.1. Riesgos genéricos de ciberseguridad

En este conjunto englobamos todos los riesgos que coinciden esencialmente con aquellos que pueden darse en una instalación de informática convencional (corporativa).

El análisis puede hacerse siguiendo cualquier metodología, aunque una muy efectiva es identificar junto con el responsable de la instalación, aquellos problemas que pueden surgir en cada unidad alrededor de los grandes controles definidos en las metodologías más conocidas. Este método permite hacer un barrido razonablemente completo, aunque ello no impide que puedan existir algunos riesgos no detectados y que todo el análisis deba ser revisado meticulosamente.

Normalmente los problemas son consecuencia de deficiencias en la aplicación de los “marcos de control” o de problemas surgidos al azar sin una intencionalidad definida.

3.7.2 Riesgos específicos del entorno industrial

Las instalaciones industriales, por las graves consecuencias que ya hemos citado, pueden ser objeto de ataques específicos dirigidos a provocar daños en la instalación, en las personas, el medio ambiente, una discontinuidad en la producción o efectos en la calidad de los productos. Todos estos objetivos pueden ser una motivación para potenciales atacantes y hacen muy verosímil la posibilidad de que un ataque imprevisible (o improbable) se produzca.

Por esta razón los análisis de riesgos deben contemplar escenarios de posibles amenazas de gran impacto, y en ellos se deberá tener muy en cuenta que los modelos de riesgos cibernéticos no son lineales, es decir, la probabilidad se incrementa notablemente con el horizonte temporal.

Habitualmente los modelos de riesgos consideran que los riesgos de una instalación industrial son lineales, es decir, la probabilidad de que se produzca una avería en un componente a 5 años vista es aproximadamente 5 veces la de que se produzca a un año, todo ello suponiendo que no se modifica la respuesta de control durante ese tiempo

En el caso de la ciberseguridad esto no es así, a 5 años vista y sin modificar la respuesta, la probabilidad de que un determinado riesgo se haga efectivo es prácticamente del 100%.

De ahí se deduce que en ciberseguridad la respuesta debe modularse año a año, de forma que se mantenga controlada la curva exponencial. Este enfoque es aún más importante para aquellos riesgos derivados de amenazas dirigidas, fundamentalmente por el alto impacto que suponen. Solo así se podrá considerar que el modelo de riesgos tiene una cobertura razonable.

Es papel del auditor y una de sus primeras tareas, evaluar el análisis de riesgos realizado y concluir sobre si tiene la cobertura que debe.

4 La Regulación

4.1 Nacional

Tras el atentado de las Torres Gemelas del año 2001 y, sobre todo, el del 11 de Marzo en Madrid, la Unión Europea (UE) impulsó el desarrollo de un **programa para la protección de las infraestructuras críticas.**

Inicialmente se publicó un Libro Verde [1] con el *brainstorming* llevado a cabo entre todos los actores interesados en este tema, tanto públicos como privados. Un poco más tarde, el 12 de febrero del 2007 se aprueba el Programa Europeo para la Prevención, preparación y gestión de las consecuencias del terrorismo y otros riesgos relacionados con la seguridad.

Poco más de un año después, la iniciativa inicial desemboca en la **Directiva 2008/114/CE** del Consejo, de 8 de diciembre de 2008 [2]. Esta directiva propine la identificación y designación de infraestructuras críticas europeas (ICE), proporcionando al mismo tiempo, un enfoque común para la evaluación de estas infraestructuras.

Pasando al plano español, la Seguridad Nacional es competencia en primer lugar de la Secretaría de Estado del Ministerio del Interior, pero se apoya en números actores que se articulan gracias al Departamento de Seguridad Nacional.

Previa a la directiva europea ya mencionada, la Secretaría de Estado de Seguridad del Ministerio del Interior elabora el Plan Nacional de Protección de las Infraestructuras Críticas, de 7 de mayo de 2007, así como el primer Catálogo Nacional de Infraestructuras Estratégicas.

Las áreas en las que dicha seguridad se dividen se articulan en doce ejes, uno de los cuales es el de las **Infraestructuras Críticas.**

La trasposición de la Directiva Europea 2008/114/CE se tradujo en la **Ley de Protección de Infraestructuras Críticas (LPIC)**, Ley 8/2011 de 28 de abril [3].

En esta ley se establecen una serie de objetivos y competencias a destacar:

- Señalar los sectores prioritarios (ver nota 1).
- Definición de Infraestructura Crítica.
- Definir los Planes Estratégicos Sectoriales.
- Definir el concepto de Operador Crítico.

Como complemento de dicha ley se promulgó el **Real Decreto 704/2011,** de 20 de mayo, por el que se aprueba el **Reglamento de protección de las infraestructuras críticas.** Por otra parte, se crea en el 2014 la **Comisión Nacional para la Protección de las Infraestructuras Críticas,** órgano colegiado adscrito a la Secretaría de Estado de Seguridad y que tendrá desde entonces como misión las siguientes tareas:

- Aprobar los distintos Planes Estratégicos Sectoriales (PES).
- Designar a los Operadores Críticos (OC) que se propongan.
- Aprobar la creación, modificación o supresión de grupos de trabajo sectoriales o de carácter técnico, estableciendo sus objetivos y sus marcos de actuación.

Los **Planes Estratégicos Sectoriales (PES)**, permiten identificar los servicios esenciales prestados a la sociedad por los sectores objeto de estudio, el funcionamiento general de éstos, las principales amenazas de origen deliberado sobre los mismos y sus principales vulnerabilidades, las infraestructuras críticas que proporcionan servicio y los operadores propietarios y/o gestores

de las mismas. Estos planes culminan con una evaluación de las consecuencias potenciales de su inactividad, así como con una propuesta de medidas estratégicas para su mantenimiento.

Los **Operadores Críticos (OC)** son los Agentes del Sistema, provenientes tanto del sector público como del sector privado, responsables del funcionamiento diario de una instalación, red, sistema o equipo físico o de tecnología de la información designada como infraestructura crítica conforme a la **Ley 8/2011**, **por la que se establecen medidas para la Protección de las Infraestructuras Críticas**. Los operadores críticos forman parte del Sistema de Protección de Infraestructuras Críticas, con una especial relación con las autoridades competentes, a través del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).

Para estos operadores implica una serie de obligaciones:

- Participación de los operadores en la **mesa de coordinación** establecida en el Plan Nacional de Protección de Infraestructuras Críticas.
- **Intercambio de información** relevante para la seguridad de sus instalaciones, redes y sistemas, en el acceso a los sistemas de comunicación previstos por la Ley.
- Implementación de medidas de protección alineadas con el **Plan de Protección y Prevención Antiterrorista**, actualmente en nivel 4.

En lo relativo al Sistema de Seguridad Nacional, **la protección de infraestructuras críticas queda recogida** en la Ley 36/2015 de Seguridad Nacional [4]**,** en su art. 7 Colaboración Privada:

*"1. **Las entidades privadas**, siempre que las circunstancias lo aconsejen y, en todo caso, **cuando sean operadoras de servicios esenciales y de infraestructuras críticas** que puedan afectar a la Seguridad Nacional, **deberán colaborar con las Administraciones Públicas**. El Gobierno establecerá reglamentariamente los mecanismos y formas de esta colaboración."*

y art. 11 Obligaciones de las Administraciones Públicas:

*"2. Asimismo, sin perjuicio de lo establecido en la normativa reguladora de protección de infraestructuras críticas, **las Administraciones Públicas citadas anteriormente asegurarán la disponibilidad de los servicios esenciales y la garantía del suministro de recursos energéticos, agua y alimentación, medicamentos y productos sanitarios, o cualesquiera otros servicios y recursos de primera necesidad o de carácter estratégico**."*

En la Estrategia de Seguridad Nacional 2017 [5], la amenaza contra las infraestructuras críticas se encuentra entre las principales amenazas identificadas, junto con conflictos armados, el terrorismo, el crimen organizado, la proliferación de armas de destrucción masiva y el espionaje, dado el impacto que una agresión sobre ellas puede comportar para la provisión de los servicios esenciales. Igualmente, la ESN 2017 establece como línea de acción en el ámbito de la Ciberseguridad, y respecto a las infraestructuras críticas el reforzar, impulsar y promover los mecanismos normativos, organizativos y técnicos, así como la aplicación de medidas, servicios, buenas prácticas y planes de continuidad para la protección, seguridad y resiliencia, de manera que se garantice un entorno digital seguro y fiable.

En el anexo de la Ley PIC aparecen los 12 sectores contemplados y los ministerios (del año 2011) que eran competentes en la materia a saber:

Administración.	Ministerio Presidencia.
	Ministerio Interior.
	Ministerio Defensa.
	Centro Nacional de Inteligencia.
	Ministerio Política Territorial y Administración Pública.
Espacio.	Ministerio Defensa.
Industria nuclear.	Ministerio Industria, Turismo y Comercio.
	Consejo de Seguridad Nuclear.
Industria química.	Ministerio Interior.
Instalaciones de investigación.	Ministerio Ciencia e Innovación.
	Ministerio Medio Ambiente, y Medio Rural y Marino.
Agua.	Ministerio Medio Ambiente, y Medio Rural y Marino.
	Ministerio Sanidad, Política Social e Igualdad.
Energía.	Ministerio Industria, Turismo y Comercio.
Salud.	Ministerio Sanidad, Política Social e Igualdad.
	Ministerio Ciencia e Innovación.
Tecnologías de la Información y las Comunicaciones (TIC).	Ministerio Industria, Turismo y Comercio.
	Ministerio Defensa.
	Centro Nacional de Inteligencia.
	Ministerio Ciencia e Innovación.
	Ministerio Política Territorial y Administración Pública.
Transporte.	Ministerio Fomento.
Alimentación.	Ministerio Medio Ambiente, y Medio Rural y Marino.
	Ministerio Sanidad, Política Social e Igualdad.
	Ministerio Industria, Turismo y Comercio.
Sistema financiero y tributario.	Ministerio Economía y Hacienda.

Ilustración 3: Sectores en la Ley de Protección de Infraestructuras Críticas. 2011

4.2 Internacional

En el ámbito internacional, muchos países de todo el mundo han comenzado a desarrollar legislación para regular tanto la ciberseguridad, como la seguridad física de los sistemas de control

industrial y de las infraestructuras críticas. Sin embargo, el enfoque y la cobertura de las regulaciones difieren considerablemente en algunas zonas. A continuación, se muestra un resumen de la legislación internacional en esta materia:

4.2.1 Unión Europea

Desde el año 2004 la Comisión Europea lleva emitiendo comunicaciones, directivas, y leyes en relación a la ciberseguridad en general y a las infraestructuras críticas en particular, al mismo tiempo que promueve el desarrollo de legislación en dicha materia en los países de la Unión.

- **Comunicación COM (2004)** [6], de la Comisión al Consejo y al Parlamento Europeo, del 20 de octubre 2004, Protección de las infraestructuras críticas en la lucha contra el terrorismo. Describe las acciones que la Comisión adoptó en su momento para proteger las infraestructuras críticas y proponía medidas adicionales para consolidar los instrumentos existentes.
- **Comunicación COM (2005)** [1], de 17 de noviembre de 2005, Libro Verde sobre un Programa Europeo para la Protección de Infraestructuras Críticas. Identifica los principales temas a tratar en el Programa Europeo para la Protección de Infraestructuras Críticas
- **Comunicación COM (2006)** [7], de la Comisión sobre un Programa Europeo para la Protección de Infraestructuras Críticas. Obliga a todos los Estados miembros a transponer los componentes del Programa Europeo de Protección de Infraestructuras Críticas a sus legislaciones nacionales.
- **Directiva 2008/114/CE del Consejo**, de 8 de diciembre de 2008 [2], sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. La directiva establece que cada Estado miembro debe identificar las infraestructuras críticas existentes en su territorio, y debe asegurarse de que disponen de un plan de seguridad del operador y de un responsable de enlace para la seguridad. Así mismo, cada Estado miembro ha de realizar una evaluación de amenazas sobre los subsectores de las Infraestructuras críticas
- **Agenda Digital**. Publicada el 19 de mayo de 2010, [8] se considera parte de la Estrategia Europa 2020; uno de cuyos siete pilares fundamentales es la consolidación de la confianza y de la seguridad en los bienes y servicios digitales. Entre los objetivos de la agenda está el reforzar la política europea de la lucha contra la ciberdelincuencia. En este sentido la Agenda Digital prevé la presentación de medidas relativas a la seguridad de las redes y la información y a la lucha contra los ataques informáticos.
- **Estrategia Europea de Ciberseguridad** [9] recogida en la Comunicación Conjunta de la Comisión, de 7 de febrero de 2013. Busca garantizar que los derechos fundamentales existentes en la Unión Europea también sean aplicados también en el ciberespacio. Siendo su pilar fundamental la Directiva sobre seguridad de las redes y sistemas de información (Directiva SRI), en vigor desde agosto de 2016. Entre las medidas que propone cabe destacar la adopción de gestión de riesgos por parte de los operadores de infraestructuras críticas de algunos sectores como los servicios financieros, y el transporte; así como los servicios de la sociedad de la información, tiendas de aplicaciones, plataformas de comercio electrónico y administraciones públicas.
- **Directiva 2013/40/UE del Parlamento Europeo y del Consejo** [10] , de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. Identifica la existencia en la Unión Europea de una serie de infraestructuras consideradas críticas, por cuanto resultan esenciales para el mantenimiento de funciones vitales para la sociedad, como la salud, la seguridad, la protección y el bienestar económico y social de la población. Entre tales infraestructuras se cuentan las centrales eléctricas, las redes de transporte o las redes de telecomunicación, cuya perturbación o destrucción tendría un impacto significativo en un Estado miembro, al impedirle mantener las mencionadas funciones, además de previsibles e importantes repercusiones transfronterizas.

- **Directiva 2016/943/UE del Parlamento Europeo y del Consejo**, de 8 de junio de 2016, de Protección de Secretos Comerciales [11]. Intenta armonizar la legislación de los Estados miembros con el objetivo evidente de fomentar la competitividad y evitar la práctica de comportamientos desleales que pueden afectar al comportamiento de los actores económicos en el mercado.
- **Directiva 2016/1148/UE del Parlamento Europeo y del Consejo**, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión [12]. Directiva NIS. Fue diseñada con la ayuda de la European Agency for Network and Information Security (ENISA) para aplicar normas mínimas de buenas prácticas que permitan mejorar la seguridad general de los proveedores de servicios esenciales.

  La Directiva NIS dicta que:

  - Los estados miembros deben tener equipos de respuesta a incidentes adecuados y seleccionar una autoridad NIS adecuada.
  - Los estados miembros deben cooperar e intercambiar información de seguridad pertinente con otros estados miembros mediante la creación de una Red de Equipos de Respuesta a Incidentes Informáticos para promover un intercambio rápido y eficaz.
  - Los estados miembros deben tomar las medidas de seguridad adecuadas para proteger a los sectores considerados vitales para la economía y la sociedad (energía, transporte, agua, instituciones financieras, atención médica, infraestructura digital, etc.)
- **Directiva 2017/541/UE del Parlamento Europeo y del Consejo**, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo. [13] Identifica las actividades delictivas que serán tipificadas como delitos de terrorismo. Entre los cuales se hace referencia a la interferencia ilegal en los sistemas de información, la perturbación o interrupción del suministro de agua, electricidad u otro recurso natural básico cuyo efecto sea poner en peligro vidas humanas, o la destrucción masiva de instalaciones estatales o públicas, sistemas de transporte e infraestructuras, y sistemas informáticos.
- **ALEMANIA**: IT Security ACT del 25 de julio de 2015 [14]

La ley, promovida por la Oficina Federal de Seguridad de la Información, requiere que las industrias mejoren sus sistemas de seguridad de TI en los siguientes aspectos:

- Disponibilidad, integridad, confidencialidad y autenticidad de la seguridad de TI en toda Alemania.
- La seguridad informática dentro de las empresas.
- Proporcionar una mayor seguridad y protección de TI para los ciudadanos que utilizan Internet.
- Proteger la infraestructura considerada crítica para la función de la comunidad.

Esta ley afecta a los operadores de sitios web, a las compañías de telecomunicaciones y a los operadores de infraestructura crítica. Su cumplimiento es obligatorio para todos los proveedores de servicios y terceros; pero incluye un período de transición de dos años para restaurar la infraestructura crítica. Así mismo, los proveedores y operadores no conformes están sujetos a multas.

- **FRANCIA**: Military Programming Act [15]

Aprobada por primera vez en 1960, la Ley de Programación Militar establece los estándares para garantizar la integridad de las ICs. Hasta 2013, los requisitos se relacionaban principalmente con la implementación de medidas de seguridad física. Sin embargo, esto ya no es el caso ya que la Ley de Programación Militar de 2013 agregó disposiciones relacionadas con la ciberseguridad. Siendo su última actualización la del 27 de marzo de 2017. La ley obliga a las ICs entre otros aspectos a:

- Designar a un representante de seguridad de la IC para que sea el punto de contacto con ANSSI (la Agencia Nacional de Ciberseguridad de Francia)
- Redactar una Política de Seguridad
- Emplear los servicios de proveedores de servicios certificados por ANSSI
- El reporte inmediato de cualquier incidente de seguridad
- Auditorías e inspecciones regulares para verificar su nivel de seguridad.

El incumplimiento de la ley conlleva una multa de hasta € 150,000 para el director de la IC y de hasta € 750,000 para la entidad legal.

REINO UNIDO: Ley de protección de infraestructuras críticas y servicios digitales. 10 de Mayo de 2018. [16] La ley focalizada principalmente en las empresas de salud, agua, energía, transporte e infraestructura digital, está destinada a ayudar a reducir la cantidad de ataques cibernéticos perjudiciales que afectan al Reino Unido, y dará a los nuevos reguladores poderes para evaluar industrias críticas y asegurarse de que existen planes para prevenir ataques. Las empresas que no informen sobre las violaciones de seguridad y cortes de red a los reguladores dentro de las 72 horas siguientes al incidente pueden llegar a ser penalizados con multas de hasta 17 millones £.

4.2.2 Otros países

- **Estados Unidos de América**
  - **North American Electric Reliability Corporation (NERC).** [17]

    Las directrices de "Critical Infrastructure Protection" son aplicados por la Corporación de Confiabilidad Eléctrica de América del Norte (NERC). Estas regulaciones se relacionan con los protocolos de preparación y respuesta para incidentes graves que involucran infraestructura crítica en una región o nación en particular. En este caso, los estándares de confiabilidad para la mayor parte del sistema de energía de los EE. UU

  - **United States Nuclear Regulatory Commission (USNRC).** [18]

    Para la energía nuclear, la Dirección de Seguridad Cibernética de 2013 otorgó toda la responsabilidad de cumplimiento y regulación a la Comisión Reguladora Nuclear de los Estados Unidos (USNRC). La dirección centralizada de supervisión para garantizar la fiabilidad en la red eléctrica de América del Norte. Estas amplias regulaciones se han implementado para proteger las computadoras digitales, los sistemas de comunicación y las redes asociadas con la energía nuclear

- **China**
  - **Cybersecurity Law**. (CSLaw) on 7 November 2016 [19]

    La ley tiene como objetivo regular las actividades de las empresas que operan en este país y que acceden al ciberespacio chino, siendo aplicable a las organizaciones establecidas allí. Ha sido una ley bastante controvertida entre otras razones porque permite al Ministerio de Seguridad Pública realizar pruebas de penetración y análisis de redes a distancia o en el sitio, explotar vulnerabilidades, y obligar a las empresas a crear puertas traseras. Uno de los ámbitos de aplicación son los que ellos denominan "operadores de infraestructuras de información crítica", entre los que se encuentran algunas infraestructuras críticas tales como las telecomunicaciones, la salud pública, la energía, el transporte, o el tratamiento de aguas. La ley obliga a los operadores de información crítica a almacenar sus datos en territorio chino, y a celebrar un contrato con los subcontratistas, con independencia de que estén localizados dentro de China o fuera de su territorio, que incorpore cláusulas con las medidas de seguridad exigibles, quedando sometidas al poder de inspección de las autoridades chinas.

- **Australia**
  - **Security of Critical Infrastructure** Act 2018 [20]

    Dado que la mayoría de las infraestructuras críticas en Australia son de propiedad u operación privada, esta ley nace para permitir al gobierno introducir medidas que le permitan tener una mejor comprensión y control sobre la propiedad de las infraestructuras, y así poder responder mejor a los riesgos de la seguridad nacional. Además, en los últimos años se ha observado un incremento del riesgo debido a una mayor conexión de los activos a Internet, y al hecho del aumento de la subcontratación de empresas extranjeras, las cuales añaden amenazas adicionales como el sabotaje y el espionaje. La Ley contiene dos medidas clave: el registro de los activos de las infraestructuras críticas, y la facultad del Ministerio del Interior de emitir instrucciones al propietario u operador de la infraestructura para mitigar los riesgos de seguridad nacional (por ejemplo, obligando a que no externalice las operaciones de su red central a ciertos proveedores).

Si comparamos la legislación europea con la del resto del mundo, observamos que la Comisión Europea lleva legislando sobre la materia desde 2003 y la mayor preocupación de los países europeos es la prevención de los ciberataques, EEUU legisla sobre sectores específicos y se focaliza más en la respuesta a incidentes y, por otro lado, tanto a China como a Australia, donde la legislación es más reciente, les inquieta más el riesgo que introducen los proveedores extranjeros.

5 Diseño de un modelo de control para instalaciones industriales

Para proceder a realizar una auditoría informática sobre Infraestructuras Industriales hay que conocer previamente si existe un modelo de control y sobre qué base o referencia se ha construido. Denominamos Modelo de Control a un conjunto amplio de controles que pretende ser completo y que se diseña con el objetivo de que mitiguen los riesgos detectados en el Mapa de Riesgos.

Es decir, debe existir una fuerte relación entre los riesgos definidos en el Mapa de Riesgos y las iniciativas establecidas para mitigarlos, las cuales se denominan controles. No debería haber por tanto riesgos sin, al menos, un control asociado.

Lo habitual es que este modelo no haya existido en la Instalación hasta hace poco, cuando las amenazas de ciberseguridad han obligado a tomar conciencia del riesgo, de manera que la práctica diaria ha ido consolidando unas formas de trabajo que suelen dificultar bastante la implantación de un modelo de control estándar. Por todo ello se suele diseñar un modelo "ad-hoc" que se inspira en algún estándar, procurando adaptar la forma en la que se alcanzan los objetivos de control del estándar elegido.

Se puede decir que la práctica y la producción industrial imponen severas limitaciones a los controles de diseño clásico, razón por la cual deben ser sustituidos por otros diferentes, pero con similar efecto mitigatorio de los riesgos.

Para ello se puede utilizar alguno de los modelos publicados, entre los que destacan el marco norteamericano NIST ("*Framework for Improving Critical Infrastructure Cybersecurity*", versión 1.1) y el estándar ISA99/IEC62443("*Security for industrial automation and control system* "). En ambos casos se trata de unos documentos muy detallados que precisan de una organización muy madura para su implantación completa, por lo que suelen ser inspiradores de modelos de control más limitados. En cualquier caso, es imprescindible conocer qué referencia se ha utilizado para diseñar el modelo de control aprobado.

5.1 Arquitectura

Una de las piezas fundamentales de este diseño es el establecimiento de una arquitectura adecuada para la organización de los equipos y las redes de comunicaciones en la instalación industrial. Esta arquitectura actúa por si sola como un macro-control, puesto que debe conllevar una reducción significativa de gran parte de los riesgos reconocidos. Por lo tanto, es uno de los elementos que debe ser identificado y evaluado en la fase inicial de la auditoría.

Existen muchas arquitecturas para entornos industriales, normalmente auspiciadas por los grandes fabricantes que siempre han propuesto arquitecturas para sus productos. Habitualmente se utilizaba un único fabricante para cada "unidad" dentro de una instalación industrial. Es importante por lo tanto conocer qué diseño de arquitectura está implantado en la instalación, si hay uno o varios y cuál es el criterio para interconectar la red industrial con la red corporativa.

Por ejemplo, el estándar ISA99/IEC62443 establece unos criterios que denomina "zonas y conductos" que se representan en la figura:

Ilustración 4: Zonas y Conductos según ISA/IEC 62443

Este diseño coincide en gran parte con el establecido en los años 90 por la universidad norte-americana de Purdue [21]:

Arquitectura de referencia PERA
(The Purdue enterprise reference architecture)

Ilustración 5: Arquitectura PURDUE

Hay una variante actualizada de la misma en la que se adapta al esquema NIST 800-82:

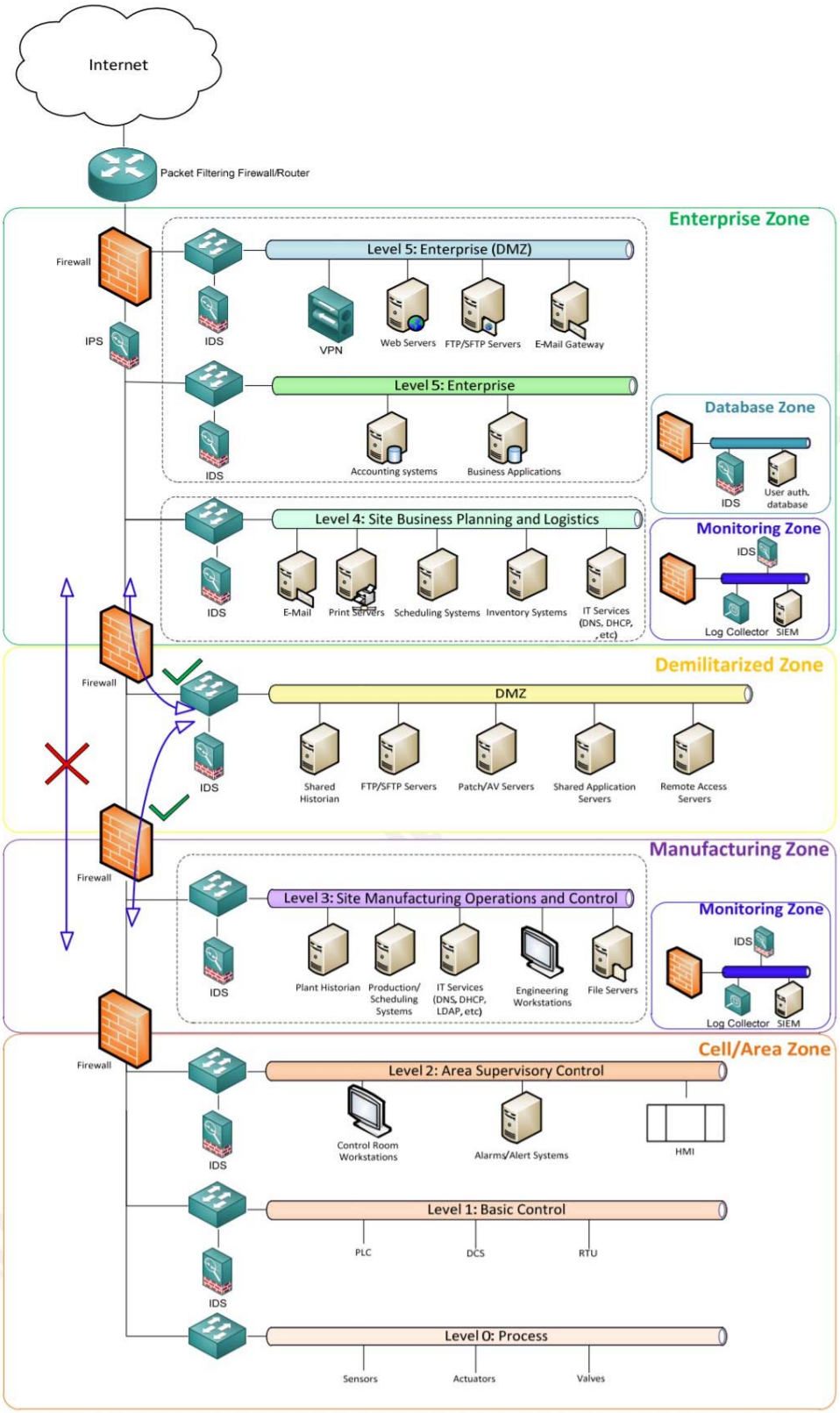

Ilustración 6: Arquitectura PURDUE adaptada al esquema NIST 800-82

Pueden encontrarse esquemas de arquitectura similares en todos los grandes fabricantes de sistemas industriales (Honeywell, Dupont, Rockwell, Siemens, etc…). Estos esquemas han evolucionado desde unos iniciales con redes de control de procesos propietarias y con escasa conectividad con el entorno corporativo, hasta las complejas redes actuales que son, en su mayoría, variantes de las descritas anteriormente. Y lo mismo ha ocurrido con los protocolos de comunicaciones de estas redes, que inicialmente eran propietarios (normalmente deterministas) y han pasado al estándar TCP/IP.

Como puede observarse, en todos los casos existe al menos una capa intermedia entre la zona de control industrial y la red corporativa, a veces hay dos o más. Lo que se pretende con estas arquitecturas, reiteramos, es que el software malicioso no pueda propagarse libremente desde una zona a otra, puesto que los accesos no son directos y se utilizan equipos especiales para proteger el tráfico. También se limita el alcance de aquellos accesos dirigidos manualmente y que pretenden explorar la red industrial con objeto de localizar vulnerabilidades y preparar ulteriores ataques. Ambos casos, “automáticos” y “dirigidos por humanos”, se ven muy dificultados por estas arquitecturas.

Los puntos de interconexión son únicos en cada capa y están fortalecidos, para ello normalmente se incluye un firewall con IPS/IDS y unas listas de acceso muy restringidas. Desde un equipo de esa zona, si existe autorización, se establece un conducto a otro equipo de la zona siguiente, de forma que las zonas están comunicadas por conductos que están a su vez muy vigilados.

Aunque con estas arquitecturas no se elimina el riesgo de ataques externos a la red industrial, se limitan notablemente, por lo que es muy importante identificar en la auditoría si existe una arquitectura similar a la descrita, su diseño e implementación y cuáles son sus posibles deficiencias.

5.2 Controles

El siguiente paso en el diseño de un modelo de control es la elaboración de los controles, en base a los riesgos. Dado que los riesgos son muy comunes en los sistemas industriales, los estándares que hemos mencionado proponen unos controles de propósito general.

5.2.1 ISA/IEC 62443

Por ejemplo, ISA/IEC62443 [22] [23] define siete bloques (detallados en el Anexo 1):

Nº	Abrv.	Descripción
1	**IAC**	Controles de Identificación y Autenticación
2	**UC**	Control de Uso
3	**SI**	Integridad del Sistema
4	**DC**	Confidencialidad de los Datos
5	**RDF**	Flujo de Datos Restringido
6	**TRE**	Tiempo de Respuesta a Eventos
7	**DR**	Disponibilidad de Recursos

Ilustración 7: Arquitectura PURDUE adaptada al esquema NIST 800-82

5.2.2 NIST Framework

Por su parte el estándar NIST [24] establece 5 componentes de su Framework (detallados en el Anexo 2):

ID	**Identificar**	Gestión de activos
		Entorno de negocio
		Gobernanza
		Evaluación de riesgos
		Gestión de riesgos
		Gestión de riesgos de la cadena de suministro
PR	**Proteger**	Gestión de identidades y control de acceso
		Concienciación y formación
		Seguridad del dato
		Procesos de protección de la información y procedimientos
		Mantenimiento
		Tecnologías de protección
DE	**Detectar**	Anomalías y eventos
		Monitorización continua de la seguridad
		Procesos de detección
RS	**Responder**	Planificación de la respuesta
		Comunicaciones
		Análisis
		Mitigación
		Mejoras
RC	**Recuperar**	Planificación de la recuperación
		Mejoras
		Comunicaciones

Ilustración 8: Controles NIST

5.2.3 CIS

Por su parte CIS [25] ("Center for Internet Security") propone todo un conjunto de 171 sub-controles alrededor de los siguientes 20 controles principales. (detallados en el Anexo 3):

Nº	Descripción
1	Inventario de Dispositivos Autorizados y No Autorizados
2	Inventario de Software Autorizado y No Autorizado
3	Configuraciones seguras para hardware y software
4	Evaluación continua de la vulnerabilidad y remediación
5	Uso controlado de privilegios administrativos.
6	Mantenimiento. vigilancia y análisis de los registros de auditoría
7	Protección del correo electrónico y del navegador web
8	Defensa contra el *malware*
9	Limitación y control de puertos de red.
10	Capacidad de recuperación de datos
11	Configuraciones seguras para dispositivos de red
12	Protección perimetral
13	Protección del dato
14	Acceso controlado basado en la necesidad de saber
15	Control del acceso inalámbrico
16	Seguimiento y control de cuentas.
17	Evaluación de habilidades de seguridad y capacitación apropiada
18	Seguridad del software de aplicación
19	Respuesta y gestión de incidentes
20	Pruebas de penetración y ejercicios *RED TEAM*

***Ilustración 9**: Controles CIS*

5.3 Otros modelos de control

Existen otros muchos modelos de control que pueden inspirar el que finalmente se haya decidido implantar en la instalación industrial objeto de auditoría. Algunos trascienden el enfoque clásico de riesgos-controles e intentan hacer una mejor identificación de riesgos, que es el punto más delicado del esquema mostrado hasta aquí.

Entre ellos podemos mencionar el modelo CEE del Laboratorio Nacional Idaho [(9)] en el que se muestra una novedosa aproximación para reforzar aquellos puntos más delicados de una instalación industrial. La denominan "Ingeniería ciber-informada dirigida por las consecuencias" con el acrónimo CEE ("*Consequence-Driven, Cyber-Informed Engineering*").

Consideran que solo algunos elementos de la instalación concentran la mayoría de las consecuencias catastróficas, con lo que proponen mitigar esos riesgos con soluciones muy robustas y en ocasiones analógicas, fuera del ámbito digital, en definitiva, siguiendo la premisa "piensa como un *hacker* y actúa como un ingeniero"

Se basa en los siguientes 4 puntos:

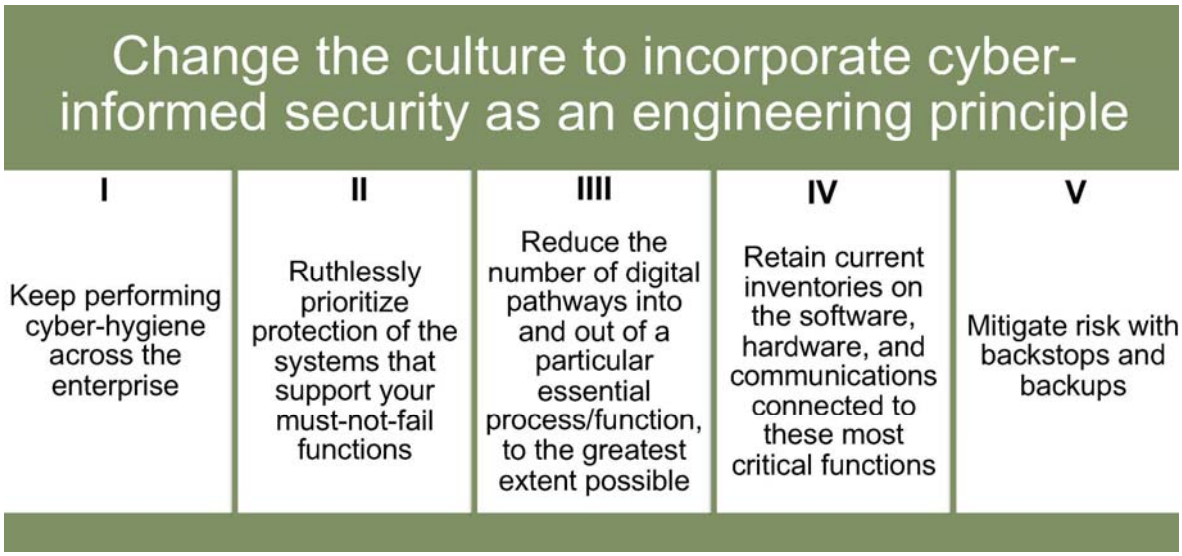

Ilustración 10: Metodología CEE del INL

6 Despliegue de un modelo de control para instalaciones industriales

Una vez establecido el modelo de control, es importante analizar el riesgo y el impacto que pueden llegar a tener en las operaciones de la organización la implantación de dichos controles. Es crítico que la forma en que el modelo de control se incluya en los procesos productivos no les afecte en su desempeño, ni implique riesgos añadidos. Es por ello recomendable hacerlo de forma planificada y ordenada. La creación de un plan de despliegue de controles es de vital importancia para que el objetivo de los mismos se consiga. El plan debería incluir entre otros aspectos el alcance (sistemas cubiertos), el presupuesto, las responsabilidades, los recursos, los riesgos, las dependencias, y un calendario. En este sentido el auditor de seguridad debería verificar la existencia y el seguimiento de este plan de despliegue.

Un factor importante que influye en la planificación del despliegue del modelo de control es si el sistema productivo es nuevo o si el sistema lleva a pleno rendimiento cierto tiempo y debido a sus requerimientos de disponibilidad o a la antigüedad de sus componentes no sea sencilla la introducción de los controles. En el primer caso los controles de seguridad se pueden observar como requerimientos del propio sistema, y se despliegan a lo largo del propio ciclo de desarrollo del sistema productivo. Sin embargo, en los sistemas antiguos los controles se introducen para mitigar un conjunto de riesgos identificados y es probable que ya existan controles anteriores.

6.1 Enfoques de despliegue

Existen dos principales enfoques de despliegue de controles. El primero de ellos se basa en aplicar el modelo de control completo en un subsistema piloto en el que el análisis de impacto de la aplicación de los controles haya resultado asumible. Una vez probado el modelo se exporta al resto de los sistemas de control industrial.

El segundo enfoque consiste en introducir progresivamente los controles mediante una hoja de ruta. De esta forma se empieza por los controles con menos impacto potencial en el proceso productivo y se va ampliando hasta su completa implantación. A la hora de establecer la secuencia de la implantación de los controles es interesante tener en cuenta la priorización de los controles "*quick fix*", ya que proporcionan soluciones rápidas a bajo coste que pueden reducir significativamente el riesgo. Durante el despliegue los controles se van integrando en la operación diaria.

6.2 Fases del despliegue

Para que el plan de despliegue de controles tenga éxito es necesario que se aborden los siguientes pasos:

- Comunicación del modelo de controles y el plan de despliegue a la dirección de la entidad para su validación y aprobación para poder iniciar las actividades.
- Identificación de responsabilidades dentro del proyecto.
- Concienciación en ciberseguridad y formación del modelo de control a las partes interesadas para que colaboren en el plan de despliegue.
- Introducción progresiva de los controles del modelo mediante la hoja de ruta.
- Establecimiento de métricas e indicadores de la seguridad y de la producción para valorar la seguridad, así como el efecto de los controles sobre la misma.
- Monitorización de los indicadores con el objeto de detectar sus desviaciones y ajustarlos en consecuencia.

El papel del auditor estará principalmente en verificar que las medidas de los indicadores de seguridad se encuentran en el rango previsto, y que los indicadores de producción se mantienen estables y al mismo nivel que antes de introducir los controles de seguridad.

6.3 Consideraciones de la implantación de distintos tipos de controles

Los controles organizativos tales como políticas, directrices, procedimientos, documentación, o formación son los que menos impacto van a tener sobre los procesos productivos, y por ello se pueden aplicar inmediatamente después de aprobar el plan de despliegue.

Entre ellos cabe destacar el inventariado de activos (equipamiento hardware y software) ya que permite visibilizar el alcance del sistema global y definir el plan de seguridad. Aunque existen herramientas de descubrimiento de activos también para redes OT, este control se puede llevar a cabo con una simple hoja de cálculo o herramientas de inventario que no interactúen con el proceso industrial. Sin embargo, controles como la defensa contra el malware, o la configuración segura de los dispositivos de red, y la aplicación de actualizaciones software, que se aplican directamente sobre los sistemas de control, requieren de un proceso de pruebas de regresión y de un procedimiento de gestión del cambio para garantizar la disponibilidad y la fiabilidad para que el sistema no se vea afectado negativamente.

Nos encontramos otros controles que introducen un nivel de riesgo mayor en los sistemas y redes OT, tales como las herramientas automatizadas que escanean las vulnerabilidades software, o que realizan inventariados de cuentas, servicios y puertos abiertos. En estos casos hay que elevar las precauciones, configurando las herramientas de forma que sean lo menos intrusivas posible (modo pasivo), y aplicarlas en ventanas de tiempo no críticas para el proceso.

En relación a la protección de la confidencialidad de los datos, si bien es cierto que los sistemas de control industrial de forma general no manejan datos sensibles en el sentido tradicional (datos personales, números de tarjetas de crédito); nos encontramos que en ciertos entornos se manejan datos confidenciales tales como las recetas o fórmulas industriales, que están sujetas a la ley de patentes.

Ante esta situación, aunque en un entorno IT se aplicaría un control criptográfico, en los sistemas de control industrial no es siempre aplicable dada la limitación de capacidad de cálculo de los dispositivos; y en cualquier caso del retardo que añadiría al proceso. Por esta razón, es más adecuado el uso de herramientas pasivas como las de detección de anomalías de protocolos, y complementarlo con análisis de tráfico de red periódicos para detectar fugas de información.

Un control que se suele emplear en los entornos de TI, y que no se aplica en los sistemas de control industrial salvo en bancos de pruebas o escenarios no productivos, son las pruebas de penetración y los ejercicios de “*Red Team*”. Este tipo de control puede provocar tiempos de inactividad, destrucción y lesiones que reducen la seguridad o el rendimiento del sistema probado.

Por otro lado, se observa que los controles de seguridad física suelen estar implantados antes que los de ciberseguridad. Pero en el caso de instalaciones que no los tengan, no supone demasiado esfuerzo implantarlos porque no suelen afectar directamente al proceso productivo. De alguna forma son controles que se aplican alrededor del proceso, tales como sistemas de detección de incendios, cámaras de vigilancia, barreras físicas, o puestos de recepción de visitas. No obstante, hay que tener presente que el despliegue de este tipo de controles a menudo está sujeto a requisitos ambientales, y regulatorios que deberán ser estudiados previamente.

Como se puede observar en estos ejemplos de controles, en las auditorías de seguridad de los sistemas de control industrial e infraestructuras críticas, es fundamental identificar no sólo qué controles se están aplicando, sino también su idoneidad para proteger los activos objetivo, y cómo se están aplicando en cada escenario concreto, ya que el hecho de incluir los propios controles supone un riesgo adicional al desempeño del proceso industrial, y en ocasiones incluso a la seguridad física.

7 Las Infraestructuras críticas y sus obligaciones específicas

En virtud de la Ley 8/2011 [3], que nos referiremos como LPIC, cuando una infraestructura es designada como crítica por el CNPIC y se lo comunica al operador (que pasa a ser entonces un operador crítico), este nombramiento conlleva una serie de obligaciones para el operador crítico responsable de esta infraestructura.

Los Operadores Críticos son las Entidades u organismos responsables de las inversiones, mantenimiento u operación de una instalación, red, sistema, o equipo físico o de tecnología de la información designada como infraestructura crítica.

Según la LPIC, estos Operadores Críticos deben ser designados como tales una vez que el CNPIC tiene conformado el Catálogo Nacional de Infraestructuras Estratégicas.

Es de prever que los operadores críticos sean los **mayores proveedores de servicios esenciales al ciudadano**. Por ejemplo, en el sector de distribución del agua, en Madrid será el Canal de Isabel II, en Barcelona será Aguas de Barcelona S.A, etc. En alimentación en Madrid será Mercamadrid y los supermercados más grandes como Carrefour o Alcampo. Si hablamos de transportes aéreos serán Aena, Enaire y las grandes compañías aéreas que operan en los principales aeropuertos españoles como Iberia, Ryanair, Air Europa, Air France, etc. Si hablamos de transporte terrestre uno podría ser ALSA, si hablamos de suministros energéticos serán Naturgy, Iberdrola, etc.

Posteriormente, en el año 2016, conscientes de la importancia que las TIC tenían para dar soporte a cualquier infraestructura crítica y que, de por sí, las TIC constituían el pilar de cualquier nación, la Directiva NIS (Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión) [12] expuso la necesidad también de controlar a los Operadores Esenciales que son aquellos operadores críticos (según la LPIC) cuyas actividades se sustentan en las TIC.

En España la Directiva NIS se traspuso mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información [26]**.**

- Ámbito de aplicación: Servicios esenciales para la comunidad y Servicios Digitales que precisen de las TIC (normalmente todos, ya que los procesos industriales cada vez interconectan a IT las OT).
- Sujeto a esta ley:
  - Operadores de Servicios Esenciales: Se definen en la Ley 8/2011, de 28 de abril (Ley PIC). (Está previsto que se complete a finales del 2019 el catálogo).
  - Prestadores de Servicios Digitales: Los definidos en la LSSI, pero no todos, sólo los que se refieran a comercio electrónico, motores de búsqueda on line y servicios de Cloud. Se excluyen las micro empresas.
- Autoridades supervisoras: CNPIC para los del ámbito Ley PIC. Resto de operadores: Autoridad sectorial. Secretaría de Estado de Avance Digital para los prestadores de Servicios. Digitales.
- Framework: El artículo 8 hace referencia al marco de la Estrategia Nacional de Ciberseguridad.
- **Medidas importantes a adoptar tanto por los Operadores de Servicios Esenciales como los Prestadores de Servicios Digitales (además de las derivadas de la LPIC): Designar un CISO, implantar un SGSI y notificar incidentes de seguridad al supervisor.**

A continuación, se presentan las obligaciones que esto conlleva para los operadores y en el posterior apartado para los responsables de las Infraestructuras.

7.1 Obligaciones para los operadores críticos

Obligaciones indicadas en la Ley 8/2011 y se marcan en negrita los conceptos más relevantes:

Artículo 13:

a) Asesorar técnicamente al Ministerio del Interior, a través del CNPIC, en la **valoración de las infraestructuras propias** que se aporten al Catálogo**, actualizando los datos disponibles con una periodicidad anual** y, en todo caso, a requerimiento del citado Ministerio.
b) Colaborar, en su caso, con el Grupo de Trabajo en la elaboración de los **Planes Estratégicos Sectoriale**s y en la realización de los **análisis de riesgos** sobre los sectores estratégicos donde se encuentren incluidos.
c) Elaborar el **Plan de Seguridad del Operador** en los términos y con los contenidos que se determinen reglamentariamente.
d) Elaborar, según se disponga reglamentariamente, un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas en el Catálogo.
e) Designar a un **Responsable de Seguridad** y Enlace en los términos de la presente Ley.
f) Designar a un **Delegado de Seguridad por cada una de sus infraestructuras consideradas Críticas o Críticas Europeas** por el Ministerio del Interior, comunicando su designación a los órganos correspondientes.
g) Facilitar las **inspeccione**s que las autoridades competentes lleven a cabo para verificar el cumplimiento de la normativa sectorial.

De este artículo se infiere que:

1) **Hay que mantener los datos actualizados sobre las infraestructuras críticas propias. Pero la cuestión es, ¿qué datos del catálogo hay que actualizar?**
   El artículo 2 de la LPIC establece que el Catálogo debe contener la información completa, actualizada, contrastada e informáticamente sistematizada relativa a las características específicas de cada una de las infraestructuras estratégicas existentes en el territorio nacional
2) **Planes Estratégicos Sectoriales. ¿Qué son?**
3) **Planes de Protección Específicos. ¿Qué contienen?**
4) **Responsable de Seguridad según la LPIC no es un CISO, sino un Director de Seguridad**
   Artículo 16. El Responsable de Seguridad y Enlace
   Los operadores críticos nombrarán y comunicarán al Ministerio del Interior un Responsable de Seguridad y Enlace con la Administración en el plazo que reglamentariamente se establezca.

   *2. En todo caso, el Responsable de Seguridad y Enlace designado deberá contar con la habilitación de Director de Seguridad expedida por el Ministerio del Interior según lo previsto en la normativa de seguridad privada o con la habilitación equivalente, según su normativa específica***.**

   3. Las funciones específicas del Responsable de Seguridad y Enlace serán las previstas reglamentariamente.
5) **El Delegado de Seguridad por cada una de las infraestructuras críticas será un Director de Seguridad.**
6) **Facilitar inspecciones: Proveer de un punto de contacto y expertos suficiente.**

RESUMEN DE ACCIONES

1) Elaboración del Plan de Seguridad del Operador
2) Elaboración del Plan de Protección Específico por cada infraestructura seleccionada
3) Colaboración en el Plan Sectorial del Operador
4) Implantar las medidas de protección previstas en los planes elaborados
5) Tras realizar el Análisis de Riesgos adecuado tanto en conjunto como por Infraestructura Crítica, es preciso analizar los resultados y proponer una serie de medidas correctoras para rebajar el nivel de riesgo hasta unos niveles aceptables.
6) Este Plan de actuación se debe incluir en el Plan Director de Seguridad. De hecho, debería existir al más alto nivel para que tenga el efecto buscado.
7) Acciones específicas para Sistemas SCADA/Industrial OT
8) Como marco de referencia Aplicaremos la guía de referencia del CCN además de la del NIST

7.1.1 Plan de Seguridad del Operador

Para la elaboración del PSO seguiremos la Guía de Contenidos Mínimos para su estructuración. Para su análisis y recomendaciones usaremos la Guía de Buenas Prácticas.*(Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos*) [28]

1) En primer lugar, el PSO se debe realizar en formato digital y custodiarlo en la zona acondicionada para uso de la información con el grado de Difusión Limita.
2) El PSO debe ser actualizado cuando existan cambios organizativos/estructurales que lo justifiquen y por defecto se revisará cada dos años.
3) Se recomienda elaborar antes de su realización la Norma de Clasificación de la Información y contar entre sus criterios el de sensibilidad respecto a la LPIC.
4) Es preciso elaborar dentro del PSO la referencia a una Política de Seguridad que debe estar refrendada al más alto nivel. Será por tanto preciso elaborar y negociar dicha política al nivel del Comité de Dirección. La Política de Seguridad debe incluir como mínimo:
    a. Objetivo
    b. Ámbito o Alcance (a poder ser lo más generalista posible)
    c. Compromiso expreso de la Alta Dirección (debe constar por escrito)
    d. Integralidad de la función de seguridad (física, lógica, operacional).
    e. Cláusula de compromiso de revisión periódica.

5) Marco de Gobierno: Organigrama donde se identifiquen que departamentos/grupos se encargan de la función de seguridad. Marcar dónde se ubican. Comités u órganos de decisión. Contacto del Responsable de Seguridad y de los Delegados de Seguridad por Infraestructura Crítica. Informar a las Delegaciones del Gobierno y CCAA los contactos de los Delegados de Seguridad.
6) Plan de Formación: A este respecto hay que hacer constar en el PSO el **Plan de Formación del personal directamente implicado en la operación de las Infraestructuras Críticas** al respecto de los siguientes puntos:
    a. Capacidad de comprensión de la seguridad integral (física y lógica).
    b. Capacidad de comprensión de la autoprotección.
    c. Capacidad de comprensión de la seguridad del medio ambiente.
    d. Habilidades organizativas y de comunicación

    Para el resto del personal bastará con incluir alguna acción de concienciación en el Plan de Formación Anual.

7) En el PSO hay que indicar qué **modelo de Gestión de los diferentes aspectos de la Seguridad** se está siguiendo: En Seguridad Lógica se sigue el modelo de la ISO 27001 [29], con los controles de seguridad de la ISO27002. En Seguridad Física y Operativa presumiblemente se debe seguir la ISO 31000.
8) **Servicios Esenciales e Inventarios:** En el PSO hay que detallar el listado de los servicios esenciales del Operador Crítico. Hay que tener en cuenta que un Servicio Esencial es aquel servicio proporcionado por el Operador Crítico, que es necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, además del eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas

7.2 Obligaciones concretas para las Infraestructuras Críticas

Los Planes de Protección Específicos se elaboran por cada Infraestructura Crítica Específica. La información que debería ir en el PPE sería la siguiente:

1) Organización de la seguridad.
    a. En el PPE se debe constar quién son los Delegados de Seguridad para la infraestructura
    b. Además, debe constar con quién se debe coordinar el plan
2) Descripción de la infraestructura.
3) Resultado del análisis de riesgos:
    a. Medidas de seguridad (tanto las existentes como las que sea necesario implementar) permanentes, temporales y graduales para las diferentes tipologías de activos a proteger y según los distintos niveles de amenaza declarados a nivel nacional.
    b. Plan de acción propuesto (por activo).
4) **Protección de la Información y Revisión del PPE**. Al igual que el PSO, el PPE debe revisarse cada dos años y siempre que haya cambios significados en los activos que componen la infraestructura o en los datos proporcionados. Tiene una clasificación de Difusión Limitada y como tal debe protegerse (ver consideraciones para el PSO).
5) Cómo aplica la Política de Seguridad (el PSO).
6) Cómo aplica el análisis de riesgos (misma metodología, herramientas, etc.)
7) Con quién se deben coordinar de las Fuerzas y Cuerpos de Seguridad del Estado, Delegación del Gobierno, etc.
8) Quién es el responsable de la aprobación del PPE.
9) Quién es el responsable de su revisión y actualización si fuera necesario.
10) Cuáles son los pasos para su aprobación y a quién se comunican las modificaciones en el plan (incluyendo cualquier tercero afectado por dichas modificaciones).
11) Un apartado importante del PPE es el de describir la información relevante de la Infraestructura, sobre la que luego se detallará el análisis de riesgos. En particular, hay que incorporar al PPE la siguiente información:
    a. Información de carácter estratégico.
    b. Descripción del servicio esencial que soporta y ámbito geográfico del mismo
    c. Relación con otras posibles infraestructuras necesarias para la prestación de ese servicio esencial.
        i. Del mismo sector
        ii. De otros sectores
    d. Descripción de sus funciones y de su relación con los servicios esenciales soportados
12) Información de carácter general.
    a. Denominación y tipo de instalación (ahí ya la información general).

b. Descripción general de la infraestructura a proteger.

c. Propiedad y gestión de la Infraestructura Crítica.

13) Localización física y estructura de la infraestructura a proteger.
   a. Ubicación geográfica de la infraestructura.
   b. Planos generales de la infraestructura con referencia a todos los elementos, así como su ubicación relativa y absoluta.
   c. Fotografías relevantes de la infraestructura y los elementos que la componen.
   d. Componentes (Edificios/Instalaciones/etc.).

14) Sistemas TIC y arquitectura.
   a. Mapa de red y comunicaciones.
   b. Mapa de sistemas y servicios.
   c. Sistemas de control.

7.3 Medidas establecidas por el Esquema Nacional de Seguridad

Para aquellas infraestructuras albergadas o usando sistemas de información que estén en el ámbito del Esquema Nacional de Seguridad [30] (El Sector de Administración), se consideran las medidas del ENS para la categoría ALTA, con la dimensión de Disponibilidad respondiendo a ese nivel.

Entre dichas medidas están las siguientes:

- **Op.pl.1 ++: Obligación de la realización de un Análisis de Riesgos formal**, con metodología de análisis de riesgos y una herramienta adecuada para ello. En la AGE la metodología es MAGERIT y la herramienta PILAR, que no son obligatorias sino recomendables.
- **Op.pl.2 ++: Obligación de abordar una arquitectura de seguridad de los sistemas** considerando la documentación de todos sus componentes, la arquitectura de red, etc.
- **Op.pl.5 : Los componentes del sistema deben estar certificados formalmente.** Esto supone la certificación de los componentes o la adquisición de componentes certificados siguiendo un esquema formal de certificación (Common Criteria o similar).
- **Op.exp.9, mp.com.9, mp.per.9, mp. eq.9, mp.if.9, mp.s.9, : Medios alternativos.** Se debe contar con medios alternativos para garantizar las operaciones del sistema (CPD, redes, equipamiento, personal, software, etc.)
- **Op.cont.1, Op.cont.2, Op.cont.3: Continuidad de Negocio**. Se debe contar con un Análisis de Impacto, un Plan de Continuidad de Negocio y Pruebas periódicas.

8 Auditando la ciberseguridad en instalaciones industriales /infraestructuras críticas

8.1 El inicio de la Planificación de la Auditoria

Podemos identificar dos diferentes aproximaciones a la hora de realizar la planificación de la Auditoria. En algunas organizaciones podríamos encontrarnos con Departamentos de Auditoria, con su propio estatuto de auditoría interna, un documento formal que define el propósito y la autoridad de la auditoría interna. Este estatuto inicialmente es la mejor manera de acordar y describir cómo la auditoría interna proporcionará valor a la organización, la naturaleza de los servicios que prestará y el enfoque o énfasis específico requerido de Auditoría interna para ayudar a la organización a alcanzar sus objetivos.

Tener este estatuto también suele establecer la posición de la actividad de auditoría interna dentro del organización, incluyendo las líneas de reporte del jefe de auditoría interna, autorizando el acceso a registros, personal y propiedades físicas relevantes para el desempeño de los diferentes compromisos. También define el alcance de las actividades de auditoría interna, de manera que es un punto de referencia para medir su efectividad. Consideramos necesario incluir en este estatuto las características requeridas para las auditorias de sistemas.

En este caso, abogamos por incluir dentro de este estatuto interno algunos criterios básicos a la hora de planificar las diferentes auditorias de sistemas como la necesidad de realizar planes anuales de Auditoria de Sistemas, tal y como se recomienda en las diferentes referencias sobre ciberseguridad en infraestructuras críticas y sistemas industriales. Además, recomendamos incluir los diferentes roles y responsabilidades que participaran durante la planificación y ejecución de las auditorias de sistemas y las diferentes líneas de reporte. La revisión periódica de este estatuto es también necesaria para garantizar que sigue siendo relevante para las necesidades de la organización. Al menos, debería incluir la Misión de Auditoría Interna, los Principios Básicos para la Práctica Profesional de la Auditoría Interna, El Código de ética, los estándares, y la definición de auditoría interna.

En aquellas organizaciones carentes de este tipo de Departamentos, será necesario recibir una Carta de Encargo con la Auditoria o disponer de Políticas y Directivas en lo que se refiere a la Auditoria Interna de Sistemas. Abogamos por esto último en el caso de las Infraestructuras Criticas, incluyendo una Directiva Especifica sobre Auditoria de Sistemas que permita determinar todas las cuestiones que se abordan en un estatuto de auditoria interna, al menos para la parte de Auditoria de Sistemas.

Existen otras organizaciones que, siendo carentes de Departamentos de Auditoria Interna de Sistemas o/y de Políticas y Directivas específicas sobre Auditoria Interna de Sistemas, delegan esta actividad en terceros, bien con procesos de contratación de auditorías o bien con acuerdos específicos para llevar a cabo esta actividad. En el caso de Infraestructuras Criticas, por su especial naturaleza, abogamos por la identificación, al menos, de estas Políticas y Directivas, pese a que desde el punto de vista organizativo se decida por razones de negocio delegar esta actividad en un tercero. Estas Políticas y Directivas permitirán crear un marco común dentro de la organización que soporte de manera coherente y alineada al negocio la planificación y posterior ejecución de las auditorias.

Una vez identificadas las Políticas y Directivas asociadas, o los contenidos específicos del Estatuto de Auditoria, el responsable de auditoria interna de sistemas tendrá bajo su responsabilidad la planificación de las auditorias.

8.2 La Pre-Planificación de la Auditoria

El proceso de Planificación de una Auditoria de Sistemas es un proceso bastante complejo, sobre todo en el caso de Infraestructuras Criticas o Sistemas Complejos. Las recomendaciones de todos los estándares y guías es la preparación previa de un una Pre-Plan de Auditoria de Sistemas. Una de las razones esgrimidas por la mayor parte de los Auditores y entidades asociadas a la planificación de las auditorias es la obtención de recursos para la propia planificación. En muchos casos son necesarios recursos específicos para planificar una auditoria compleja. Sin un Pre-Plan aprobado será más complicado contar con estos recursos necesarios para planificar adecuadamente la auditoria.

El proceso de Auditoria de Sistemas se esquematiza en la figura siguiente, donde partimos de un estatuto de auditoria o carta de encargo, pre-planificamos la auditoria, realizamos el plan y posteriormente ejecutamos la auditoria. El proceso de monitorización continua es fundamental para garantizar el correcto seguimiento de la auditoria y su mejora continua.

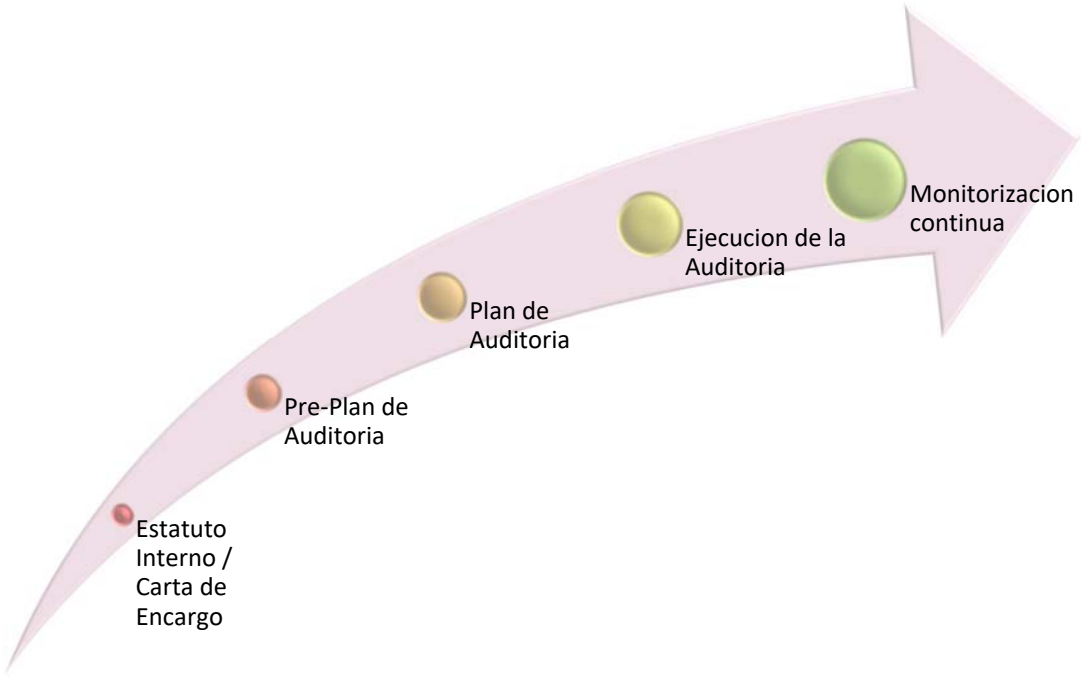

Ilustración 11: - Proceso de Auditoria de Sistemas

Existen varios aspectos importantes a la hora de desarrollar el Pre-Plan de Auditoria de Sistemas para nuestras Infraestructuras Criticas o Sistemas Industriales. Consideramos que, al menos, deberían cubrirse los siguientes aspectos en el Pre-Plan que recomendamos, al menos, actualizar por periodos trianuales, para enmarcar los diferentes planes derivados de auditoria con carácter anual.

Ilustración 12**:** *Plan de Auditoría de Sistemas*

En primer lugar, es necesario elaborar los objetivos principales de las auditorias de sistemas que se van a llevar a cabo. Posteriormente recomendamos realizar una evaluación inicial de los riesgos. Las normas de auditoría ISACA contienen los principios básicos y los procedimientos esenciales de Auditoria de Sistemas, en ellos se destaca que el auditor de sistemas utilice una técnica o un enfoque de evaluación de riesgos adecuado para desarrollar el plan de auditoría general de sistemas. En el caso de infraestructuras críticas y sistemas industriales recomendamos la realización de esta evaluación inicial de los riesgos al objeto de determinar las diferentes prioridades para la asignación efectiva de recursos de auditoría con carácter trianual. A la hora de realizar las posteriores auditorias con carácter anual el auditor, como analizaremos posteriormente, identificará y evaluará los riesgos relevantes para el área bajo revisión especifica.

Este análisis de riesgos inicial nos permitirá programar los diferentes alcances de las auditorias anuales, considerando las diferentes prioridades y criticidad de los activos identificados durante la evaluación de los riesgos. Como se recomienda por las guías de la ISACA, los ejercicios de evaluación de riesgos para facilitar el desarrollo del plan de Auditoria de Sistemas deben realizarse y documentarse al menos anualmente. En nuestro caso abogamos por la realización de un ejercicio de evaluación de riesgos trianual para el Pre-Plan de auditoria y una actualización del mismo de forma específica para las correspondientes auditorias anuales, enfocado a los activos bajo revisión detallada.

El uso de esta evaluación de riesgos durante el desarrollo del Pre-Plan permitirá al auditor realizar una cuantificación inicial y obtener una justificación sobre la cantidad de recursos de Auditoria de Sistemas necesarios para completar los diferentes planes anuales.

Es importante mencionar que esta evaluación de riesgos se deberá realizar de forma independiente por parte del auditor para garantizar la independencia del proceso global de auditoria. Los procesos de evaluación de riesgos pueden ser elaborados por la organización desde diferentes ámbitos: a nivel de negocio, financiero, de programas, etc. Si bien recomendamos usar un marco común a nivel organizativo para la evaluación de riesgos, en el caso de las auditorias el criterio debe establecerlo el propio auditor para garantizar su independencia.

Posteriormente a la evaluación de los riesgos recomendamos realizar un análisis inicial de las referencias críticas que serán consideradas durante el desarrollo de los diferentes planes de auditoria. Al menos deberían identificarse las siguientes referencias que consideramos más importantes:

1. **Aspectos regulatorios** como la GDPR y la regulación específica sobre Infraestructuras criticas ya analizada en otras secciones de este documento. Recomendamos realizar un listado de estas regulaciones que consideramos aplicables a nuestra auditoria, e incluso que el auditor mantenga estas regulaciones como evidencias relevantes durante el proceso de ejecución de la auditoria.

2. **Políticas, estrategias y Directivas organizacionales.** El estatuto de auditoria interna, las políticas de seguridad de la información y de auditoria interna y de sistemas, las estrategias corporativas, especialmente sobre tecnologías de la información y comunicaciones (TIC) y aspectos relevantes de recursos humanos que puedan afectar al mantenimiento o desarrollo de infraestructuras TIC. Recomendamos realizar un listado de estas políticas, estrategias y directivas organizaciones que consideramos aplicables a nuestra auditoria e incluso que el auditor mantenga estas regulaciones como evidencias relevantes durante el proceso de ejecución de la auditoria.

3. **Infraestructuras** de tecnologías de la información bajo responsabilidad de la organización. Deberían, al menos, identificarse los Centros de Procesamiento de la Información principales y las instalaciones con terminales de usuario. Recomendamos realizar un listado de estas instalaciones que consideramos aplicables a nuestra auditoria e incluso que el auditor mantenga este listado durante el proceso de ejecución de la auditoria. No se requiere mantener complejas bases de datos de activos de la información como una CMDB o un inventario de activos dentro de la elaboración del Pre-Plan, pues es un proceso complejo que requiere de considerables recursos, pero si al menos una identificación de las instalaciones principales.

4. **Interfaces externos** con otras organizaciones con las que se intercambie información, incluyendo los diferentes proveedores. Deberían, al menos, identificarse que tipos de entidades son y los principales puntos de contacto. También abogamos por identificar todos los acuerdos de alto nivel que se tengan con este tipo de entidades. Recomendamos realizar un listado de estas entidades y acuerdos, e incluso que el auditor mantenga este listado durante el proceso de ejecución de la auditoria.

Una vez identificadas las referencias más críticas y realizada la evaluación de los riesgos procederemos a especificar el alcance de nuestra auditoria. A la hora de realizar la planificación de una auditoria uno de los aspectos más complejos es la identificación clara del alcance. En el Pre-Plan recomendamos realizar una política de máximos incluyendo todas aquellas infraestructuras que consideremos prioritarias y se puede realizar un proceso incremental de tal forma que con una periodicidad trianual se pueda cubrir casi todo el alcance organizativo. Recomendamos, además, identificar este alcance teniendo en cuenta las referencias críticas: infraestructuras, aspectos regulatorios e interfaces.

A continuación, procederemos con la elaboración del cronograma de las diferentes auditorias anuales, y la descripción de los diferentes hitos principales de las mismas. Posteriormente, recomendamos identificar los recursos críticos necesarios para la ejecución de las auditorias, incluyendo recursos humanos, herramientas y sistemas necesarios para su elaboración. En el Pre-Plan consideramos prioritario, además, la identificación de los recursos necesarios para planificar y mantener las auditorias. Contar con herramientas comunes como CAATS o procedimientos y herramientas específicos para realizar análisis de vulnerabilidades o *pentests* serán de gran valor a la hora de realizar nuestras auditorias. Por esa razón, el análisis de estos recursos es esencial.

Otro aspecto importante dentro del Pre-Plan es el Plan de comunicación de la auditoria, donde al menos recomendamos identificar la lista inicial de distribución y el formato de la presentación de las diferentes auditorias y sus entregables asociados. Por último, otro aspecto que consideramos importante dentro de la elaboración del Pre-Plan de Auditoria de Sistemas es el enfoque que vamos a dar a la auditoria continua. En este punto deberíamos identificar como los procesos de auditoria continua contribuyen o interactúan con el resto de procesos del negocio relacionados con la gestión TIC o la gestión de seguridad de la información. Aspectos como la gestión de incidentes de seguridad y la planificación de la continuidad de negocio deberían identificarse y elaborar los diferentes interfaces entre el proceso continuo de auditoria y otros procesos críticos del negocio relacionados con las TIC.

8.3 La Planificación de la Auditoria

Una vez consolidado el Pre-Plan de auditoria y con los recursos asignados para la elaboración de los diferentes Planes anuales de Auditoria de Sistemas, procederemos a realizar el Plan específico anual de Auditoria. Consideramos que, al menos, deberían cubrirse los siguientes aspectos en el Plan anual de Auditoria de Sistemas:

CONTEXTO Y OBJETIVOS
ALCANCE FINAL
ENFOQUE Y MÉTODO
PLANIFICACIÓN Y EQUIPO
PLAN DE COMUNICACIÓN
REFERENCIAS Y CICLO DE VIDA DE EVI-

Ilustración 13: Esquema del Plan de Auditoría

8.3.1 Contexto y Objetivos

En primer lugar, el Plan debería contextualizar la auditoria, con una breve descripción del objeto auditable, incluyendo información sobre empresa, entidad, departamento, organización, etc. No se trata de especificar en detalle el alcance de la auditoria, sino más bien en qué contexto se va a realizar la ejecución de la auditoria. Toda la información de vital importancia y alto nivel que se derive de la fase de pre-planificación de la auditoria debería incluirse en este apartado del plan, incluyendo un resumen del resto de apartados.

En segundo lugar, deberían describirse el mandato de auditoria o carta de encargo y los principales objetivos a cubrir durante la ejecución de la auditoria. Aspectos como el tipo de auditoria deberían considerarse a la hora de describir los objetivos.

8.3.2 Alcance Final de la Auditoria

Una vez clarificado el contexto en el que se mueve la auditoria, el mandato o carta de encargo y los principales objetivos, es necesario especificar en detalle el alcance final de la auditoria. Probablemente este aspecto sea de los más complejos a la hora de planificar la auditoria, pero es clave a la hora de planificar los recursos necesarios para abordarla .

Para elaborar y delimitar el alcance en detalle una de las fuentes básicas es el análisis que hemos llevado a cabo durante la pre-planificación de la auditoria, las denominadas “referencias críticas”. Esto incluye, por un lado, los aspectos regulatorios, las políticas y directivas que estarán bajo el paraguas de nuestra auditoria.

Por otro lado, debemos especificar en detalle también el conjunto de infraestructuras que están dentro de nuestro alcance y los principales roles que tienen responsabilidad de gestión de dichas infraestructuras. El análisis de roles y responsabilidades y sus aspectos relacionados como la segregación de funciones se realizarán durante el transcurso de la auditoria, no obstante, es esencial delimitar los principales roles que gestionan las infraestructuras que son objetivo de nuestra auditoria, incluyendo entidades, departamentos, organizaciones u otros roles que sean considerados de importancia.

Detallar infraestructuras en detalle puede llegar a ser una labor bastante compleja, pero al menos deberíamos identificar el conjunto de sistemas de información asociados, los servicios de negocio asociados y las instalaciones principales, incluyendo centros de procesamiento de datos y terminales de usuario final.

Si se trata de auditorías con relaciones contractuales relacionadas con diferentes empresas u otros organismos o entidades, hay que especificar en detalle los diferentes contratos que están bajo el paraguas de la auditoria. Desde un punto de vista legal y regulatorio esta actividad es crítica. En algunos casos no será sencillo este análisis, pero recomendamos encarecidamente llevarlo a cabo durante la planificación de la auditoria y reflejarlo en el plan.

Por último, tras el análisis de los interfaces llevado a cabo en la fase de pre-planificación de la auditoria, recomendamos también incluir todos los interfaces principales entre nuestras entidades, contratos e infraestructuras y el resto, de tal forma que quede bien claro la delimitación de nuestro perímetro.

8.3.3 Enfoque y método

Existe una notable diferencia entre las auditorías de diagnóstico y las de cumplimiento. En las auditorías de cumplimiento se pretende verificar que un determinado marco de control está implantado y en funcionamiento, normalmente como consecuencia de alguna regulación legal. En este caso el auditor seguirá minuciosamente el marco de control y verificará que los controles definidos se ajustan a ese marco y están efectivamente implantados siendo éste el objetivo de su informe.

Por su parte, en las auditorías de diagnóstico, la compañía pretende conocer, de forma independiente y a través de un equipo auditor, el estado de situación y los riesgos que puedan expresarse en una instalación industrial. Para ello el equipo de auditoria en su examen puede seguir algún marco de control conocido, pero no debe limitarse a él, sino extender su revisión para identificar aquellos riesgos que no se encuentren recogidos en el mapa de riesgos o no estén suficientemente cubiertos por el marco de control implantado. En este caso el informe es más extenso y tiene recomendaciones muy amplias. Como puede verse, son dos alcances muy distintos y es fundamental que quede especificado como parte de los objetivos a cubrir.

El análisis de riesgos llevado a cabo por el equipo de auditoria debe reflejarse en esta sección o parte del Plan de auditoria, incluyendo la metodología utilizada y los sistemas de soporte.

Como parte del enfoque y método recomendamos identificar todas las herramientas que se utilizan durante la auditoria, incluyendo, al menos, el siguiente conjunto de herramientas:

- Las técnicas de auditoría asistidas por computador (CAATS, Computer Audit Assisted Techniques) y los sistemas asociados a las mismas.
- Las herramientas para el análisis de riesgos.
- Las herramientas para la realización de pentests y análisis de vulnerabilidades.
- Las herramientas de soporte a la gestión de evidencias
- Las herramientas para la generación de informes y de soporte a la presentación de los resultados de la auditoria.

8.3.4 Planificación y Equipo de trabajo

Una vez hemos detallado los objetivos principales, el enfoque y el método, y el alcance de la auditoria es más sencillo llevar a cabo un plan de trabajo, con su cronograma asociado. Recomendamos identificar los hitos principales de la auditoria, incluyendo la pre-planificación, la planificación, la ejecución, la elaboración del informe y la presentación asociada. También debe identificarse el camino crítico y las actividades principales.

En este punto, si se trata de auditorías logísticamente complejas con multitud de centros en muchos lugares geográficamente dispersos, hay que desarrollar en detalle todas las visitas necesarias. Este aspecto puede llegar a ser muy complejo en escenarios internacionales con multitud de países y diferentes marcos regulatorios y de seguridad. De ahí que es clave detallar en el alcance todos estos aspectos a la hora de identificar nuestras infraestructuras. Hacemos notar que las visitas resultan esenciales para observar procedimientos, examinar en detalle los aspectos (principalmente de seguridad física), realizar las entrevistas oportunas y llegar a tener un entendimiento del entorno que rodea a las infraestructuras.

Recomendamos, además, identificar los diferentes roles que van a participar durante la ejecución de la auditoria y dividir las diferentes tareas de ejecución, incluyendo la revisión de documentación, desarrollo de herramientas, pruebas, recopilación de evidencias, entrevistas, auditorias físicas, *pentests*, análisis de vulnerabilidades, etc. Todo ello aconsejamos reflejarlo en un cronograma de tareas, donde quede claro, como hemos mencionado anteriormente, cual es el camino crítico.

Es de gran importancia que el equipo de trabajo tenga una cualificación adecuada para la realización de este tipo de auditorías. Por mucho que se intente minimizar, el caso es que una auditoría en un entorno industrial tiene un impacto indudable sobre la operación y genera mucha incertidumbre. Por ello es muy conveniente conseguir una buena relación entre el equipo de trabajo auditor y el personal de planta. Una forma de conseguir esto es facilitando el entendimiento entre ambos equipos con una formación adecuada del equipo auditor.

Es por lo tanto necesario que el equipo auditor, además de los conocimientos que debe tener para efectuar una Auditoria de Sistemas deberá poseer conocimientos y experiencia en:

- Funcionamiento de una planta industrial del tipo a auditar
- Conocimientos sobre seguridad industrial, metodologías de seguridad y normativa de medio ambiente
- Organización, funcionamiento y relaciones internas en los equipos de trabajo industriales
- Características de la tecnología desplegada por el proveedor principal de tecnología
- Características de las redes utilizadas
- Características principales de los equipos de control distribuido y de control directo

A la hora de organizar el trabajo de auditoría en un entorno industrial siempre hay que considerar aspectos relacionados con la peligrosidad del entorno industrial a auditar. En primer lugar, hay que considerar estos aspectos de seguridad y tenerlos en cuenta para proteger a los auditores. En segundo lugar, pero no menos importante, se deberá evitar que una intervención inadecuada del equipo de auditoría pueda poner en riesgo al resto de personas, la instalación o al medio ambiente.

8.3.5 Plan de Comunicación

Los trabajos de auditoría siempre deben de tener en cuenta el destinatario del informe, porque según de qué área se trate la auditoría deberá ser más o menos analítica. Cuando el destinatario sea a su vez el responsable del proceso, normalmente será suficiente con una revisión, que incluya todos los “hechos significativos” así como alguna elaboración global del conjunto.

Si por el contrario el destinatario del trabajo del auditor es la Comisión de Auditoría o la Alta Dirección, el documento deberá incluir además un análisis estratégico sobre la madurez de los procesos revisados, de forma que este análisis explique la incidencia de los "hechos significativos" y plantee las necesarias reformas de fondo de los procesos.

La lista de distribución debe de quedar clara dentro del Plan de Auditoria, en el apartado de Plan de comunicación, con la identificación de todos los destinatarios.

Por otro lado, recomendamos incluir dos aspectos diferentes dentro del Plan de Comunicación. Por un lado, la presentación del informe a los destinatarios finales, y por otro lado las sesiones de concienciación que puedan derivarse de los resultados finales de la auditoria.

En algunos casos, se le pedirá al auditor que realice este tipo de sesiones con diferentes tipos de responsables asociados a las infraestructuras bajo el paraguas de la auditoria. Estas sesiones recomendamos que se identifiquen como parte de los objetivos de la auditoria, y dentro del Plan de Comunicación incluir un calendario de sesiones con la lista de destinatarios asociados.

8.3.6 Referencias y Ciclo de Vida de Evidencias

Por último, recomendamos incluir como parte del Plan de Auditoria las principales referencias del Plan, incluyendo el mandato o carta de encargo, el pre-plan y el listado de referencias críticas obtenidos durante la fase de pre-planificación de la auditoria:

- El listado de regulaciones que consideramos aplicables a nuestra auditoria
- El listado de políticas, estrategias y directivas organizaciones que consideramos aplicables a nuestra auditoria.
- El listado de Infraestructuras de tecnologías de la información bajo responsabilidad de la organización objeto de la auditoria.
- El listado de entidades y acuerdos, incluyendo los contratos que puedan impactar en nuestra auditoria.

Una vez identificadas las referencias más importantes, recomendamos detallar el proceso de cómo se van a gestionar las diferentes evidencias que se obtengan durante la ejecución de la auditoria, incluyendo los sistemas de soporte asociados y los principales roles que mantendrán y harán uso de las evidencias.

8.4 Ejecución de la Auditoria

8.4.1 Reuniones de preparación con responsables de la Infraestructura

La primera actuación del equipo de auditoría una vez preparada la misma, es organizar una serie de reuniones preliminares con los responsables del proceso industrial.

En estas reuniones se deberá acordar los siguientes puntos:

- Fechas para realizar la revisión
- Lugar para efectuar las reuniones con personal de la instalación
- Lugar para compilar las evidencias y preparar los borradores
- Condiciones de acceso, seguridad en la instalación y equipos de protección individual necesarios
- Documentación disponible con antelación:

- Marcas y Modelos del equipamiento de control. Ingenierías involucradas en la construcción de la instalación
- Diagramas generales de *lay-out* de la instalación
- Diagramas generales del proceso industrial
- Organización del equipo responsable del control de procesos
- Diagramas de red y de conexión de los sistemas principales de control
- Modelo de control implementado, si lo hubiera.
- Políticas, normas, estándares y procedimientos existentes
- Ubicación de los repositorios de evidencias, históricos y *back-up*

8.4.2 Elementos básicos de recogida de evidencias

8.4.2.1 Controles de back-office (normas y estándares)

Se requiere la presentación del plan de normativa y los documentos que lo componen. Lo habitual es que ese plan tenga una estructura jerárquica, donde nivel superior lo ocupan las "políticas", seguido de las "normas" y finalizando en los más específicos "estándares", "procedimientos" y "manuales de uso".

Es muy importante recopilar toda esta información porque es la que sirve de base para identificar si los controles están adecuadamente diseñados, toda vez que deben seguir alguno de los documentos citados. Es decir, se trata de un control fundamental.

Su ausencia es una deficiencia grave.

8.4.2.2 Controles de configuración de equipos

Estos controles, más específicos que los anteriores, se realizan verificando su aplicación sobre una copia actualizada de la configuración de los equipos. Se basan en los estándares y se recomienda efectuar por este orden:

1. Equipos de comunicaciones
2. Equipos de control de alto nivel (control avanzado, gestión de históricos, conciliación de datos etc…)
3. Equipos de control distribuido (gestión de concentradores)
4. Equipos de control final (lazos de control, sensores, medida de variables complejas, PLCs etc…)
5. IoT

8.4.2.3 Controles de procedimientos

Estos controles se refieren a aquellos controles que están soportados por procedimientos que normalmente trascienden los estándares de configuración.

- Por ejemplo, la forma en que debe conectarse un *router* en una red una vez configurado. El procedimiento explicará los pasos que hay que dar y qué equipos deberán estar desconectados previamente para evitar problemas, así como la secuencia de su posterior conexión.

En las plantas industriales es muy común la existencia de muchos procedimientos para todo tipo de actuación, por lo que esta costumbre ha favorecido también la procedimentación en las redes de control.

8.4.2.4 Controles de actividad

Son controles que registran la actividad de todos los elementos controlados. Estos se diferencian de los controles históricos que registran todas las variables sea cual sea su naturaleza.

Entre los controles de actividad se encuentran los cambios en los "puntos de consigna", cambios de sesión y de usuario, altas y bajas de los mismos, cambios en los programas etc.…

Es preciso confirmar que estos controles están activos y sin debilidades, porque generalmente son evidencia de las causas reales de incidentes.

8.4.2.5 Controles Históricos

Como ya se ha mencionado, los históricos registran la evolución temporal de todas las variables. Es también un control importante porque da soporte y respaldo a los controles de actividad. Por ello es imprescindible verificar su existencia, condiciones de seguridad de acceso y buen funcionamiento del *back-up*.

8.4.2.6 Controles externalizados

Se trata de controles que están siendo supervisados por entidades externas (empresas de mantenimiento, ingeniería, proveedores de equipos especializados etc…)

Normalmente están entidades tienen contratos con la instalación industrial en los que se especifica la obligatoriedad de mantenerlos y de proporcionar acceso de auditoría a los mismos. Por ello es importante conseguir estos contratos y verificar su cumplimiento. Dependiendo de la criticidad del control tendrá que verificarse conjuntamente con la compañía externa o sustituirse con alguna certificación del tipo SSAE18 [31] (o los anteriores SSAE16 , SAS70 o similares)

8.4.2.7 Otros controles

En los entornos industriales pueden existir controles que tengan algunas diferencias con los que habitualmente se utilizan en entorno corporativos. Por ejemplo, los controles de continuidad tienen una clara diferencia por el impacto que los fallos en los equipos pueden ocasionar en la producción y en el entorno. Por ello hay que identificar tales controles y darles la importancia debida, tanto en su cumplimiento como en sus debilidades.

8.5 Comunicación y Seguimiento de la Auditoria

8.5.1 Elaboración del documento final

El trabajo de auditoría culmina con la elaboración del informe de auditoría. Este pasa por varias etapas según se completa la revisión del marco de control implantado o de la investigación de los elementos de riesgo del proceso.

En una primera fase se obtiene un documento que, en esencia, es una colección de hechos significativos. En primer lugar es preciso confirmar los resultados obtenidos, para lo cual es imprescindible efectuar reuniones con el personal de la instalación auditada con el fin de verificar que tales hechos son correctos, no tienen errores de apreciación y reflejan la situación en un momento dado.

Evidentemente si los hechos observados tienen gravedad estas reuniones posibilitan que el equipo de control industrial subsane estas deficiencias con la urgencia debida.

En segundo lugar, es preciso realizar reuniones con los responsables del proceso industrial para intentar concluir sobre las causas que permiten o favorecen la existencia de los mencionados hechos significativos. Un análisis profundo y sin prejuicios permite conseguir conclusiones valiosas para el proceso.

Con todo ello se deberá redactar un documento que incluya:

1. La Instalación
    - Diseño y equipamiento de la instalación.
    - Organización
    - Diagrama de procesos
    - Diagrama de red
    - Diagrama de equipos de control
2. Documentación preliminar del modelo de control
    - Impacto regulatorio y legal
    - Políticas, normas, procedimientos y estándares
    - Modelo de control implantado
3. Metodología de revisión de los controles
4. Hechos significativos
5. Análisis y calificación de los hechos significativos
6. Modelo de madurez
7. Recomendaciones
8. Conclusiones

8.5.2 Presentación de la Auditoría

El documento definitivo de la auditoría deberá ser presentado a su destinatario, que como se ha mencionado puede ser tanto los responsables máximos del proceso industrial como la Alta Dirección o el Comité de Auditoría.

En cualquier caso, el documento deberá ser defendido personalmente por el máximo responsable de Auditoría y deberá explicar las conclusiones que, lógicamente, llevarán aparejadas una serie de recomendaciones que tiene que ser implantadas para subsanar las deficiencias y debilidades observadas.

8.5.3 Seguimiento de recomendaciones

El informe final de la auditoría incluirá una serie de recomendaciones, las cuales llevarán aparejado un tiempo razonable para su implantación.

El primer paso para ello es que el equipo de control industrial tenga acceso a esta parte de la auditoría y conozca que existe un periodo previsto para la implantación, con objeto de que prepare un plan para llevarla a cabo.

El equipo auditor por su parte, deberá mantener una base de datos de recomendaciones, que para cada una de ellas identifique:

- Responsable
- Hitos
- Fecha de finalización
- Estado de situación

9 Impacto de nuevas tecnologías (IIoT)

En los últimos años, han surgido nuevos avances tecnológicos en el mundo digital que prometen ser los desencadenantes de una auténtica revolución que cambiará el mundo tal como se conoce actualmente. Entre ellos y especialmente destaca la denominada Internet de las Cosas o "Internet of Things", que en el caso de su aplicación industrial tiene de siglas IIoT.

Como su nombre indica, se trata de cosas/dispositivos conectados entre sí y a Internet. De esta forma, los dispositivos son capaces de realizar tareas complejas manteniendo la misma interfaz de usuario que poseían con anterioridad, sin añadir complejidad en su uso, siendo el resultado los dispositivos de siempre con funcionalidades adicionales, más inteligentes y conectados para ofrecer nuevos servicios (Domótica, Logística RFID tags, Edificios, *Smartcities, Wereables, Healthtrackers*, sistemas de vigilancia).

En el caso industrial, estos dispositivos se denominan IIoT porque se conectan a través del protocolo TCP/IP. La conectividad se puede lograr a través de un enlace directo con la red de control, si esta transporta TCP/IP, o con algún tipo de conexión a Internet (Satélite, WiFi, Bluetooth, GPRS, 4G etc…)

9.1 Tendencias actuales en IIoT:

Existen varias tendencias tecnológicas que fomentan la expansión y utilización de IIoT. Destaca, por ejemplo, el bajo coste de dispositivos HW que pone al alcance de usuarios y empresas la adquisición de dispositivos plenamente utilizables en proyectos de IIoT. Por supuesto, el tamaño cada vez más reducido de estos dispositivos fomenta su uso dada la movilidad y operatividad que pueden ofrecer sin suponer un problema de espacio o peso. Además, cada vez disponen de mayor capacidad de procesamiento que permite la realización de tareas más complejas y a mayor velocidad.

Por último, la disponibilidad, alcance y capacidad de Internet que se incrementa día a día, hace posible que sean cada vez más los dispositivos conectados y que haya millones de datos difundiéndose en tiempo real. En cifras, actualmente se estima que existen 6 mil millones de dispositivos conectados a Internet y que en 2020 la cifra alcanzará los 30 mil millones en 2020.

En su aplicación industrial permite sustituir instalaciones remotas muy costosas por dispositivos más baratos que no necesitan estar conectados directamente a una red de control extensa, sino que lo pueden hacer a través de Internet.

9.2 El enfoque de Auditoria de Sistemas

Desde el punto de vista de Auditoria de Sistemas, la actuación de un auditor ante una instalación industrial que posiblemente incluya dispositivos IIoT se basa en identificar efectivamente estos dispositivos, analizar los riesgos que presentan, evaluar posibles medidas mitigatorias y reportar formalmente la situación.

9.3 Introducción a los riesgos IIoT:

Las ventajas de IIoT son obvias y su aplicación prácticamente ilimitada. Pero como cabe esperar, los principales atractivos de IoT, la movilidad, escalabilidad, conectividad, el precio etc… lo convierten en una tecnología que se debe manejar con cuidado ya que posee una serie de riesgos inherentes.

Entre ellos se destacan los siguientes:

- Dependencia de la red (eléctrica y de conexión TCP/IP a datos): Como es lógico, delegar funciones críticas en dispositivos que se basan en sensores conectados entre sí puede

suponer un gran riesgo en caso de que suceda algún incidente que interrumpa el funcionamiento o comunicación de los dispositivos.

- Actualizaciones y vulnerabilidades: En IIoT los dispositivos normalmente se encuentran distribuidos y una actualización manual puede no ser viable en muchos casos. En este entorno, si existen vulnerabilidades que de alguna forma interrumpen la funcionalidad del dispositivo, su posterior reparación puede ser inviable. A su vez, dispositivos desactualizados pueden crear vectores de ataques para posibles atacantes.
- Estándares inmaduros: Los estándares actuales son muy diversos y en muchos casos no existe una clara relación con la seguridad ni con el entorno industrial.
- Confidencialidad: Puesto que los sensores capturan gran cantidad de datos que pueden ser enviados a la nube, la confidencialidad de los datos de la instalación puede verse afectada si no se tratan estos datos adecuadamente. IIoT propicia una gestión de datos en la nube y este hecho puede crear desconfianza en el usuario ya que los datos se encuentran fuera de su control.

9.4 Identificación de dispositivos IIoT

La tarea de identificar dispositivos IIoT es especialmente difícil, dado que, por su naturaleza son equipos muy esquivos y pueden estar situados en cualquier punto de las redes industriales de la compañía. Pueden estar formalizados e incluidos en bases de datos del tipo CMDB o pueden haber sido conectados sin que exista conocimiento al respecto entre los responsables de las redes. Por esta razón, es casi imposible asegurar que se dispone de un inventario exhaustivo de todos los dispositivos activos de red.

Es muy recomendable realizar un escaneo frecuente de elementos conectados a la red de control, aunque hay dispositivos que son muy refractarios a dichos escaneos. El problema principal está en aquellos dispositivos que no se encuentran conectados directamente a la red interna de control, sino que se conectan a Internet por otros medios, por ejemplo, a través de enlaces vía satélite o con conexiones GPRS, 3G, 4G etc… Todos estos equipos terminan proporcionando datos y, en ocasiones, actuación sobre el mundo físico, por lo que son igualmente importantes y es imprescindible incluirlos en la base de datos de equipos.

Esta tarea de identificación debe ser complementada con un cruce sistemático con los dispositivos que aparecen descritos de forma lógica en los sistemas de control. Por ejemplo, localizando todas las fuentes declaradas de datos, sea cual sea su origen, localizando contratos de servicios de datos externos (*Cloud computing*), contratos de comunicaciones satelitales, GPRS, 4G etc.… En ocasiones este método ofrece mejores indicios que la citada búsqueda física.

9.5 Controles mitigatorios en IIoT

En todos estos casos es preciso estudiar la forma de diseñar y utilizar controles alternativos que protejan el principio genérico que subyace en cada control. Por ejemplo:

- Robusteciendo notablemente la protección del acceso físico al dispositivo (control fundamental)
- Estableciendo métodos de monitorización del comportamiento del dispositivo.
- Impidiendo el acceso a los canales de programación de los dispositivos, quedando los cambios físicamente en las manos de los "administradores"
- Revisando y comprobando con frecuencia la integridad, estabilidad y vigencia de los programas instalados.
- Controlando el aislamiento con los protocolos adicionales al TCP/IP.

- Considerando una batería de controles procedentes de los modelos de control para "Cloud Computing", que asegure el tramo de datos en Internet, principalmente si los datos se almacenan y/o procesan en "Cloud".

En este sentido hay que resaltar que el diseño de controles y su implantación suponen ya en sí mismo una mejora en el nivel de madurez del entorno

10 Amenazas combinadas

En los últimos años ha surgido una variante de la forma de realizar un ataque cibernético a una instalación industrial que consiste en utilizar varios vectores de ataque de forma combinada. Esta combinación se ha denominado “amenazas combinadas” o también “amenazas híbridas” (cuando tienen una componente de redes sociales).

El gran interés estratégico que comporta un ataque a una instalación industrial, incluso un incidente no exitoso, ha motivado que se inviertan grandes cantidades de dinero para su diseño y ejecución.

En este empeño están implicados todos los agentes interesados en los efectos de un ataque, desde fuerzas especiales de ciertos ejércitos, agencias gubernamentales, grupos terroristas, etc…

Desgraciadamente el análisis detallado de estas amenazas conduce a una explosión combinatoria que dificulta notablemente su sistematización, por ello haremos en este capítulo una somera exposición de algunas amenazas combinadas y los riesgos que conllevan.

10.1 Amenazas combinadas: ciber-ciber

El diseño de estos ataques se basa en utilizar varias debilidades diferentes para provocar un incidente, el cual es imposible de prever si se atiende a cada debilidad por separado, pero que puede ser efectivo si se dan ambas.

Por ejemplo, un ataque que utilice debilidades de control de acceso para permitir su inicio, introduciéndose subrepticiamente en la red interna y posteriormente aprovechar alguna otra debilidad en el entorno operativo para culminarlo. Normalmente una parte del ataque utiliza técnicas manuales (*phising*, ingeniería social etc…) junto con virus o malware diseñados para ejecutar la parte más agresiva del incidente.

Esta modalidad abarca la mayoría de los ataques reales que se han producido a instalaciones industriales en el mundo, siendo su modelo paradigmático el ataque que sufrió la red eléctrica de Ucrania en diciembre de 2015.

Una reconstrucción ficticia de estos hechos podría ser la siguiente:

1. Un intruso externo envía una serie de correos de *phising* a los administradores del sistema industrial (obtiene esa información de personas relacionadas a través de redes sociales). Uno o más administradores acceden al correo enviado y dejan comprometidas sus claves de acceso a la red corporativa

2. El intruso se conecta de forma remota vía VPN utilizando como autentificación el *user/pass* obtenido. Logra así ingresar en la red corporativa en forma remota.

3. Posteriormente, el intruso, con los mismos *user/pass* ingresa en forma remota (vía RDP) a los equipos de estos administradores, desde donde aprende, investiga, consigue más usuarios y claves, estudia manuales etc…

4. Instala un *keylogger* sobre dos estaciones de trabajo que tienen privilegios de administrador

5. Se conecta al sistema intermedio que accede a la red industrial

6. Desde ese sistema intermedio, accede vía web a la consola del sistema de control para la gestión del sistema industrial (electricidad/gas/agua). Se autentica con una pareja *user/pass* que obtuvo con el *keylogger* instalado previamente

7. El intruso aprende a utilizar el sistema

8. En el momento del ataque final, el intruso accede a la consola, bloquea subestaciones, cierra bombas, modifica la presión del gas, generando graves alteraciones del proceso. Esto puede hacerlo manualmente o a través de un malware previamente instalado en los sistemas de control (por ejemplo, el virus "BlackEnergy" con su módulo "KillDisk")

9. Después el intruso accede a los servidores del sistema de control a nivel del sistema operativo, borra las configuraciones del sistema principal y del secundario.

10. Finaliza apagando los sistemas, de los que ya no hay *back-up* local

11. Para provocar más confusión, organiza un bombardeo cibernético de los sitios web y centrales telefónicas de la compañía, de forma que los clientes no puedan llamar a la misma ni ser informados por web sobre lo que ha sucedido

*Ilustración 14***:** *Reconstrucción ficticia de un ataque ciber-ciber*

Este relato, en gran parte imaginario, revela varias debilidades de control sin las cuales no hubiera sido posible efectuar este ataque. Por ello, la primera y más importante conclusión es que la implantación de Modelos de Control en un entorno industrial es imprescindible, para limitar drásticamente las posibilidades de los atacantes.

10.2Amenazas combinadas: dron-ciber

El año 2014 se detectaron vuelos de drones sobre al menos 7 centrales nucleares francesas, dando pábulo a diversas teorías sobre los objetivos de estas acciones. Finalmente, en julio de 2018 la organización Greenpeace estrelló un dron en una central nuclear cerca de Lyon (Francia).

Por otra parte, en el año 2019, se produjeron unos cuantos incidentes con drones en instalaciones industriales, varios de los cuales fueron ataques a las infraestructuras petrolíferas de Arabia Saudí. Estos ataques tuvieron gran repercusión internacional, con fuertes consecuencias políticas y económicas y demostraron la vulnerabilidad de estas instalaciones ante equipos que pueden ser de muy diversa entidad, tamaño, coste y sofisticación.

La coincidencia de un ataque estas características con un ataque cibernético a la misma instalación multiplicaría enormemente el potencial de destrucción, creando una nueva clase de amenaza de muy difícil mitigación.

Unos ejemplos de cómo se puede amplificar el ataque un dron con un ataque cibernético son los siguientes:

- Inactivando momentáneamente los sistemas de protección anti-incendios
- Generando alarmas inexistentes en otros puntos alejados para dispersar las brigadas de bomberos
- Saturando la red interna de la compañía para evitar la coordinación de la respuesta
- Inventando alarmas inexistentes para provocar bloqueos preventivos de la instalación y crear así desabastecimiento (*blackout* eléctrico, pérdida de suministro de agua, gas, etc…)
- etc…

10.3 Amenazas combinadas: ciber-ataque físico

Una variante de la amenaza ciber-dron es aquella en la que se produzca un ataque físico convencional junto a un ataque cibernético.

Normalmente un ataque físico exige la presencia de los atacantes en la zona de la instalación por lo que una de las características de las amenazas descritas hasta ahora, su ubicuidad y proliferación imprevisible, se desvanece, y el ataque cobra características más tradicionales.

En estos casos la componente cibernética tendrá como fin principal facilitar la acción del ataque físico, desactivando alarmas, generando confusión o eliminando la coordinación de la respuesta.

10.4 Amenazas combinadas: ciber-redes sociales (amenazas híbridas)

Otro tipo de amenazas combinadas, que habitualmente se denominan “amenazas híbridas”, son las que se pueden conseguir al producir un ataque cibernético junto con acciones en redes sociales. El objetivo es amplificar el efecto del ataque con una manipulación de la opinión pública a través de una campaña de desinformación que busca:

- Avisar o mostrar con manipulación el incidente a la población
- Engañar sobre su dimensión o consecuencias
- Confundir sobre las causas o las consecuencias, involucrando opiniones políticas
- Provocar movimientos de la población hacia la instalación industrial, colapsando accesos, limitando la llegada de equipos de socorro, etc…
- Creando un relato alternativo que se imponga sobre la realidad del incidente

11 Conclusiones

La experiencia de estos últimos años nos indica que no existe sector tecnológico libre de posibles ciberataques. Sus efectos en el sector industrial son potencialmente desastrosos con consecuencias gravísimas, siendo además la tolerancia al riesgo en este tipo de escenarios muy limitada. Por ello, la primera conclusión es que se hace imprescindible llevar a cabo un correcto análisis de riesgos y una adecuada protección dirigida a mitigarlos. En este sentido es importante destacar la necesidad de aplicar una metodología conocida con el fin de obtener unos buenos mapas de riesgo que permitan ajustar los controles debidamente.

Por lo tanto, hay que aplicar la metodología ya conocida con el fin de obtener unos buenos mapas de riesgo que permitan ajustar los controles debidamente.

Sin embargo, hay que precisar que el entorno industrial tiene unas características muy específicas que hacen que las soluciones tradicionales para mitigar los riesgos sean de difícil si no imposible aplicación. Esto conduce a un enfoque que debe ser muy adaptado y que requiere la integración de equipos multidisciplinares, con experiencia tanto en ingeniería y producción industrial como en sistemas y ciberseguridad.

Esta integración de los equipos es el punto crítico del problema y lo que dificulta la aplicación de las diversas regulaciones que están siendo desarrolladas en todo el mundo, con especial relevancia en Europa y en particular en España.

Desgraciadamente, existe una notable carencia de profesionales de la ciberseguridad que sean capaces de desenvolverse con soltura en un entorno industrial, lo que limita la consolidación de los equipos de trabajo, por lo que consideramos que hay muchas oportunidades para mejorar la formación y experiencia de los profesionales que deberán proteger estas instalaciones industriales.

Por último, hay que mencionar los retos que suponen los nuevos vectores de ataque, las amenazas combinadas y todo el entorno IoT, lo que obliga a una constante revisión y actualización de los análisis de riesgos.

12 Referencias

[1] «Comunicación COM (2005), Libro Verde sobre un Programa Europeo para la Protección de Infraestructuras Críticas,» 7 noviembre 2005. [En línea]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52005DC0576&from=EN.

[2] «Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección,» [En línea]. Available: https://www.boe.es/doue/2008/345/L00075-00082.pdf .

[3] «Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas,» 8 4 2011. [En línea]. Available: https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf.

[4] «Ley 36/2015, de 28 de septiembre, de Seguridad Nacional,» 28 9 2015. [En línea]. Available: https://www.boe.es/boe/dias/2015/09/29/pdfs/BOE-A-2015-10389.pdf.

[5] «Estrategia de Seguridad Nacional 2017,» 2017. [En línea]. Available: https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017.

[6] C. a. C. Parlamento, «Comunicación COM (2004), de la Comisión al Consejo y al Parlamento Europeo, del 20 de octubre 2004,» 2004. [En línea]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:ES:PDF.

[7] «Comunicación COM (2006), de la Comisión sobre un Programa Europeo para la Protección de Infra-estructuras Críticas,» 2006. [En línea]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:ES:PDF.

[8] «Agenda Digital,» 19 mayo 2010. [En línea]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:es:PDF .

[9] «Estrategia Europea de Ciberseguridad,» 7 febrero 2013. [En línea]. Available: https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2013-0376+0+DOC+PDF+V0//ES .

[10] «Directiva 2013/40/UE del Parlamento Europeo y del Consejo, relativa a los ataques contra los sistemas de información,» 12 agosto 2013. [En línea]. Available: https://www.boe.es/doue/2013/218/L00008-00014.pdf .

[11] «Directiva 2016/943/UE del Parlamento Europeo y del Consejo, de Protección de Secretos Comerciales.,» 8 junio 2016. [En línea]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0943&from=DA.

[12] «Directiva 2016/1148/UE 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. Directiva NIS,» 6 julio 2016. [En línea]. Available: https://www.boe.es/doue/2016/194/L00001-00030.pdf .

[13] «Directiva 2017/541/UE del Parlamento Europeo y del Consejo, relativa a la lucha contra el terrorismo.,» 15 marzo 2017. [En línea]. Available: https://www.boe.es/doue/2017/088/L00006-00021.pdf.

[14] «ALEMANIA: IT Security ACT del 25 de julio de 2015,» 25 julio 2015. [En línea]. Available: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf .

[15] «FRANCIA: Military Programming Act,» 27 marzo 2017. [En línea]. Available: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000028338825/ .

[16] «REINO UNIDO: Ley de protección de infraestructuras críticas y servicios digitales.,» 10 mayo 2018. [En línea]. Available: https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/1708.pdf.

[17] «North American Electric Reliability Corporation (NERC),» [En línea]. Available: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[18] «United States Nuclear Regulatory Commission (USNRC),» [En línea]. Available: https://www.nrc.gov/docs/ML1222/ML122210013.pdf .

[19] «Cybersecurity Law. (CSLaw),» 7 november 2016. [En línea]. Available: https://www.china-briefing.com/news/chinas-cybersecurity-law-an-introduction-for-foreign-businesspeople/ .

[20] «AUSTRALIA Security of Critical Infrastructure Act,» 2018. [En línea]. Available: https://www.legislation.gov.au/Details/C2018A00029.

[21] «The Purdue Enterprise Reference Architecture and Methodology (PERA),» [En línea]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.194.6112&rep=rep1&type=pdf.

[22] «ANSI/ISA-62443-1-1 (99.01.01)-2007 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and ModelsPa,» [En línea]. Available: https://www.isa.org/store/products/productdetail/?productId=116720.

[23] «ANSI/ISA-62443-2-1 (99.02.01)-2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program:,» [En línea]. Available: https://www.isa.org/store/products/product-detail/?productId=116731.

[24] «ISACA. Implementing the NIST Cybersecurity Framework. Control Objectives for Information and Related Technology (COBIT):,» [En línea]. Available: http://www.isaca.org/COBIT/Pages/default.aspx.

[25] «CIS Critical Security Controls for Effective Cyber Defense (CIS Controls):,» [En línea]. Available: https://www.cisecurity.org .

[26] «Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información,» 7 9 2018. [En línea]. Available: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-12257-consolidado.pdf.

[27] BOE, «RDL 12/2018,» [En línea]. Available: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-12257-consolidado.pdf.

[28] «Resolución de 8 de septiembre de 2015 Planes de Seguridad del Operador y de los Planes de Protección Específicos,» 8 9 2015. [En línea]. Available: https://www.boe.es/boe/dias/2015/09/18/pdfs/BOE-A-2015-10060.pdf.

[29] «ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems -- Requirements:,» [En línea]. Available: https://www.iso.org/standard/54534.html.

[30] «Real Decreto 951/2015 de modificación del R.D 3/2010 por el que establece el Esquema Nacional de Seguridad,» [En línea]. Available: https://www.boe.es/eli/es/rd/2015/10/23/951/dof/spa/pdf.

[31] «El estándar de auditoría SSAE 18,» 2016. [En línea]. Available: https://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/SSAE_No_18.pdf.

13 ANEXOS

13.1 Anexo 1 – Controles ISA/IEC 62443

Nº	Abrv.	Descripción
1	**IAC**	Controles de Identificación y Autenticación
2	**UC**	Control de Uso
3	**SI**	Integridad del Sistema
4	**DC**	Confidencialidad de los Datos
5	**RDF**	Flujo de Datos Restringido
6	**TRE**	Tiempo de Respuesta a Eventos
7	**DR**	Disponibilidad de Recursos

FR 1 - CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN (IAC)
SR 1.1 -Identificación y autenticación de usuarios humanos
RE (1) Identificación y autenticación única
RE (2) Múltiple factor de autenticación para redes no confiables
RE (3) Múltiple factor de autenticación para todas las redes
SR 1.2 - Identificación y autenticación de procesos de software y dispositivos
RE (1) identificación y autenticación única
SR 1.3 - Gestión de cuentas
RE (1) Gestión de cuentas unificada
SR 1.4 - identificación de gestión
SR 1.5 - Gestión de autenticación
RE (1) Hardware de seguridad para identificar credenciales mediante procesos de software
SR 1.6 - Gestión de acceso inalámbrico

FR 2 - CONTROL DE USO (UC)
SR 2.1 - Aplicación de autorización
RE (1) Aplicación de autorización para todos los usuarios
RE (2) Mapeo de permisos a roles
RE (3) Anular supervisor
RE (4) Doble Aprobación
SR 2.2 - Control de uso inalámbrico
RE (1) Identificar y reportar dispositivos inalámbricos no autorizados
SR 2.3 - Control de uso para dispositivos portátiles y móviles
RE (1) Aplicación del estado de seguridad de dispositivos portátiles y móviles
SR 2.4 - Código móvil

FR 3 - INTEGRIDAD DEL SISTEMA (SI)

SR 3.1 - Integridad en las comunicaciones

RE (1) Usar criptografía para proteger la integridad

SR 3.2 - Protección contra código malicioso

RE (1) Protección contra código malicioso en los puntos de entrada y salida

RE (2) Gestión centralizada para protección contra código malicioso

SR 3.3 - Verificación de funcionalidades de seguridad

RE (1) Mecanismos automáticos para verificar funcionalidades de seguridad

RE (2) Verificaciones de funcionalidades de seguridad durante la operación normal

SR 3.4 - Integridad del software e información

RE (1) Notificaciones automáticas sobre violaciones de integridad

SR 3.5 - Validación de entradas

SR 3.6 - Salidas Determinísticas

SR 3.7 - Manejo de errores

SR 3.8 - Integridad de sesiones

RE (1) Invalidar IDs de sesión una vez que la sesión fue terminada

RE (2) Generación de IDs únicos de sesión

RE (3) Aleatoriedad de IDs de sesión

FR 4 - CONFIDENCIALIDAD DE LOS DATOS (DC)

SR 4.1 - Confidencialidad de la información

RE (1) Protección de la confidencialidad de la información alojada o en tránsito por redes no confiables

RE (2) Protección de la confidencialidad a través de los límites de las zonas

SR 4.2 - Persistencia de la información

RE (1) Purga de recursos de memoria compartida

SR 4.3 - Uso de criptografía

FR 5 - FLUJO DE DATOS RESTRINGIDO (RDF)

SR 5.1 - Segmentación de redes

RE (1) Segmentación física de redes

RE (2) Independencia de redes sin sistemas de control

RE (3) Aislamiento lógico y físico de redes criticas

SR 5.2 - Protección de límites de zonas

RE (1) Denegar por defecto, permitir por excepción

RE (2) Modo isla

RE (3) Cierre ante fallos

SR 5.3 - Restricción en comunicaciones persona a persona de propósito general

RE (1) Prohibir todas las comunicaciones persona a persona de propósito general

SR 5.4 - Particionamiento de aplicaciones

FR 6 - TIEMPO DE RESPUESTA A EVENTOS (TRE)
SR 6.1 - Auditar accesibilidad a *logs*
RE (1) Acceso programado a *logs* de auditoria
SR 6.2 - Monitoreo continuo

FR 7 - DISPONIBILIDAD DE RECURSOS (RA)
SR 7.1 - Protección contra denegación de servicio
RE (1) Gestionar la carga en las comunicaciones
RE (1) Limitar los efectos de una denegación de servicio a otros sistemas o redes
SR 7.2 - Gestión de recursos
SR 7.3 - Control de *backup* del sistema
RE (1) Verificación de *backup*
RE (2) Automatización de *backup*
SR 7.4 - Restauración y reconstitución del sistema de control
SR 7.5 - Energía de emergencia
SR 7.6 - Ajustes de redes y configuraciones de seguridad
RE (1) Reportes de ajustes de seguridad actuales legibles desde una máquina
SR 7.7 - Menos funcionalidades
SR 7.8 - Inventario de componentes de sistemas de control

13.2Anexo 2 – Controles NIST

ID	**Identificar**	Gestión de activos
		Entorno de negocio
		Gobernanza
		Evaluación de riesgos
		Gestión de riesgos
		Gestión de riesgos de la cadena de suministro
PR	**Proteger**	Gestión de identidades y control de acceso
		Concienciación y formación
		Seguridad del dato
		Procesos de protección de la información y procedimientos
		Mantenimiento
		Tecnologías de protección
DE	**Detectar**	Anomalías y eventos
		Monitorización continua de la seguridad
		Procesos de detección
RS	**Responder**	Planificación de la respuesta
		Comunicaciones
		Análisis
		Mitigación
		Mejoras
RC	**Recuperar**	Planificación de la recuperación
		Mejoras
		Comunicaciones

13.3 Anexo 3 – Controles CIS

Nº	Descripción
1	Inventario de Dispositivos Autorizados y No Autorizados
2	Inventario de Software Autorizado y No Autorizado
3	Configuraciones seguras para hardware y software
4	Evaluación continua de la vulnerabilidad y remediación
5	Uso controlado de privilegios administrativos.
6	Mantenimiento. vigilancia y análisis de los registros de auditoría
7	Protección del correo electrónico y del navegador web
8	Defensa contra el *malware*
9	Limitación y control de puertos de red.
10	Capacidad de recuperación de datos
11	Configuraciones seguras para dispositivos de red
12	Protección perimetral
13	Protección del dato
14	Acceso controlado basado en la necesidad de saber
15	Control del acceso inalámbrico
16	Seguimiento y control de cuentas.
17	Evaluación de habilidades de seguridad y capacitación apropiada
18	Seguridad del software de aplicación
19	Respuesta y gestión de incidentes
20	Pruebas de penetración y ejercicios *RED TEAM*

Estos 20 controles se desdoblan en los siguientes 171 subcontroles:

1.1	Utilize an Active Discovery Tool
1.2	Use a Passive Asset Discovery Tool
1.3	Use DHCP Logging to Update Asset Inventory
1.4	Maintain Detailed Asset Inventory
1.5	Maintain Asset Inventory Information
1.6	Address Unauthorized Assets
1.7	Deploy Port Level Access Control
1.8	Utilize Client Certificates to Authenticate Hardware Assets
2.1	Maintain Inventory of Authorized Software
2.2	Ensure Software is Supported by Vendor
2.3	Utilize Software Inventory Tools
2.4	Track Software Inventory Information
2.5	Integrate Software and Hardware Asset Inventories
2.6	Address unapproved software
2.7	Utilize Application Whitelisting
2.8	Implement Application Whitelisting of Libraries
2.9	Implement Application Whitelisting of Scripts
2.10	Physically or Logically Segregate High Risk Applications
3.1	Run Automated Vulnerability Scanning Tools
3.2	Perform Authenticated Vulnerability Scanning
3.3	Protect Dedicated Assessment Accounts
3.4	Deploy Automated Operating System Patch Management Tools
3.5	Deploy Automated Software Patch Management Tools
3,6	Compare Back-to-back Vulnerability Scans
3,7	Utilize a Risk-rating Process
4,1	Maintain Inventory of Administrative Accounts
4,2	Change Default Passwords
4,3	Ensure the Use of Dedicated Administrative Accounts
4,4	Use Unique Passwords
4,5	Use Multifactor Authentication For All Administrative Access
4,6	Use of Dedicated Machines For All Administrative Tasks
4,7	Limit Access to Script Tools
4,8	Log and Alert on Changes to Administrative Group Membership
4,9	Log and Alert on Unsuccessful Administrative Account Login
5,1	Establish Secure Configurations
5,2	Maintain Secure Images
5,3	Securely Store Master Images
5,4	Deploy System Configuration Management Tools
5,5	Implement Automated Configuration Monitoring Systems
6.1	Utilize Three Synchronized Time Sources
6.2	Activate audit logging
6.3	Enable Detailed Logging
6.4	Ensure adequate storage for logs
6.5	Central Log Management
6.6	Deploy SIEM or Log Analytic tool
6.7	Regularly Review Logs
6.8	Regularly Tune SIEM
7.1	Ensure Use of Only Fully Supported Browsers and Email Clients
7.2	Disable Unnecessary or Unauthorized Browser or Email Client Plugins
7.3	Limit Use of Scripting Languages in Web Browsers and Email Clients
7.4	Maintain and Enforce Network-Based URL Filters
7.5	Subscribe to URL-Categorization service
7.6	Log all URL requests
7.7	Use of DNS Filtering Services
7.8	Implement DMARC and Enable Receiver-Side Verification
7.9	Block Unnecessary File Types
7.10	Sandbox All Email Attachments
8.1	Utilize Centrally Managed Anti-malware Software
8.2	Ensure Anti-Malware Software and Signatures are Updated
8.3	Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies
8.4	Configure Anti-Malware Scanning of Removable Devices
8.5	Configure Devices Not To Auto-run Content
8.6	Centralize Anti-malware Logging
8.7	Enable DNS Query Logging
8.8	Enable Command-line Audit Logging
9.1	Associate Active Ports, Services and Protocols to Asset Inventory
9.2	Ensure Only Approved Ports, Protocols and Services Are Running
9.3	Perform Regular Automated Port Scans
9.4	Apply Host-based Firewalls or Port Filtering
9.5	Implement Application Firewalls
10.1	Ensure Regular Automated Back Ups
10.2	Perform Complete System Backups
10.3	Test Data on Backup Media
10.4	Ensure Protection of Backups

10.5	Ensure Backups Have At least One Non-Continuously Addressable Destination
11.1	Maintain Standard Security Configurations for Network Devices
11.2	Document Traffic Configuration Rules
11.3	Use Automated Tools to Verify Standard Device Configurations and Detect Changes
11.4	Install the Latest Stable Version of Any Security-related Updates on All Network Devices
11.5	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
11.6	Use Dedicated Machines For All Network Administrative Tasks
11.7	Manage Network Infrastructure Through a Dedicated Network
12.1	Maintain an Inventory of Network Boundaries
12.2	Scan for Unauthorized Connections across Trusted Network Boundaries
12.3	Deny Communications with Known Malicious IP Addresses
12.4	Deny Communication over Unauthorized Ports
12.5	Configure Monitoring Systems to Record Network Packets
12.6	Deploy Network-based IDS Sensor
12.7	Deploy Network-Based Intrusion Prevention Systems
12.8	Deploy NetFlow Collection on Networking Boundary Devices
12.9	Deploy Application Layer Filtering Proxy Server
12.10	Decrypt Network Traffic at Proxy
12.11	Require All Remote Login to Use Multi-factor Authentication
12.12	Manage All Devices Remotely Logging into Internal Network
13.1	Maintain an Inventory Sensitive Information
13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organization
13.3	Monitor and Block Unauthorized Network Traffic
13.4	Only Allow Access to Authorized Cloud Storage or Email Providers
13.5	Monitor and Detect Any Unauthorized Use of Encryption
13.6	Encrypt the Hard Drive of All Mobile Devices.
13.7	Manage USB Devices
13.8	Manage System's External Removable Media's Read/write Configurations
13.9	Encrypt Data on USB Storage Devices
14,1	Segment the Network Based on Sensitivity
14,2	Enable Firewall Filtering Between VLANs
14,3	Disable Workstation to Workstation Communication
14,4	Encrypt All Sensitive Information in Transit
14,5	Utilize an Active Discovery Tool to Identify Sensitive Data
14,6	Protect Information through Access Control Lists
14,7	Enforce Access Control to Data through Automated Tools
14,8	Encrypt Sensitive Information at Rest
14,9	Enforce Detail Logging for Access or Changes to Sensitive Data
15.1	Maintain an Inventory of Authorized Wireless Access Points
15.2	Detect Wireless Access Points Connected to the Wired Network
15.3	Use a Wireless Intrusion Detection System
15.4	Disable Wireless Access on Devices if Not Required
15.5	Limit Wireless Access on Client Devices
15.6	Disable Peer-to-peer Wireless Network Capabilities on Wireless Clients
15.7	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data
15.8	Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication
15.9	Disable Wireless Peripheral Access of Devices
15.10	Create Separate Wireless Network for Personal and Untrusted Devices
16.1	Maintain an Inventory of Authentication Systems
16.2	Configure Centralized Point of Authentication
16.3	Require Multi-factor Authentication
16.4	Encrypt or Hash all Authentication Credentials
16.5	Encrypt Transmittal of Username and Authentication Credentials
16.6	Maintain an Inventory of Accounts
16.7	Establish Process for Revoking Access
16.8	Disable Any Unassociated Accounts
16.9	Disable Dormant Accounts
16.10	Ensure All Accounts Have An Expiration Date
16.11	Lock Workstation Sessions After Inactivity
16.12	Monitor Attempts to Access Deactivated Accounts
16.13	Alert on Account Login Behavior Deviation
17.1	Perform a Skills Gap Analysis
17.2	Deliver Training to Fill the Skills Gap
17.3	Implement a Security Awareness Program
17.4	Update Awareness Content Frequently
17.5	Train Workforce on Secure Authentication
17.6	Train Workforce on Identifying Social Engineering Attacks

17.7	Train Workforce on Sensitive Data Handling
17.8	Train Workforce on Causes of Unintentional Data Exposure
17.9	Train Workforce Members on Identifying and Reporting Incidents
18,1	Establish Secure Coding Practices
18,2	Ensure Explicit Error Checking is Performed for All In-house Developed Software
18,3	Verify That Acquired Software is Still Supported
18,4	Only Use Up-to-date And Trusted Third-Party Components
18,5	Use Only Standardized and Extensively Reviewed Encryption Algorithms
18,6	Ensure Software Development Personnel are Trained in Secure Coding
18,7	Apply Static and Dynamic Code Analysis Tools
18,8	Establish a Process to Accept and Address Reports of Software Vulnerabilities
18,9	Separate Production and Non-Production Systems
18.10	Deploy Web Application Firewalls (WAFs)
18.11	Use Standard Hardening Configuration Templates for Databases
19,1	Document Incident Response Procedures
19,2	Assign Job Titles and Duties for Incident Response
19,3	Designate Management Personnel to Support Incident Handling
19,4	Devise Organization-wide Standards for Reporting Incidents
19,5	Maintain Contact Information For Reporting Security Incidents
19,6	Publish Information Regarding Reporting Computer Anomalies and Incidents
19,7	Conduct Periodic Incident Scenario Sessions for Personnel
19,8	Create Incident Scoring and Prioritization Schema
20,1	Establish a Penetration Testing Program
20,2	Conduct Regular External and Internal Penetration Tests
20,3	Perform Periodic Red Team Exercises
20,4	Include Tests for Presence of Unprotected System Information and Artifacts
20,5	Create Test Bed for Elements Not Typically Tested in Production
20,6	Use Vulnerability Scanning and Penetration Testing Tools in Concert
20,7	Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards
20,8	Control and Monitor Accounts Associated with Penetration Testing

$