Lloyd's Register Foundation

La vida importa

Julio de 2020

Lloyd's Register Foundation
Serie de informes: N.° 2020.1

Esta portada y las figuras 1 y 11 se han diseñado mediante recursos de Freepik.com

Lloyd's Register Foundation

Evaluación de la previsión de la seguridad cibernética para el IoT industrial

Habilitar infraestructuras más seguras y resilientes

Julio de 2020

Lloyd's Register Foundation
Serie de informes: N.º 2020.1

Acerca de la Lloyd's Register Foundation

Nuestra visión

Nuestra visión es ser conocidos en todo el mundo como una de las principales instituciones que apoyan la investigación relacionada con la ingeniería, la formación y la educación, lo que marca realmente la diferencia a la hora de mejorar la seguridad de la infraestructura crítica en la que se basa la sociedad moderna. Para apoyar esta visión, fomentamos la excelencia científica y actuamos como catalizador, trabajando con otros para lograr el máximo impacto.

La misión benéfica de la Lloyd's Register Foundation

- Garantizar, en beneficio de la comunidad, altos niveles técnicos de diseño, fabricación, construcción, mantenimiento, operación y rendimiento, con el fin de mejorar la seguridad de la vida y las propiedades en el mar, en tierra y en el aire.
- Hacer avanzar la educación pública, también en las industrias del transporte y cualquier otra disciplina relacionada con la ingeniería y la tecnología.

Acerca de la Serie de informes de la Lloyd's Register Foundation

El objetivo de esta Serie de informes es difundir abiertamente información sobre el trabajo que se realiza con el apoyo de la Lloyd's Register Foundation. Se espera que estos informes aporten ideas para la investigación, las políticas y las comunidades empresariales, y enriquezcan un debate más amplio en la sociedad acerca de los retos relacionados con la seguridad en ingeniería que investiga la Fundación.

T +44 20 7709 9166
E info@lrfoundation.org.uk
www.lrfoundation.org.uk

Índice

Resumen ejecutivo

El Internet de las cosas (IoT, por sus siglas en inglés) se ha desarrollado para beneficiar a la sociedad mediante una variedad de plataformas inteligentes y ha experimentado una enorme expansión. Los cálculos varían, pero cuenta con decenas de miles de millones de dispositivos y está creciendo rápidamente. Esta evaluación se centra en el Internet industrial de las cosas (IIoT, por sus siglas en inglés). Los sistemas de control industrial (SCI) habilitados para IoT se están convirtiendo en una proporción significativa de infraestructuras críticas actuales y futuras, con una gran aceptación en ámbitos como la energía, el transporte, el medio urbanizado y las instalaciones de producción. Las consecuencias de un fallo pueden ser graves en esos entornos; por lo tanto, es vital entender cómo se pueden suministrar infraestructuras seguras y resilientes. El IIoT acentúa los retos para la seguridad ya existentes y plantea nuevos retos propios. Es esencial dar prioridad a la acción, identificando los principales riesgos emergentes y las deficiencias de capacidad.

El IoT se ha desarrollado para beneficiar a la sociedad mediante una variedad de plataformas inteligentes y ha experimentado una enorme expansión

Desde el punto de vista de la seguridad, esta evaluación considera que el IIoT está compuesto por tres partes fundamentales: los dispositivos físicos (en particular, los sensores), las redes de comunicación y la información y los datos, incluyendo las tecnologías correspondientes de software y hardware para suministrar los procesos y análisis.

Las tecnologías inteligentes facilitan nuevas áreas de innovación y nuevas formas de control, que permiten a las organizaciones predecir y gestionar los comportamientos de sus sistemas y entornos. Esta evaluación establece cuatro fuerzas fundamentales que impulsan la adopción de tecnologías del IIoT:

- Mejorar los procesos operativos en lo que respecta a la seguridad, la productividad, la supervisión, la eficiencia, la adaptabilidad, la gestión de riesgos u otros resultados.
- La agenda ambiental: eficiencia energética optimizada, justificación del consumo de energía, etc., ya sea para apoyar las prioridades internas o para cumplir la normativa externa.
- Mercados de datos: para capitalizar los datos protegidos en los mercados abiertos, o bien para crear o ampliar los procesos y servicios internos.
- Conveniencia y experiencia de los clientes: el suministro de personalización basada en datos y ventanas externas al estado en tiempo real será cada vez más valioso.

En conjunto, estos impulsores contribuyen a las características emergentes del IIoT que se prevé que continuarán en el futuro:

- La escala de los dispositivos, las redes y los datos del IIoT está aumentando rápidamente.
- Los sistemas IIoT de las organizaciones e industrias, y entre ellas, cada vez están más conectados entre sí.
- La industria y la sociedad están desarrollando una dependencia crítica de los sistemas IIoT y de sus funciones inteligentes.
- Las comunicaciones más rápidas y fiables entre componentes del IIoT están permitiendo nuevas funciones e interoperabilidad.
- El dinamismo y la agilidad de los sistemas y redes están aumentando como resultado de la automatización y la definición del software.

A medida que el IIoT vaya avanzando, habrá un mayor potencial de sufrir perjuicios cibernéticos, que se irán volviendo más graves y potencialmente sistémicos con la conexión y la automatización de los sistemas críticos para las misiones. Estos retos son especialmente acuciantes para la industria y los proveedores de infraestructuras, que tienen fuertes imperativos económicos y de seguridad para mantener operativos los sistemas centrales en todas las circunstancias. En el IIoT futuro:

- Los riesgos tradicionales para la seguridad cibernética evolucionan y van aumentando a medida que el IIoT va ampliándose.
- La interconexión genera riesgos comunes y sistémicos.
- Se podrían derivar riesgos directamente de los datos creados por el IIoT.
- Las tecnologías emergentes, como la inteligencia artificial (IA) y la informática cuántica, podrían generar nuevos riesgos.
- Los riesgos específicos de la industria incluyen la probabilidad de riesgos para la seguridad, la interacción imprevista entre sistemas heredados, el riesgo de contagio debido al pequeño número de fabricantes del IIoT y los riesgos relacionados con la evolución necesaria de la formación y la cultura para incluir el IIoT.

El ritmo actual de cambio en las capacidades de seguridad operativa no se equiparará con la rápida emergencia de nuevos riesgos para la seguridad en entornos de IIoT. A nivel conceptual, las normas y directrices de seguridad existentes siguen siendo relevantes para el IIoT. Sin embargo, a nivel práctico, la posibilidad de suministrar esas capacidades, así como las formas en que se deben suministrar, cambian en el IIoT. Con frecuencia, las capacidades no se amplían, no son interoperables, no son viables técnicamente, todavía no existen o todavía no se han probado. Otra complicación es que las deficiencias en algunas capacidades fundamentales tienen consecuencias para otros controles de riesgos. Hay deficiencias cada vez más amplias en habilidades y concienciación. Nos encontramos en un momento crítico para la recuperación, a medida que la alternativa manual se va volviendo inviable para los sistemas de sistemas complicados y los entornos de redes: la recuperación tendrá que plantearse de otra manera. Asimismo, hay retos para la mentalidad, la reglamentación y los seguros, a medida que procuremos fomentar la mejora de las prácticas en materia de seguridad.

El análisis de esta evaluación indica que existe la necesidad de adoptar un conjunto de principios rectores para aumentar suficientemente el ritmo de cambio en la seguridad cibernética operativa. Esos principios buscan endurecer las posiciones de las maneras siguientes: «dar por sentado el fallo» como base para la planificación de las situaciones posibles de riesgo, la arquitectura y el desarrollo de estrategias de seguridad; «dar por sentado la amenaza interna» en los sistemas y las cadenas de suministro; «dar por sentado el potencial de riesgo sistémico» y buscar formas de identificar y realizar pruebas allí donde pudiera aparecer; y métodos para limitar la propagación del perjuicio.

Esta evaluación define los siguientes siete pasos prácticos para las organizaciones que utilizan el IIoT en la actualidad. Se trata de medidas que se deben tener en cuenta al desarrollar productos y servicios a corto y largo plazo: en general, las organizaciones deberían intentar pasar de una gestión de riesgos basada en el cumplimiento normativo a una gestión basada en los resultados.

La evaluación identifica una necesidad urgente de seguir investigando y estudiando, con el objetivo de entender y poner en evidencia el rendimiento en el control del riesgo; estudiar modelos de responsabilidad, los aspectos prácticos y las implicaciones para los mercados del IoT; y exploración de una posible cooperación internacional para desarrollar confianza en la cadena de suministro en relación con los dispositivos y el software del IIoT. El informe finaliza con una llamada a la acción para tratar de apoyar la comprensión del potencial riesgo sistémico en el IIoT, ya que esto podría tener consecuencias significativas para la seguridad pública y el bienestar económico mundial; y contar con demostradores conceptuales en los entornos emergentes del IIoT para garantizar la proliferación de las prácticas recomendadas y el desarrollo de capacidad en todo el mundo.

Prólogo

El panorama industrial de la actualidad sería irreconocible para los expertos en seguridad que fundaron Lloyd's Register. Nuestros sistemas industriales, tan interconectados y globalizados, exigen nuevos enfoques de la seguridad, y aquellos que diseñan, operan y regulan nuestros nuevos panoramas industriales deben mantener la seguridad como un objetivo principal a medida que vamos adoptando rápidamente nuevas tecnologías.

Aunque las organizaciones han sufrido vulneraciones de seguridad cibernética, todavía no hemos experimentado una destrucción a gran escala en el ciberespacio. Ningún ataque ha dado lugar a un fallo sistémico a gran escala, con un colapso fundamental de la tecnología y los servicios, ni a la pérdida completa de la confianza en la infraestructura. Algunos creen que esto demuestra una resiliencia inherente en el ciberespacio. Aunque se produzcan perdedores o víctimas individuales (a todas las escalas), nuestros enfoques de la gestión de los riesgos cibernéticos son suficientes. Es poco probable que esta creencia se mantenga en el futuro a medida que desarrollamos el Internet de las cosas (IoT). Afrontaremos retos significativos para suministrar seguridad cibernética, debido a la diferencia de sistemas que el IoT creará.

Resulta difícil anticiparse en el campo de la seguridad cibernética, ya que no solo debemos tener en cuenta los avances relevantes en tecnología, sino también cómo se podrían utilizar y atacar. Esto resulta especialmente cierto con el IoT, con aplicaciones que están creciendo exponencialmente, creando nuevos ecosistemas digitales que podrían traer consigo nuevos tipos de ataques posibles.

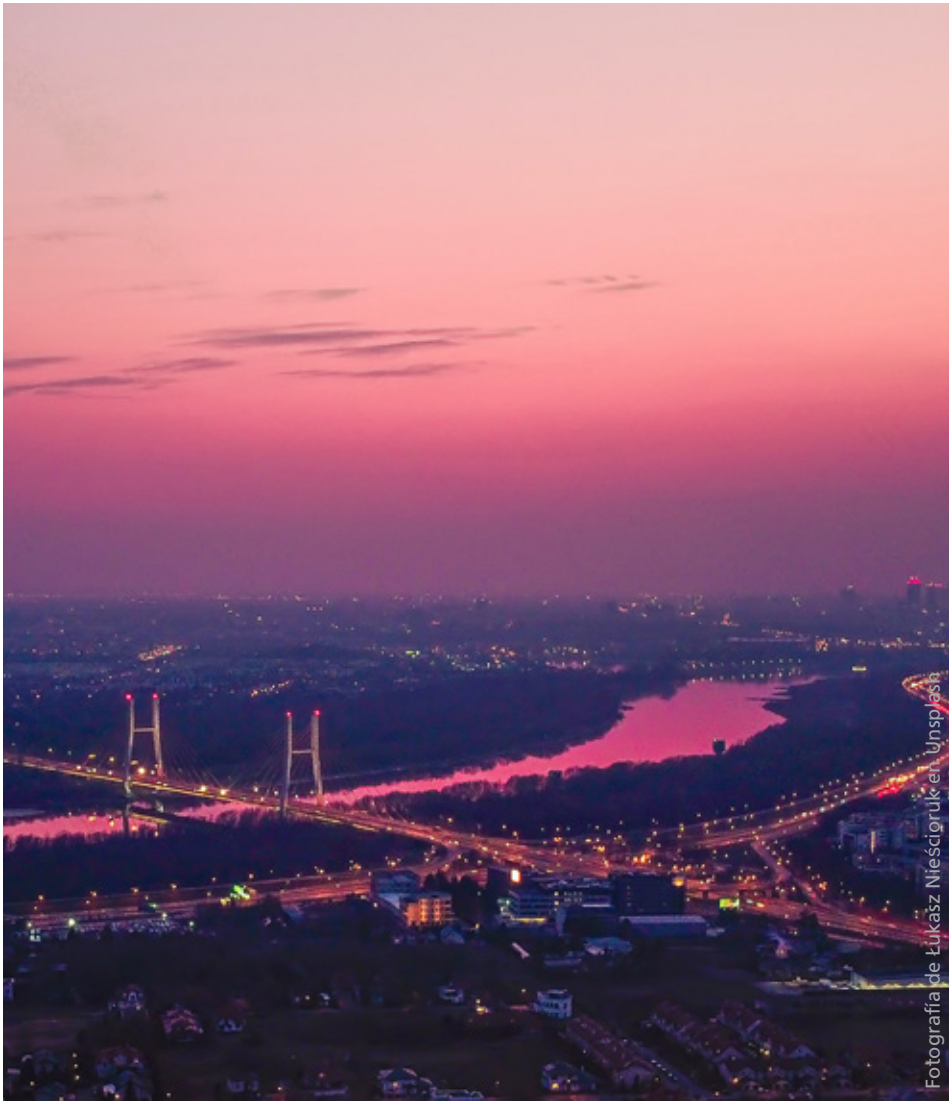
Este informe se centra en los sistemas de control industrial habilitados para el IoT, dirigidos a una proporción significativa de nuestras infraestructuras críticas futuras, en particular la energía, el transporte, el medio urbanizado y las instalaciones de producción. El ámbito del IoT considerado incluye los componentes técnicos, así como las personas y los procesos, que sustentan las infraestructuras críticas de las cuales depende la sociedad. Las observaciones y recomendaciones del informe se pueden generalizar para todas las naciones, independientemente de su riqueza, y es probable que sean válidas para todas las aplicaciones del IoT industrial (el IIoT), de forma que se pueda contar con infraestructuras más seguras, más protegidas y más resilientes.

El IoT está evolucionando rápidamente y los planteamientos actuales de la seguridad cibernética para prevenir, detectar y responder a los ataques no se pueden trasladar por completo a este dominio. Esta evaluación de la previsión describe los principales retos para la seguridad cibernética operativa en el contexto del IIoT y sugiere opciones para abordar las deficiencias en capacidad. Las conclusiones de esta evaluación constituyen una llamada a la acción en apoyo de la misión de la Lloyd's Register Foundation para construir un mundo más seguro.

Sadie Creese
Profesora de Seguridad cibernética
Universidad de Oxford

Robert Hannigan
Presidente, BlueVoyant International

Profesor Richard Clegg
Director General de la Fundación
Lloyd's Register Foundation



Fotografía de Łukasz Nieścioruk en Unsplash

Antecedentes

La finalidad de esta evaluación de la previsión es difundir información, aportar ideas a los responsables de la toma de decisiones y a los investigadores, y enriquecer un debate más amplio, centrado especialmente en esta pregunta: ¿será suficiente el cambio operativo actual en seguridad cibernética? Presenta tanto una visión a largo plazo de los retos principales, que las comunidades de investigación y desarrollo deberán abordar, como un punto de vista sobre los pasos prácticos siguientes, más amplios, que se deberían dar en la actualidad para prepararse para la adopción inmediata de las tecnologías del IoT por parte de la industria.

La complejidad irá aumentando a medida que los sistemas fundamentales vayan dependiendo cada vez más de los enfoques inteligentes o conectados para controlar el trabajo, lo que supondrá un mayor riesgo para los procesos industriales y las personas que trabajan en ellos. Por consiguiente, los requisitos en seguridad cibernética del Internet industrial de las cosas deben definirse ahora para que podamos entender mejor sus vulnerabilidades y estemos mejor formados y equipados para gestionar los riesgos correspondientes. La evaluación abarca las tecnologías y los sistemas sociotécnicos subyacentes a los sistemas críticos de los cuales depende la vida, e identifica los requisitos y las posibles respuestas para habilitar infraestructuras más seguras y resilientes y habilitar innovación más segura y protegida.

La evaluación ilustra esto centrándose en cuatro sectores: la energía, el transporte, el medio urbanizado y las instalaciones de producción.

Las conclusiones y recomendaciones se han desarrollado a partir de una serie de conversaciones y talleres, así como a partir de la revisión bibliográfica, con la cual se sintetizaron temas y cuestiones que se consideraron para su inclusión. Los talleres tuvieron lugar en Singapur, el 3 de octubre de 2019*; en Oxford (Reino Unido), el 13 de enero de 2020; y en San Francisco (EE. UU.), el 25 de febrero de 2020. En este proceso ha participado más de 110 colaboradores. Las personas que deseaban ser reconocidas aparecen en una lista alfabética en el Apéndice B. Los autores dan las gracias a todas las personas mencionadas y a las que han optado por no incluir su nombre en el informe, por su energía y sus interesantes aportaciones durante la preparación de esta evaluación. Los autores expresan su gratitud por el apoyo de la Agencia de Seguridad Cibernética de Singapur, el Consejo de Normas de Singapur, Enterprise Singapur, la Federación de Fabricantes – Organización de Desarrollo de Normas de Singapur y AXIS Capital por haber facilitado estos talleres.

*Este taller fue una subsesión de un taller sobre Concienciación sobre seguridad cibernética y Normas, organizado por la Federación de Fabricantes – Organización de Desarrollo de Normas de Singapur, que tuvo lugar como parte de la Semana Cibernética Internacional de Singapur de 2019 (SICW 2019).

Autores del informe

Sadie Creese
Profesora de Seguridad cibernética, Departamento de Informática, Universidad de Oxford

Robert Hannigan
Presidente, BlueVoyant International; Director de GCHQ 2014-2017

Ali El Kaafarani
Fundador y Consejero Delegado, PQShield

Louise Axon
Investigador posdoctoral asociada, Departamento de Informática, Universidad de Oxford

Katherine Fletcher
Gestora de proyectos y Coordinadora de Cyber Security Oxford, Universidad de Oxford

Eva Nagyfejeo
Investigadora docente, Global Cyber Security Capacity Centre, Universidad de Oxford

Arianna Schuler Scott
Investigadora de doctorado, Centro de Formación doctoral en Seguridad cibernética, Universidad de Oxford

Marcel Stolz
Investigador de doctorado, Centro de Formación doctoral en Seguridad cibernética, Universidad de Oxford

Relatores colaboradores

Mary Bispham
Matthew Rogers
Centro de Formación doctoral en Seguridad cibernética, Universidad de Oxford

Introducción al Internet industrial de las cosas

El Internet de las cosas (IoT*, por sus siglas en inglés) es la red de tecnologías que está interconectada y funciona a través de internet, en gran medida sin intervención de los seres humanos. Con frecuencia (pero no siempre) se trata de un conjunto de dispositivos pequeños y de baja potencia, diseñados para funcionar como parte de un sistema coordinado para la recopilación y el análisis de datos. Representa una enorme instrumentalización de un mundo en el que los dispositivos informáticos, tanto grandes como pequeños, están generalizados e integrados a través de una gran variedad de entornos. Esto no se limita a la creación de nuevas tecnologías, sino que también conlleva agregar hardware y software informáticos a objetos que previamente no tenían componentes digitales. Es importante señalar que, para formar parte del IoT, los componentes digitales deben conectarse a internet. Con frecuencia, esto añade un elemento cibernético a algo físico, lo que da lugar a un sistema ciberfísico. La funcionalidad de internet ya está omnipresente a través del trabajo y la vida social, y el IoT la hará todavía más cercana: las relaciones entre los dispositivos, el software y las personas variará enormemente en densidad, tiempo, espacio y automatización.

El IoT se ha desarrollado para beneficiar a la sociedad mediante una variedad de plataformas inteligentes y ha experimentado una enorme expansión. Los cálculos varían, pero el número de dispositivos siempre es grande (decenas de miles de millones y creciendo rápidamente). Esta evaluación se centra en el IoT industrial (el IIoT, por sus siglas en inglés), es decir, las aplicaciones industriales de las tecnologías del IoT. Los sistemas de control industrial (SCI) con internet, que por naturaleza tienden a ser físicamente más grandes que los del IoT «tradicional», así como a tener dispositivos más pequeños (en ocasiones, incluyen dispositivos IoT para consumidores), se están convirtiendo en una proporción importante de las infraestructuras críticas actuales y futuras. El IIoT suele tender nuevos puentes entre la tecnología de la información (TI) y la tecnología operativa (TO), dos áreas que, tradicionalmente, se han gestionado y regulado por separado[1,2].

Este informe se centra en el IIoT porque la seguridad es crítica para estos entornos

Este informe se centra en el IIoT porque la seguridad es crítica para estos entornos y es vital que entendamos cómo se pueden suministrar infraestructuras seguras y resilientes. El Informe de Riesgos Globales del Foro Económico Mundial de 2020 valoró el riesgo a corto plazo de un ataque cibernético a las infraestructuras en más del 76 %[3].

El IIoT acentúa los retos para la seguridad ya existentes y plantea nuevos retos propios. Es esencial dar prioridad a la acción, identificando los principales riesgos emergentes y las deficiencias de capacidad para los cuales no será suficiente el ritmo actual de cambio en la seguridad cibernética operativa (es decir, el conjunto de procesos de gestión de riesgos en seguridad cibernética).

Para ayudar a determinar dónde afloran los riesgos, este informe divide conceptualmente el IIoT en tres partes fundamentales, que se representan en la figura 1 de la página siguiente.

- Los dispositivos físicos incluyen los sensores, que recopilan datos del mundo físico, y los componentes de control, que realizan acciones en el mundo físico basándose en la información que se les comunica y los cálculos que realizan.
- Las redes de comunicaciones, que conectan los dispositivos a internet y entre sí. Estas redes transmiten datos para realizar su tratamiento y analizarlos, y también transmiten la información y las instrucciones de control que se derivan de ellos. Las nuevas tecnologías de la comunicación, y en particular el nuevo estándar 5G para la comunicación móvil, pero también las tecnologías «de igual a igual», se han desarrollado para mejorar drásticamente la comunicación móvil. La velocidad de la comunicación y el volumen de dispositivos que se pueden conectar seguirán aumentando drásticamente. Se prevé que este será un avance fundamental para facilitar la expansión al IIoT.
- Información y datos, y las correspondientes tecnologías de software y hardware para suministrar los procesos y análisis, tanto en entornos de servicios en la nube como, cada vez más, en sitios de edge-computing (informática de periferia). Los datos son la principal fuente de valor en el IIoT: las cuestiones fundamentales suelen girar en torno a cómo y dónde se recopilan y envían los datos, y qué ideas o mejoras se pueden obtener con el tratamiento de los datos y aprendiendo de ellos. Por consiguiente, otras tecnologías fundamentales son la IA / el aprendizaje automático y el análisis de macrodatos, nuevas técnicas en informática y datos que permiten a las organizaciones entender las enormes cantidades de datos que son capaces de recopilar.

* Este informe va dirigido a una audiencia no especializada y los términos importantes se van definiendo a medida que se van introduciendo, pero a los lectores les podría resultar útil el glosario del Apéndice C, para consultar los términos con los que no estén familiarizados. Todos los términos incluidos en el glosario aparecen subrayados la primera vez que se mencionan en el texto del informe.

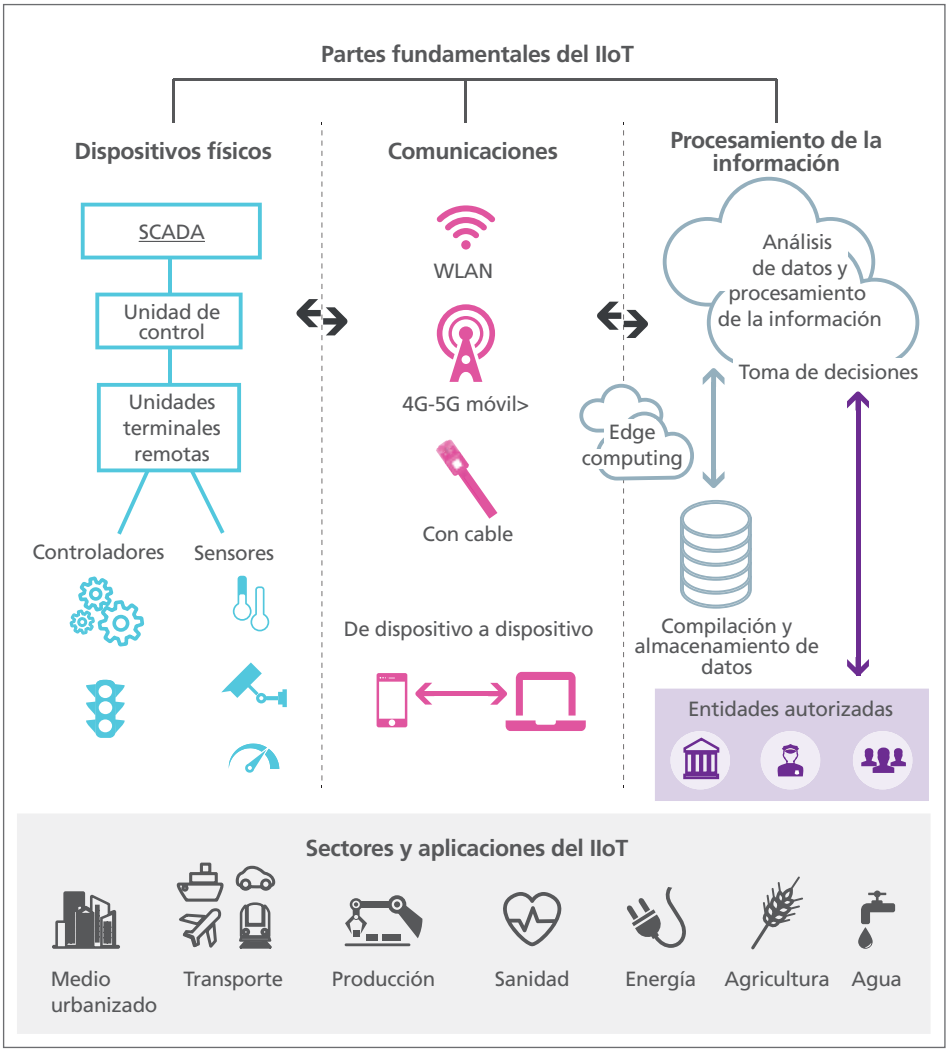


Figura 1: Las tres partes fundamentales del IIoT en contexto

¿Cómo utiliza la industria el IoT?

La adición de la tecnología habilitada con IoT a los entornos industriales puede ayudar a mejorar la eficiencia y la seguridad de muchas maneras; por ejemplo, al supervisar el estado de los equipos o procesos, al mejorar el conocimiento de la situación y al minimizar la necesidad de que los seres humanos estén presentes en entornos peligrosos. Las tecnologías del IIoT se están adoptando en organizaciones y sectores de toda la economía. Esta evaluación se centra en cuatro sectores (transporte, energía, medio urbanizado e instalaciones de producción), por tres razones:

- Hay muchas organizaciones de estos sectores que están explorando el uso del IIoT; por tanto, se puede aprovechar una gran variedad de datos.
- Proporcionan una sección representativa de los desafíos con lecciones que pueden aplicarse de forma muy variada.
- Los sectores están relativamente bien definidos, con partes interesadas conocidas; por tanto, un esfuerzo centrado debería conseguir un progreso tangible.

Transporte

El sector del transporte abarca sistemas interconectados que permiten el desplazamiento de las personas y las mercancías. La tecnología reciente que permite que suceda esto incluye los vehículos autónomos, o parcialmente autónomos, los vehículos controlados por seres humanos y la infraestructura que sostiene esos vehículos. Esta tecnología está cada vez más conectada a internet por medio del IoT. Imaginemos un pequeño puerto: la recopilación de datos sobre los niveles de agua y sal, el viento, la visibilidad y las corrientes puede aportar información que ayude a optimizar la movilidad y a mejorar la seguridad en los barcos, en el puerto y en sus proximidades, y con el tiempo también permitirá el uso de barcos, grúas y camiones autónomos para cargar y descargar mercancías, según el contenido de los contenedores, tal como se ilustra en la figura 2. Las actualizaciones de la ubicación en tiempo real, la inclinación, la temperatura, la humedad y otros datos pueden mejorar la visibilidad en toda la cadena de suministro, y también podrían mejorar la seguridad, la capacidad de realizar auditorías, la planificación y la protección.

Figura 2: IoT para un puerto inteligente

Energía

El sector de la energía abarca sistemas interconectados que crean, refinan, gestionan, transportan y suministran energía. Las redes inteligentes (figura 3) constituyen un ejemplo fundamental de la integración del IIoT: pueden gestionar la distribución de energía recopilando datos y realizando el autodiagnóstico de problemas, lo que establece una base de referencia operativa que permite a las empresas de servicios básicos evaluar continuamente el comportamiento de la red y generar las respuestas correspondientes. Una red inteligente es un conjunto de tecnologías que desempeñan varias funciones importantes: ayudar a equilibrar dinámicamente la carga y mantener un suministro continuo, al mismo tiempo que integran las fuentes de energía renovables no fiables, sustentan la facturación y la previsión correctas para los usuarios y los propietarios del sistema, y posiblemente permiten el mantenimiento preventivo o el redireccionamiento para mantener la resiliencia del suministro eléctrico crítico para la seguridad. Al recopilar datos sobre la forma en que la gente consume la energía, la red inteligente permite una distribución y una planificación más eficientes de la energía.

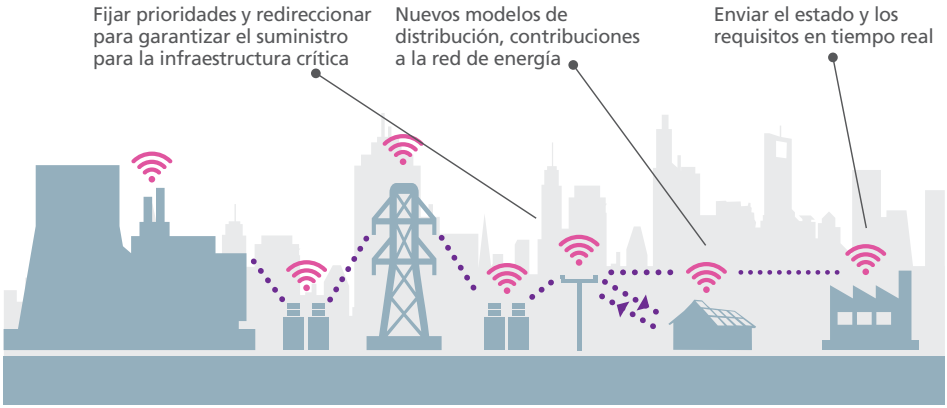


Figura 3: IoT para la energía: optimización de la distribución de energía desde diversas fuentes, según el consumo y la demanda

Medio urbanizado

Los edificios de ciudades a mayor escala, como los aparcamientos, hospitales o bloques de pisos, incorporan sensores que miden una enorme variedad de puntos de datos, incluyendo cambios de temperatura, humedad, tensión, vibraciones, movimiento de personas, vehículos o artículos, calidad del aire y consumo de recursos, como la energía, el agua y los datos (véase la figura 4). Esos datos se pueden utilizar para identificar peligros emergentes para el mantenimiento o la seguridad, sustentar las operaciones de seguridad cibernética y física, y compartirse con los proveedores de servicios para optimizar y personalizar la oferta. Asimismo, el sistema de gestión de un edificio los puede utilizar para optimizar el consumo de recursos del edificio en su conjunto, para gestionar y automatizar los sistemas de todo el edificio, como la ventilación y la calefacción, y para permitir que el edificio se integre en su entorno urbanizado más general (la ciudad, el pueblo o el país).

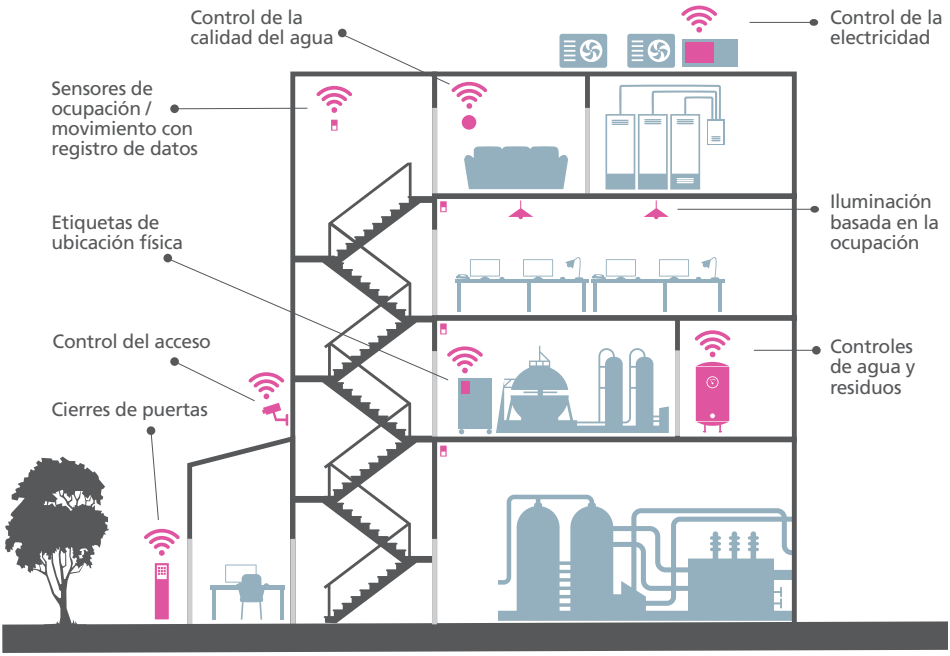


Figura 4: IoT para el medio urbanizado: los datos de los sensores pueden sustentar las misiones de mantenimiento, seguridad, protección, ecología y otras misiones

Instalaciones de producción

Los entornos de producción, como las fábricas, utilizan conjuntos de sistemas interconectados para crear productos. Las tecnologías del IoT se suelen considerar una evolución natural de los procesos ya existentes habilitados por TI y TO, que aportan datos todavía más detallados sobre el inventario, los procesos y los equipos (véase la figura 5). El IIoT puede permitir una mejora de la eficiencia y la seguridad mediante la robótica y la automatización, así como la gestión inteligente de las existencias, el procesamiento de pedidos y la planificación de los ciclos de producción. Los datos operativos de la base de referencia pueden ayudar a aportar información y permitir que se detecte y aborde cualquier comportamiento inusual.

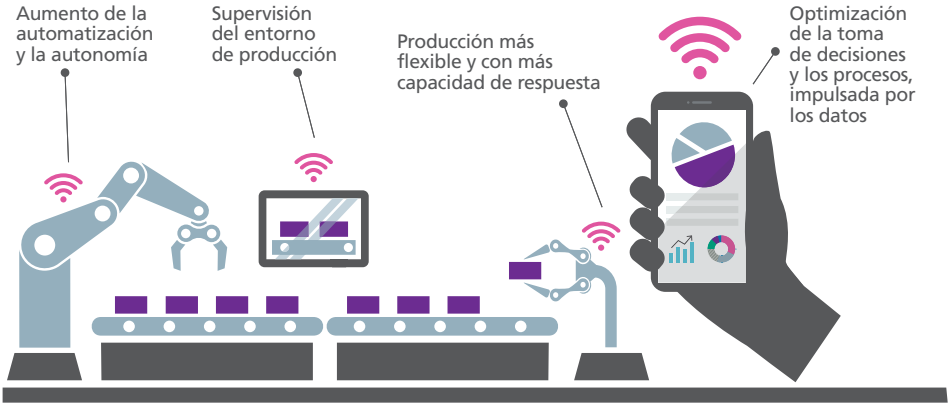


Figura 5: IoT para la producción

Impulsores y posibles futuros del IIoT

El IIoT ofrece la atractiva posibilidad de entender y gestionar sistemas complejos, tanto naturales como artificiales. Las empresas están motivadas a invertir en el IIoT porque las tecnologías inteligentes pueden facilitar nuevas formas de control (y permitir a las organizaciones prever y gestionar los comportamientos de sus sistemas y entornos, o demostrar su conformidad normativa) y nuevas áreas de innovación, tanto en servicios como en productos. Los riesgos aceptables y las medidas de protección de la seguridad cibernética pueden variar, dependiendo de cuál sea la prioridad, el control o la innovación; y un uso que dé buenos resultados deberá tener en cuenta los principales impulsores de la adopción del IIoT, ya que es posible que esos impulsores den forma a la evolución del entorno en el futuro.

Esta evaluación de la previsión establece cuatro impulsores fundamentales de la adopción del IIoT en contextos industriales, que se explican a continuación. Muchos de esos impulsores —o las tecnologías que empujan a las organizaciones a adoptar— también pueden generar riesgos. Esta cuestión se aborda en la siguiente sección de este informe. En este caso, nos centramos en las fuerzas motivadoras, ya que las recomendaciones en materia de gestión de riesgos deben tener en cuenta por qué las organizaciones creen que necesitan esas tecnologías.

Impulsor 1: Mejora de los procesos operativos

Las organizaciones que invierten en el IIoT para mejorar su proceso operativo lo hacen por diversas razones: para ayudar a maximizar la productividad, mejorar la supervisión y reducir la incertidumbre en cuanto a su estado, reducir las ineficiencias del sistema y de las operaciones, generar adaptabilidad en la escala y el ámbito de producción (y así propiciar la resiliencia y la gestión de riesgos), eliminar los riesgos de las cadenas de suministro, y permitir el mantenimiento predictivo y a distancia (véase la figura 6 de la página siguiente). La inversión en el IIoT también puede estar motivada por una normativa nacional, ya sea para apoyar la ventaja competitiva nacional o para permitir más control y supervisión de la infraestructura crítica nacional.

Esas mejoras no siempre están impulsadas exclusivamente por las capacidades inteligentes y automatizadas de los sistemas IoT, sino también por los enormes volúmenes de datos, información y conocimiento que generan. Pueden sustentar análisis que permitan (automáticamente, de forma parcial o completa) la identificación de anomalías y oportunidades de mejorar los procesos.

La mejora de la seguridad en los procesos operativos es un aspecto muy importante, sobre todo en el contexto industrial. El IIoT brinda la posibilidad de ser más eficaces en la supervisión de seguridad, el mantenimiento y la intervención temprana (por ejemplo, con el uso de telemetría IoT en el sector de la energía), el establecimiento de procedencias que se puedan auditar (por ejemplo, etiquetas inteligentes que permitan gestionar el inventario y hacer el seguimiento «desde la granja hasta la mesa»), y el potencial de reducir o reemplazar la presencia de seres humanos en entornos peligrosos.

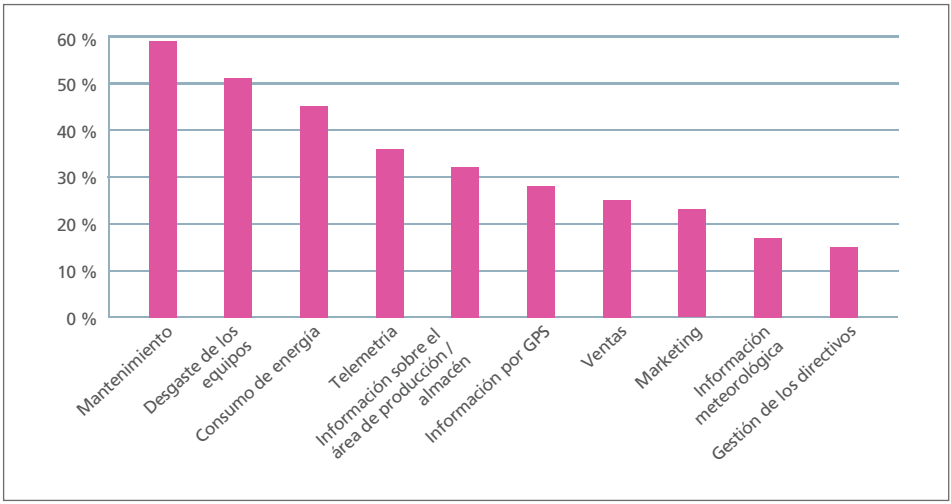


Figura 6: Uso de los datos IIoT por las empresas[4]

Impulsor 2: Agenda ambiental

Teniendo en cuenta que los objetivos de descarbonización tienen una gran prioridad en la agenda mundial y el fracaso en las medidas para luchar contra el cambio climático se considera un riesgo mundial crítico, la industria opta cada vez más por las tecnologías del IIoT para abordar los retos ambientales. La instrumentalización del mundo físico brinda la oportunidad de optimizar la eficiencia energética y mejorar el conocimiento de la situación del consumo. Entre los ejemplos de ventajas se encuentran la optimización de las rutas de transporte, la reducción de las necesidades de transporte mediante la producción local y el mantenimiento a distancia, la minimización del consumo de energía y las emisiones de los procesos de producción, y la descentralización de los modelos de generación y distribución de energía (por ejemplo, una vivienda con paneles solares que contribuyen a la red de energía).

Muchas industrias preguntan: «¿Cómo facilitará esto la descarbonización?» en cada fase del proceso de diseño. La responsabilidad medioambiental se ve reforzada por las presiones económicas de las empresas para demostrar sus credenciales «ecológicas» como ventaja competitiva o requisito contractual o de financiación. La supervisión, mediante instrumentos inteligentes, también facilita la justificación de la eficiencia energética con fines contractuales y de marketing.

Impulsor 3: Mercados de datos

Los proveedores de infraestructuras y las empresas tecnológicas y de transporte tienen la oportunidad de cambiar y convertirse en empresas de datos. Las enormes cantidades de datos que produce la infraestructura, como objetivo y como producto derivado de la actividad del IIoT, dan lugar a oportunidades económicas centradas en los datos. Es probable que los proveedores de infraestructuras ocupen una posición única, como proveedores de flujos de datos protegidos que no pueden ser objeto de ingeniería inversa o simulación, y tengan una gran variedad de usos a la hora de suministrar productos y servicios con destinatarios más específicos. Es posible que las organizaciones quieran aprender de sus datos para mejorar y personalizar productos y aplicaciones y ejecutar servicios basados en datos, o convertirse en vendedores de datos. El valor de los datos se ve magnificado por el hecho de que los datos permiten generar ventajas y oportunidades (para las organizaciones, los clientes y las comunidades) relacionadas con el IIoT; por ejemplo, la plataforma danesa Open Data y la iniciativa The Green Button llevada a cabo por data.gov en los Estados Unidos. En general, es probable que las organizaciones presten cada vez más atención a la propiedad intelectual generada al analizar los datos del IIoT, con el fin de crear información sobre empresas, procesos y personas, que se pueda comercializar y a partir de la cual se pueda actuar.

Ejemplo: Open Data en Dinamarca
Dinamarca ha creado la plataforma Open Data (https://www.opendata.dk/) para que los municipios abran sus datos, con el fin de mejorar la transparencia en la administración, contribuir a los objetivos de reducción de las emisiones de carbono y descubrir colaboraciones y valor económico. Asimismo, la ciudad de Copenhague llevó a cabo un programa piloto para que las universidades, las personas y las empresas compartieran y vendieran diversos tipos de datos. Se prevé que el programa se amplíe en 2020.

Impulsor 4: Conveniencia y experiencia de los clientes

La aceptación del IIoT y las aplicaciones desarrolladas a partir de datos del IIoT también se ven impulsadas por el potencial de mejorar la experiencia de los clientes y su conveniencia. Por ejemplo, las fábricas que tengan que cumplir contratos pueden suministrar a sus clientes información sobre estadísticas e inventarios de productos, así como ofrecer envíos consolidados, reposición automática u otros servicios. El factor de la conveniencia también impulsa la integración del IIoT en la sociedad; por ejemplo, el potencial de mejorar la accesibilidad y la eficiencia de los viajes por medio de redes de transporte inteligentes. A medida que los clientes y los proveedores empiecen a esperar los tipos de servicios y la información en tiempo real que la instrumentalización IoT pone a su disposición, las organizaciones se verán presionadas a facilitar esa información para conseguir contratos.

Características emergentes del IIoT

En conjunto, estos impulsores contribuyen a las características emergentes del IIoT que se prevé que continuarán en el futuro:

- La escala de los dispositivos, las redes y los datos del IIoT está aumentando rápidamente.
- Los sistemas IIoT de las organizaciones e industrias, y entre ellas, cada vez están más conectados entre sí.
- La industria y la sociedad están desarrollando una dependencia crítica de los sistemas IIoT y de sus funciones inteligentes.
- Las comunicaciones más rápidas y fiables entre componentes del IIoT están permitiendo nuevas funciones e interoperabilidad.
- El dinamismo y la agilidad de los sistemas aumentan a medida que van incorporando una gama cada vez mayor de dispositivos, y las redes pueden crearse, crecer, reducirse y desaparecer sin intervención humana.

El panorama del riesgo cibernético del IIoT

Tras analizar las fuerzas motrices y los posibles futuros si las industrias adoptan las tecnologías IoT, el informe pasa a explorar los riesgos. Esta sección abarca el contexto (qué son el riesgo, la amenaza y el perjuicio, y cómo se pueden determinar), así como una exploración más detallada de las diversas categorías de riesgo. Algunos riesgos están relacionados con los impulsores analizados en la sección anterior, pues la nueva innovación genera nueva exposición a riesgos, y algunas amenazas para la seguridad son comunes para todos los dispositivos con internet. Todo ello se analiza brevemente. En particular, se tienen en cuenta las características estructurales que hacen de la seguridad cibernética un aspecto particularmente complicado para los proveedores de infraestructuras críticas.

Contexto

¿Cómo definimos el riesgo?

El riesgo se define como un riesgo presente si se dan:

- una amenaza en el entorno (independientemente de que se trate de un atacante humano o un factor ambiental);
- y un activo en el sistema con una vulnerabilidad que se pueda explotar (esto también se conoce como «superficie de ataque»).

Luego, el riesgo se clasifica y cuantifica evaluando:

- la probabilidad de que el riesgo tenga lugar (ya sea en forma de accidente o de secuencia de eventos que constituyen un ataque);
- y el nivel de pérdida que se experimentaría en caso de manifestarse el riesgo.

El perjuicio se deriva de que se produzca un solo riesgo o se produzcan varios.

Las características emergentes del IIoT, mencionadas en la sección anterior, están cambiando el riesgo cibernético afrontado, y seguirán cambiándolo. Están cambiando el panorama de la amenaza, la superficie de ataque, el conjunto de métodos de gestión de riesgos que pueden utilizar los defensores y los perjuicios que podrían producirse debido a un incidente cibernético. La figura 7 de la página representa el efecto que los cambios en estas variables pueden tener en el riesgo.

Las características emergentes del IIoT están cambiando el riesgo cibernético afrontado, y seguirán cambiándolo

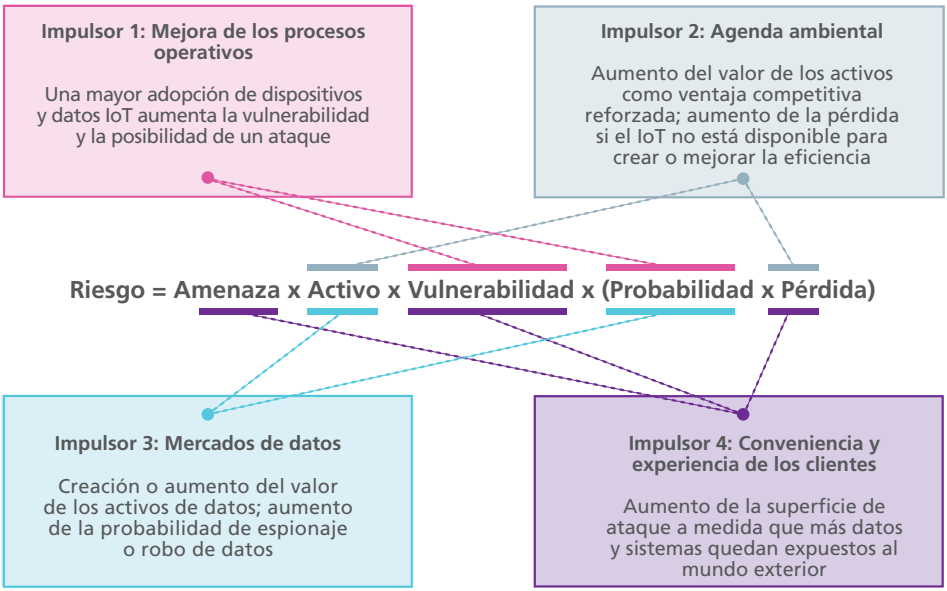


Figura 7: Maneras en que los impulsores del IIoT están cambiando el panorama del riesgo cibernético

Amenaza y perjuicio

El riesgo operativo en todos los entornos con IIoT puede derivarse de accidentes, errores, sucesos naturales y ataques intencionados. Por tanto, es vital que las organizaciones, al planificar su resiliencia, tengan en cuenta tanto los incidentes como los accidentes. Estos términos suelen solaparse y se utilizan de forma distinta en contextos distintos: la distinción importante a efectos de este informe es que los «accidentes» no conllevan intencionalidad. Según la información recibida, las organizaciones suelen tender a tratar los incidentes de seguridad cibernética como si fueran accidentes. Así lo resumió un participante en un taller: «No nos planteamos esto: ¿Y si una persona se propuso que sucediera esto?».

La seguridad se convierte en un requisito esencial para la seguridad en el contexto del IIoT. Los ataques pueden presentarse en una gran variedad de formas: distribuidos o con objetivos, llevados a cabo por actores de la amenaza internos o externos, activos o pasivos, para explotar las vulnerabilidades de los sistemas físicos o del software.

Se prevé que el riesgo de ataques deliberados vaya aumentando conforme se vaya ampliando el IIoT, pues los autores de ataques cibernéticos, desde los delincuentes hasta los estados nacionales, tratan de explotar los sistemas de nueva conexión y las vulnerabilidades recién generadas.

El perjuicio resultante de los incidentes cibernéticos también puede adoptar muchas formas distintas, incluyendo el perjuicio físico, económico, psicológico, social y para la reputación.

A medida que el IIoT vaya avanzando, habrá un mayor potencial de sufrir perjuicios cibernéticos, que se irán volviendo más graves y potencialmente sistémicos con la conexión y la automatización de los sistemas cruciales y esenciales. La figura 8 representa el punto de entrada más habitual de los ataques cibernéticos en las empresas en 2019. La figura 9 de la página siguiente presenta ataques de alto perfil recientes que afectan al IIoT; algunos iban dirigidos específicamente a sistemas de control industrial y otros, indirectamente (y, a veces, es posible que de forma involuntaria), afectaron a funciones relacionadas con el IIoT. En conjunto, presentan un panorama en el que las rutas de ataque están ampliamente distribuidas y, como el malware se puede difundir de formas imprevistas, resulta prácticamente imposible defenderse por completo de esas amenazas o predecirlas. Un ataque que comienza con un mensaje de correo electrónico de phishing (el 31 % de todos los ataques a empresas en 2019) podría dar a los atacantes el control remoto de sistemas de control industrial, así como deshabilitar la columna vertebral de TI (BlackEnergy); un malware sustraído, diseñado con una finalidad, podría acabar teniendo drásticas consecuencias en otros entornos (NotPetya) (ambos ejemplos se han incluido en la figura 9 de la página siguiente).

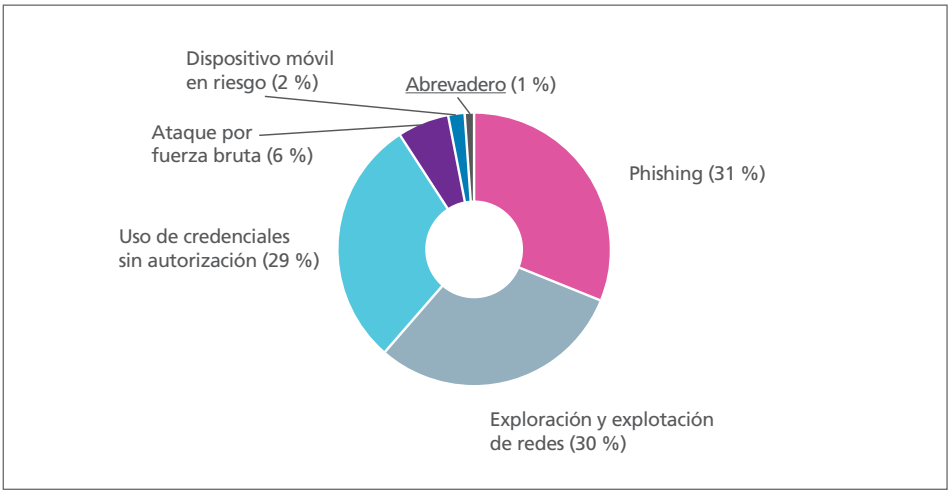


Figura 8: Primer punto de entrada de los ataques cibernéticos a empresas en 2019[5]

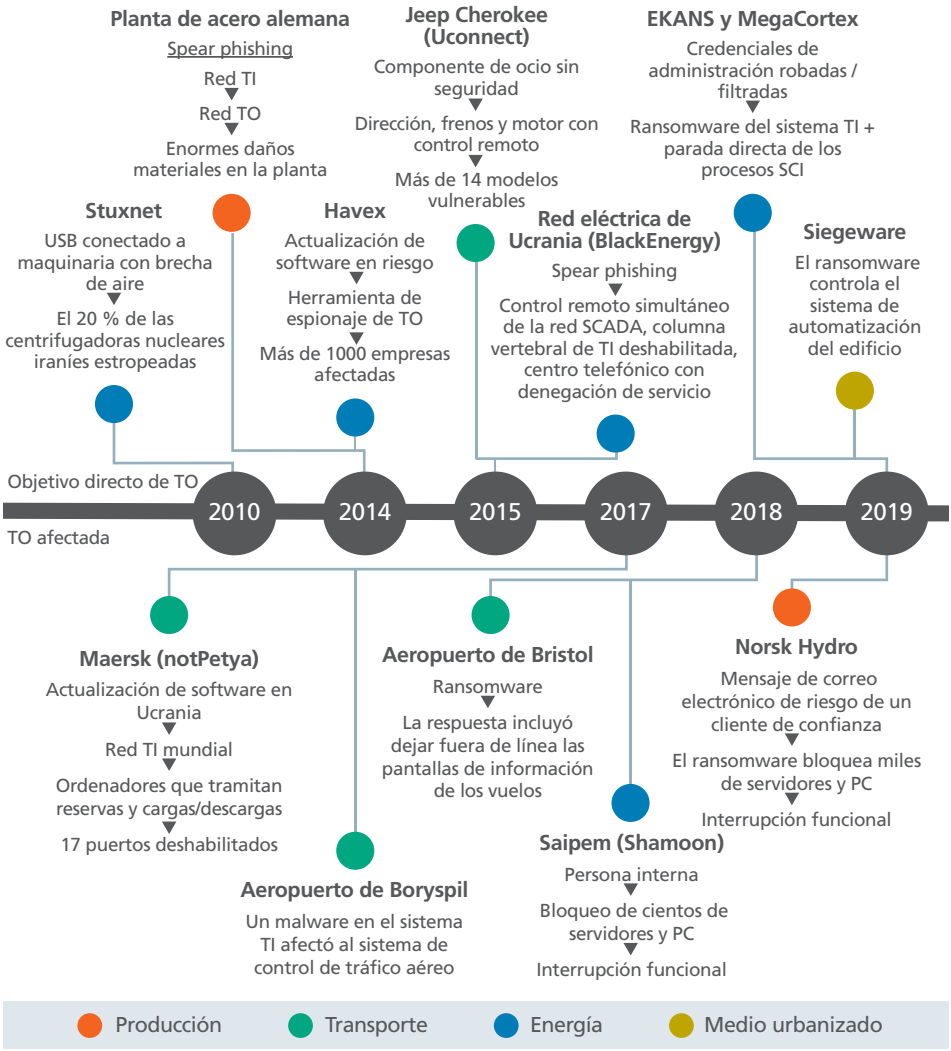


Figura 9: Ejemplos de ataques cibernéticos que afectan a un conjunto de sistemas que utilizan el IIoT

Requisitos especiales de los proveedores de infraestructuras

Una característica fundamental de las industrias incluidas en esta evaluación de la previsión es que, con frecuencia, han asignado una prioridad abrumadora a mantener operativos sus sistemas centrales. Esto puede limitar su variedad de opciones de defensa y dar forma a su percepción de lo que es necesario proteger. Esta prioridad se sustenta en un caso económico explícito (el tiempo de inactividad perjudica a la facturación o los contratos) y, con frecuencia, en un caso de seguridad o adyacente a la seguridad (las personas internas y externas de la organización dependen de que esos sistemas estén disponibles). Las cuestiones jurídicas y de reputación suelen considerarse secundarias (aparte de la seguridad). En el futuro, siguiendo la trayectoria de los impulsores descritos anteriormente, algunas organizaciones podrían pasar de ser un proveedor de infraestructuras a una empresa de datos, o un híbrido de estos dos aspectos. En este caso, tendrán muchas preocupaciones distintas, por ejemplo, prevenir la pérdida de propiedad intelectual, así como un conjunto distinto de estrategias de defensa.

Categorías de riesgo en el IIoT

Los riesgos tradicionales para la seguridad cibernética evolucionan y van aumentando a medida que el IIoT va ampliándose

Los riesgos habituales para los entornos informáticos tradicionales podrían expandirse conjuntamente con la adopción a gran escala del IIoT, debido al aumento de ritmo, escala, densidad y variedad de dispositivos.

- **La nueva tecnología da lugar a una mayor superficie de ataque**. Conforme se van introduciendo dispositivos y se cambian las infraestructuras físicas, se crea una nueva superficie de ataque. Esto puede deberse a vulnerabilidades de la misma tecnología o al uso imprevisto de la tecnología, que crea una superficie de ataque en los procesos operativos, o una superficie de ataque en los seres humanos derivada de su interacción con la tecnología. Todas las vulnerabilidades, si se explotan, pueden dar lugar a más oportunidades de poner en riesgo los datos y sistemas, ya que los atacantes las utilizan como plataformas desde las cuales pueden acceder a los sistemas.
- **Superficie de ataque basada en el software**. Como las funciones y comunicaciones se basan cada vez más en el software (mediante redes definidas por software y funciones de redes virtualizadas), está aumentando la superficie de ataque basada en el software y en la que se pueden explotar las vulnerabilidades. Esto podría acentuar las carencias en las prácticas de desarrollo y mantenimiento del software, que a menudo no son suficientemente seguras, ni siquiera en los entornos ya existentes.
- **Ataques de malware**. El número de ataques de malware (ransomware, exfiltración de datos y sabotaje, por ejemplo) aumentará con el número de dispositivos conectados a internet y basados en software, con la probabilidad cada vez mayor de sufrir un impacto ciberfísico.
- **«Riesgo oculto»**. Existe el riesgo de que los dispositivos no seguros queden «ocultos», o desatendidos de cualquier otra manera, con la extensión de los sistemas conectados. Las metodologías de seguridad podrían omitir los dispositivos clasificados de forma intuitiva como irrelevantes (por ejemplo, una tetera inteligente en la cantina o los dispositivos de los contratistas se podrían usar como vector de ataque, pero podrían ser ignorados en la evaluación de seguridad de la organización).

- **Amenaza continua**. Una conexión constante con el vector de la amenaza (es decir, internet) es prácticamente inevitable y podría resultar inviable desconectar los dispositivos para reducir el impacto de un ataque. Podría resultar difícil mantener los perímetros.
- **Riesgo ciberfísico**. En el mundo del IIoT, los sensores y ordenadores estarán más localizados y dispersos. Resultará difícil (o imposible) proteger físicamente todos los parámetros frente a daños o manipulación. Son ejemplos significativos de ello las redes eléctricas inteligentes (en las que se distribuyen contadores inteligentes, que podrían considerarse una infraestructura crítica nacional, por las casas particulares) y la red 5G (con estaciones de base construidas en el entorno urbano).

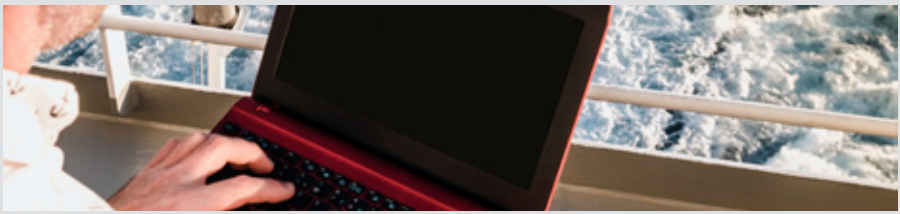
La interconexión genera riesgos comunes y sistémicos

A medida que los sistemas industriales y sus cadenas de suministro se van interconectando, las organizaciones irán compartiendo cada vez más los riesgos. Asimismo, está cambiando la naturaleza de los riesgos sistémicos para los sistemas industriales y el riesgo de un fallo sistémico generalizado podría volverse más probable.

- **Riesgo de propagación del perjuicio**. Como la interoperabilidad entre organizaciones se utiliza para mejorar la eficiencia y apoyar nuevos modelos de negocio, su interconectividad genera el riesgo de que los perjuicios se puedan propagar entre sistemas industriales críticos, con un impacto social sistémico.
- **Responsabilidad indeterminada.** Decidir quién debe asumir la responsabilidad de aplicar medidas de seguridad cibernética operativa llega a ser muy difícil en los sistemas distribuidos (en los cuales no está claro necesariamente quién es el propietario de los activos y los segmentos de red). Decidir quién debe asumir la responsabilidad de la seguridad de los dispositivos y servicios también resulta complicado, ya que las personas y las empresas dependen cada vez más de los proveedores de servicios. Estos factores podrían impedir la aplicación de medidas de seguridad adecuadas.

Ejemplo: crucero

Se diseñó un nuevo crucero teniendo muy en cuenta la seguridad cibernética. Se especificaron incluso los factores de resistencia de los cables de Ethernet. Sin embargo, unos meses después, el buque tuvo que volver para hacer reparaciones, ya que se tenían que cambiar los cables de Ethernet. La tripulación había arrancado los cables para venderlos y los había sustituido por cables de cobre. Los tripulantes ignoraban el riesgo que estaban generando para ellos mismos y para sus pasajeros al hacer esto.



- **Riesgo para la cadena de suministro**. La dependencia de las cadenas de suministro seguirá aumentando el riesgo introducido por componentes específicos. Conforme se va desarrollando la densidad de los dispositivos IIoT y sus conexiones, se van volviendo cada vez más difíciles la asignación, la supervisión o la mitigación de los riesgos para la cadena de suministro: podría resultar difícil saber qué está «dentro» o «fuera» de la cadena de suministro (por ejemplo, vehículos que no transportan sus mercancías en ese momento), o garantizar la procedencia de los dispositivos IoT, que incluyen componentes de varios proveedores.
- **Exposición al riesgo precedente y posterior**. El flujo de datos precedente o posterior podría no estar controlado por una organización (técnica o contractualmente), pero la organización seguiría estando expuesta a los riesgos resultantes. Esto podría adoptar la forma de un riesgo de disponibilidad (por ejemplo, un ataque a un proveedor de servicios de internet que deja fuera de línea a los dispositivos del cliente), pero también podría incluir riesgos derivados de la forma en que las organizaciones de fases posteriores utilizan o protegen sus partes del ecosistema industrial.
- **Titularidad compartida**. Los fabricantes y los clientes comparten los riesgos y la titularidad de los datos. Los contratos están cada vez más relacionados con la prestación de servicios, o con el uso de los datos con licencia, en lugar de definir claramente quién es el propietario de los datos. Los riesgos emergentes se pueden compartir a muchos niveles, incluyendo las empresas, las personas, la sociedad o la comunidad, o a nivel nacional.
- **Exposición al riesgo por medio de los usuarios**. Los usuarios de los dispositivos pueden exponer a riesgos al propietario del dispositivo, e incluso a su fabricante. Los usuarios pueden burlar, ignorar o suprimir las medidas de seguridad. Las fuentes de datos podrían quedar en peligro, o las organizaciones podrían verse obligadas a asumir responsabilidad por los componentes que hayan fallado. Esto también podría conducir a (o derivarse de) una atribución poco clara del fallo; por ejemplo, si la aplicación de la legislación o los aseguradores atribuyen un incidente a alguien (una persona interna) que trabaja con la organización víctima y que introduce accidentalmente malware en el sistema; un delincuente que intenta introducir el malware en el sistema; o un fallo técnico (por ejemplo, un sesgo logarítmico o un incumplimiento por parte del fabricante) en un entorno del IoT. Cuando los dispositivos IoT tienen una interfaz de usuario humana, las personas se pueden convertir en objetivos, lo que podría introducir la superficie de ataque a ámbitos no tenidos en cuenta anteriormente.
- **IoT esclavizado**. Existe el riesgo de que unos botnets compuestos por dispositivos IoT en riesgo puedan coordinarse en ataques muy distribuidos y se utilicen para causar un perjuicio mucho mayor. Se podrán conseguir botnets mucho más grandes, sencillamente debido al número de dispositivos disponibles para hacerlos esclavos, y resultará muy difícil defenderse de esos nuevos botnets del IoT. En caso de que se produjeran daños graves como consecuencia de esos botnets alimentados por el IoT, es probable que la responsabilidad jurídica de los propietarios y fabricantes de los dispositivos se convierta en el foco del control de riesgos.

Se derivan riesgos de los datos creados por el IIoT

El aumento del volumen de datos generado por los sistemas y comunicaciones del IIoT genera un importante riesgo para los datos.

- **Uso malicioso de los datos**. Como el control de las funciones críticas del IIoT depende cada vez más de la toma de decisiones automatizada e impulsada por los datos, el riesgo que plantea la posible corrupción de los datos se vuelve cada vez más grave. La corrupción o la manipulación de los datos utilizados para entrenar los algoritmos de aprendizaje automático, por ejemplo, podrían permitir que los atacantes saboteen los sistemas o modifiquen la funcionalidad de los sistemas críticos.
- **Riesgo de filtración de datos**. Las filtraciones de datos podrían volverse cada vez más frecuentes, ya que los datos, desde los datos personales hasta la información de seguridad nacional, se recopilan y se comparten; y se trata de datos que son valiosos para los atacantes y podrían ser muy delicados para las personas, las empresas y los estados.
- **Impacto de las filtraciones de datos**. Las filtraciones de datos también darán lugar a impactos cada vez más negativos.
  El Reglamento general de protección de datos de la UE (el RGPD) y otras normativas emergentes en materia de protección de datos aportan un componente económico al riesgo para las organizaciones, porque dan lugar a sanciones en caso de producirse una filtración de datos importante. La pérdida o filtración de datos (incluidos los datos de clientes) también conlleva el riesgo de perjudicar la reputación de una organización, y la posibilidad de usar los datos filtrados en espionaje podría perjudicar al margen competitivo de las organizaciones, por ejemplo, con la exposición de la propiedad intelectual o las intenciones comerciales.
- **Disponibilidad de los datos**. A medida que los dispositivos y la toma de decisiones de los seres humanos dependen cada vez más de los datos, la disponibilidad de estos es cada vez más importante. El riesgo podría deberse a que no haya suficientes datos (por ejemplo, ataques que impiden que los dispositivos devuelvan datos de telemetría), o que haya demasiados (es el caso de los ataques de denegación de servicio, que inundan un sistema con más datos de los que su diseño permite procesar).
- **Privacidad.** Las organizaciones podrían descubrir que están recopilando y llevando a cabo el tratamiento de datos relacionados con personas físicas (ubicación, consumo, direcciones IP, etc.). Esto podría dar lugar a un cumplimiento de la normativa relativamente simple (aunque posiblemente oneroso), pero también a un riesgo para la reputación o pérdidas comerciales si los empleados o los clientes llegan a preocuparse por la forma de abordar este problema.

Fotografía de chuttersnap en Unsplash

Surgen riesgos específicos del contexto industrial

Las funciones e interacciones de los sistemas industriales, y de los procesos operativos que se llevan a cabo en el contexto industrial, dan lugar a un conjunto específico de aspectos de la gestión de riesgos que se deben tener en cuenta en el IIoT.

- **Riesgo para la seguridad**. Como las funciones críticas para la protección y la seguridad se establecen juntas (por ejemplo, el control del acceso habilitado por IoT en la puerta de una sala de control de una central eléctrica, o la configuración de seguridad de un control de temperatura conectado a internet en un horno de fundición), existen posibilidades cada vez mayores de que los ataques cibernéticos den lugar a incidentes de seguridad. La protección se vuelve esencial para garantizar la seguridad.
- **Riesgo de sistemas heredados**. Los sistemas industriales SCADA (Sistema de Control, Supervisión y Adquisición de Datos (por sus siglas en inglés) suelen utilizarse durante veinte años o más, mucho tiempo después de que los fabricantes originales hayan dejado de prestar asistencia técnica. Cada vez hay más sistemas heredados, que no se diseñaron para entornos del IIoT y carecen de protección, que se están vinculando a redes de TI o de IoT, lo que supone un riesgo.
- **Riesgo de contagio**. Existe un riesgo potencial de contagio, debido al pequeño número de fabricantes de dispositivos y componentes del IIoT en comparación con el número de usuarios y las opciones de protocolos de comunicación, que son relativamente limitadas. Las vulnerabilidades en tipos de dispositivos o software de uso generalizado podrían afectar a los sistemas de una gran parte de la sociedad y la industria: este riesgo de embotellamiento queda claro en ejemplos como Spectre y Meltdown (una vulnerabilidad de hardware afecta a prácticamente todos los tipos de dispositivos), Heartbleed (una vulnerabilidad de software que afecta a millones de servidores web) y URGENT/11 (una vulnerabilidad de pila de TCP/IP que afecta a miles de millones de dispositivos).
- **Riesgo humano**. Los sistemas de organizaciones humanas (a veces denominados factores humanos) constituyen un riesgo genérico para la seguridad, pero esto tiene un significado específico en el contexto industrial, ya que es probable que esas organizaciones tengan muy arraigadas su formación y su cultura. En los entornos industriales de nueva conexión, el personal sin experiencia en seguridad cibernética (por ejemplo, los especialistas en TO) se está incorporando al ámbito de la seguridad cibernética, y es posible que las organizaciones afronten riesgos debido a la inexperiencia o la falta de coordinación entre los expertos en protección y seguridad.

Las tecnologías emergentes generan nuevos riesgos

- **Informática cuántica**. En el futuro, cuando se hayan construido suficientes ordenadores cuánticos potentes, los adversarios podrán resolver la criptografía de clave pública de la que dependen tantas aplicaciones digitales fundamentales, incluidas las técnicas criptográficas vitales para proteger el IIoT, en lo que respecta tanto al hardware como al software. Los recientes y prometedores avances en informática cuántica demuestran que en un futuro cercano se podrían construir máquinas con esa potencia. Teniendo en cuenta el largo ciclo de vida o los duraderos requisitos de confidencialidad de muchos sistemas IIoT, la informática cuántica constituye un riesgo importante que se debe mitigar con técnicas criptográficas resistentes a la tecnología cuántica.

- **IA y aprendizaje automático**. Estas tecnologías ya constituyen una herramienta habitual en la defensa cibernética, por ejemplo, el uso de un complejo análisis de modelos para detectar ataques y automatizar las respuestas. También es probable que los atacantes aprovechen las novedades continuas en las técnicas de IA y aprendizaje automático para desarrollar capacidades para realizar ataques cibernéticos más potentes. Por ejemplo, la IA se puede utilizar para organizar ataques con botnets más eficaces, predecir contraseñas y agilizar el proceso de descubrir vulnerabilidades de software y generar códigos para explotar esas vulnerabilidades. Asimismo, el aprendizaje de confrontación podría permitir que los adversarios exploten las debilidades de los mismos procesos de IA o contribuyan a cambios de estrategia generales.
- **La infraestructura común de las próximas comunicaciones móviles por 5G** genera un riesgo común, además de la posibilidad de que se produzca una alteración sistémica. Esto podría resultar particularmente cierto cuando la industria deja los elementos de seguridad en manos de la red 5G.

Enfoques actuales de la seguridad operativa y la gestión de riesgos

El riesgo de seguridad cibernética se suele plantear en términos de confidencialidad, integridad y disponibilidad (CID) de los componentes tecnológicos del entorno operativo: sistemas y datos. En la figura 10 se representa la base de las prácticas existentes en gestión de riesgos de seguridad cibernética. Los riesgos se controlan mediante tecnologías y procesos, y se transfieren o comparten por medio del ciberseguro, con el objetivo de habilitar cinco áreas principales de seguridad operativa. La adopción de controles de riesgos y prácticas seguras está impulsada por la reglamentación y la legislación, la competencia del mercado (incluyendo los requisitos contractuales y la seguridad como margen competitivo), la mentalidad de seguridad cibernética de las organizaciones con el fin de mitigar los efectos perjudiciales de un posible incidente cibernético y los requisitos de los proveedores de ciberseguros.

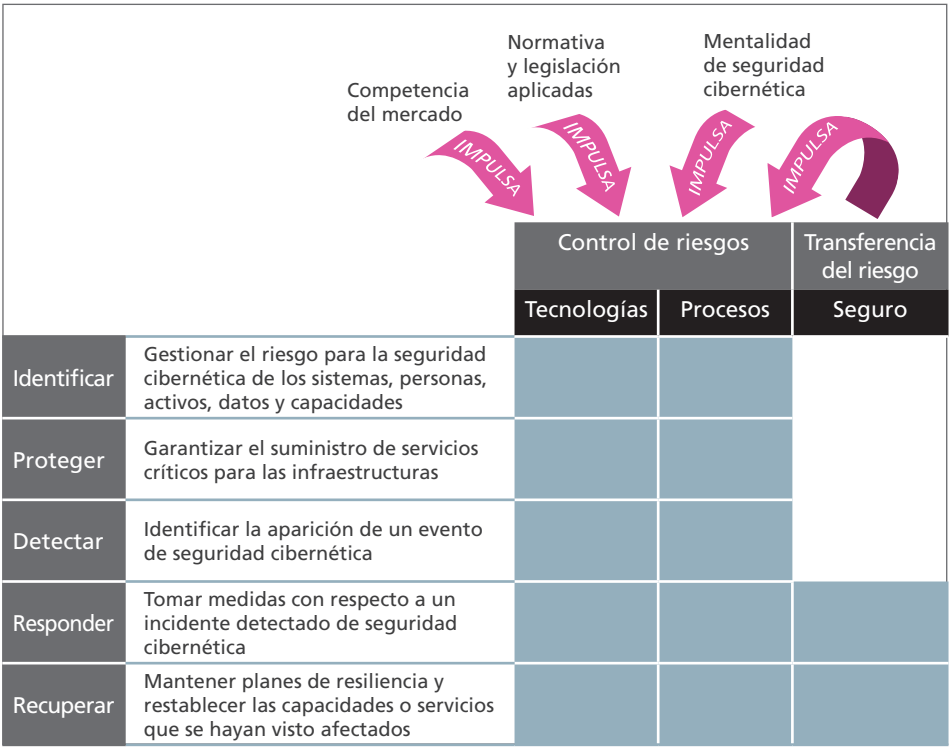


Figura 10: Relación de los controles de riesgos con la seguridad operativa (definida en términos del NIST CSF 5: Identificar, detectar, proteger, responder y recuperar)

Hay diversas normas internacionales, prácticas recomendadas y estructuras de la industria, y métodos de gestión y recomendaciones sobre cómo establecer prioridades en los controles de riesgos de un sistema. Los principales ejemplos son el Cyber Security Framework (Marco de Seguridad cibernética) del National Institute of Standards and Technology (Instituto Nacional de Normas y Tecnología) de EE. UU. (NIST CSF, por sus siglas en inglés)[6]; los Controles críticos de seguridad del Center for Internet Security (Centro para la Seguridad de Internet o CIS, por sus siglas en inglés) (los CSC, por su siglas en inglés)[7]; la norma de seguridad ISO 27001[8]; las pautas de los Cyber Essentials (Componentes cibernéticos esenciales) del el National Cyber Security Centre (Centro Nacional de Seguridad Cibernética) del Reino Unido, destinados a las pequeñas y medianas empresas[9]; y las pautas sobre prácticas recomendadas en materia de gestión de riesgos y específicas para el IIoT, como las proporcionadas por el Industrial Internet Consortium (Consorcio de Internet Industrial)[10, 11], ENISA[12] y el IoT Security Institute (Instituto de Seguridad del IoT)[13]. El Modelo de Madurez en seguridad del IoT[10] del Industrial Internet Consortium procura proporcionar un punto de partida para las decisiones relativas a las inversiones en seguridad. Están surgiendo también prácticas recomendadas relativas al establecimiento de la fiabilidad de los dispositivos y sistemas, por ejemplo, la labor realizada por el Industrial Internet Consortium en este ámbito y las directrices del NIST dirigidas a los fabricantes de dispositivos IoT[14, 15].

Aunque estas normas y guías sobre prácticas recomendadas varían, todas tienen elementos comunes y un subconjunto de controles de riesgo, ya sea de forma explícita o implícita. Estas son las principales clases de control de riesgos en las que se ha logrado un amplio consenso de los expertos, profesionales e investigadores, que las consideran esenciales para abordar el riesgo para la seguridad cibernética. La figura 11 es un ejemplo simplificado de cómo encaja todo esto, que indica dónde podrían aplicarse las clases comunes de control de riesgos en el esquema del IIoT de la figura 1.

Otras clases de control de riesgos, que son críticas para proteger los entornos del IIoT en su conjunto, incluyen una actividad frecuente de evaluación de riesgos y garantía (p. ej., pruebas de penetración); supervisión y análisis de registros de actividad entre sistemas; y desarrollo y ejecución de planes de respuesta a incidentes, así como de planes para la continuidad de las operaciones. Estos no están representados en el diagrama, pero se deben considerar esenciales en todas las organizaciones que tengan que ver con el IIoT.

Tal como refleja la figura 11, el despliegue de controles de riesgos en el IIoT puede resultar bastante complejo, y la interdependencia de esos controles de riesgos (como se refleja en la figura 12 de la página siguiente) solo aumenta esa complejidad. Sin embargo, hay determinadas clases de control (p. ej., los inventarios de dispositivos y la supervisión de registros) que son críticas, ya que una gran parte de controles de otras clases dependen de ellas y, por lo tanto, la gestión de los riesgos resulta incluso más difícil de organizar en la práctica.

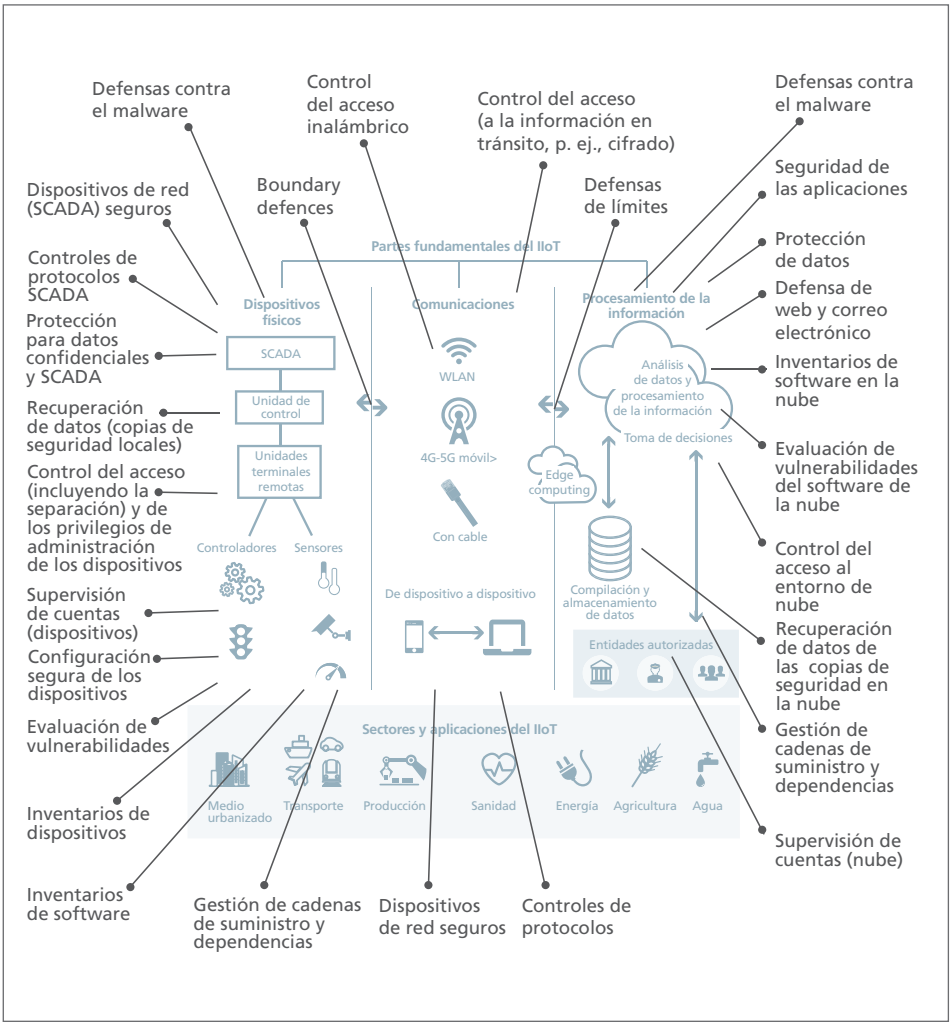


Figura 11: Despliegue de clases ampliamente recomendadas de controles de riesgos para la seguridad cibernética en el IIoT

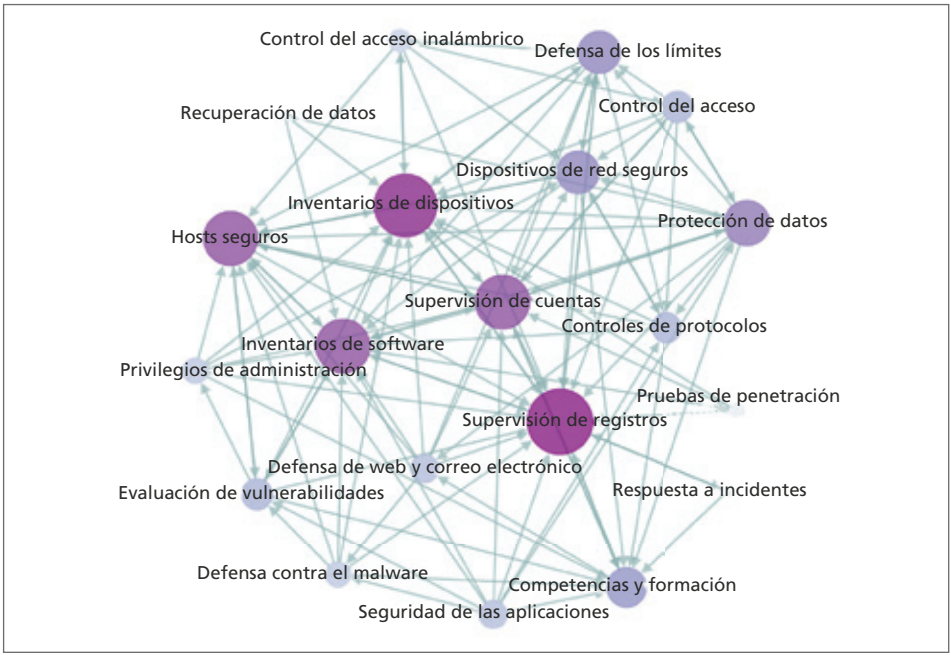


Figura 12: Mapa de dependencias entre los controles de riesgos (adaptación de un trabajo anterior[16]).
El origen de la flecha se encuentra en el control dependiente. El color y el tamaño de los nodos representan el grado en el que un control crea dependencia en otros.

La gestión del riesgo para la seguridad cibernética en los sistemas tradicionales ya afronta muchos retos. Entre ellos se incluyen la tremenda dificultad de intentar representar las complicadas relaciones entre los sistemas técnicos y humanos, y las dificultades de comunicación entre comunidades distintas en las que los marcos para entender el riesgo son fundamentalmente distintos (p. ej., operaciones y miembros del consejo de administración; empresas y autoridades reguladoras; o equipos de abastecimiento y de seguridad cibernética). Habrá enormes diferencias entre las organizaciones y entre los equipos que forman parte de esas organizaciones: su formación, cómo reaccionan ante una crisis, las personas y los sistemas que son de confianza, etc. Muchos de estos retos ya existentes[17] seguirán existiendo y se acentuarán, y aparecerán nuevos retos a medida que los métodos de gestión de riesgos se trasladen al IIoT, lo que generará deficiencias en capacidad.

Seguridad cibernética operativa par el IIoT: Deficiencias en capacidad

El IIoT puede, simultáneamente, permitir el progreso y aumentar el riesgo operativo. Es importante conseguir el equilibrio adecuado, con unas organizaciones que tomen decisiones con la información adecuada y basándose en una comprensión realista del riesgo y un apetito de riesgo claramente articulado. Como se refleja en la red vial inteligente más abajo, la falta de claridad en cualquiera de sus puntos puede provocar que se pierdan oportunidades y se desperdicien inversiones.

Los enfoques actuales de la seguridad operativa y la gestión de riesgos, que se han ido desarrollando durante años en entornos tradicionales de TI, podrían no trasladarse eficazmente cuando se aplican en industrias que, tradicionalmente, han alcanzado un nivel de seguridad cibernética no conectando muchos de sus sistemas a internet. Históricamente, esta desconexión se conocía como la brecha de aire, es decir, que no había una conexión digital directa. Sin embargo, en los últimos años este planteamiento se ha cuestionado como método para aportar seguridad, ya que con frecuencia se utilizan dispositivos de almacenamiento de datos humanos y móviles para conectar dichos sistemas, lo que suprime la brecha (aunque solo sea por poco tiempo). Lo cierto es que el ritmo actual de cambio en las capacidades operativas no se equiparará con la rápida emergencia de nuevos riesgos para la seguridad en entornos de IIoT.

A nivel conceptual, los resultados de la seguridad operativa y la gestión de riesgos descritos en las normas y directrices de seguridad existentes siguen siendo relevantes para el IIoT. No obstante, en la práctica, lograr esos resultados resulta difícil por varios motivos: las capacidades no se amplían, no son interoperables, no son viables técnicamente, no existen todavía o no se han probado, y los incentivos de competitividad en las relaciones en evolución pueden agravar la dificultad. En la tabla 1 de la página siguiente se presentan las deficiencias en capacidad. En las páginas 36–39 se analizan los principales problemas que surgen de este análisis.

Ejemplo: Red vial inteligente
Los túneles de carretera pueden depender enormemente de sensores IoT y de señalización con IoT para los conductores, para poder controlar los flujos de tráfico en tiempo real. En relación con un túnel de mucho tráfico, se abordaron preocupaciones sobre seguridad cibernética por lo que podría suceder si esos sistemas fueran pirateados. Como resultado, el túnel se acabó desconectando y se restableció el control manual, lo que afectó al rendimiento y generó sus propios riesgos para la seguridad (además de desperdiciar el presupuesto invertido en equipar el túnel). Se produjo una enorme brecha de competencias y comprensión que fomentó la tendencia a la aversión al riesgo.


Foto de Burak K, de Pexels

Tabla 1: Brechas de capacidad en seguridad operativa

	¿Qué se ha roto?	¿Se puede abordar?
Identificar		
Identificación de componentes de red / asignación de conexiones	• Las prácticas recomendadas no se amplían • Incentivos de competitividad en las relaciones en evolución	
Convenciones de nomenclatura de los dispositivos	• Falta de interoperabilidad entre los subsistemas IoT • Las prácticas recomendadas no se amplían	
Identificación y protección de la reputación como activo		• Enfoques emergentes, no probados suficientemente
Establecimiento de la titularidad y la responsabilidad de los componentes de red		• Enfoques emergentes, no probados suficientemente
Estrategia de evaluación de riesgos / gestión de riesgos, sobre todo combinando TI y TO	• Falta de interoperabilidad entre los subsistemas IoT	• Podría responder a una solución técnica
Garantías técnicas (pruebas de penetración, exploración de vulnerabilidades, etc.)		• Podría responder a una solución técnica
Gestión de riesgos de la cadena de suministro (para activos inmateriales, como el software como servicio, o para los componentes físicos)	• Las prácticas recomendadas no se amplían • Incentivos de competitividad en las relaciones en evolución	• Enfoques emergentes, no probados suficientemente
Proteger		
Gestión de la identidad y control de acceso	• Las prácticas recomendadas no se amplían	• Enfoques emergentes, no probados suficientemente
Conocimiento y formación	• Falta de interoperabilidad entre los subsistemas IoT	• Enfoques emergentes, no probados suficientemente • Podría responder a una solución técnica
Seguridad de los datos	• Las prácticas recomendadas no se amplían • Incentivos de competitividad en las relaciones en evolución	
Procesos y procedimientos de protección de la información	• Falta de interoperabilidad entre los subsistemas IoT • Las prácticas recomendadas no se amplían	• Podría responder a una solución técnica
Mantenimiento de sistemas y componentes	• Falta de interoperabilidad entre los subsistemas IoT	• Podría responder a una solución técnica

	¿Qué se ha roto?	¿Se puede abordar?
Proteger, continuación		
Tecnología de protección	• Falta de interoperabilidad entre los subsistemas IoT	• Enfoques emergentes, no probados suficientemente • Podría responder a una solución técnica • No viable técnicamente*
Defensa de los límites	• Falta de interoperabilidad entre los subsistemas IoT	• Podría responder a una solución técnica
Detectar		
Anomalías y eventos / procesos de detección	• Falta de interoperabilidad entre los subsistemas IoT • Las prácticas recomendadas no se amplían	• Enfoques emergentes, no probados suficientemente • Podría responder a una solución técnica
Supervisión continua de la seguridad	• Falta de interoperabilidad entre los subsistemas IoT • Las prácticas recomendadas no se amplían	• Podría responder a una solución técnica
Responder		
Comunicaciones de respuesta (informes)	• Las prácticas recomendadas no se amplían • Incentivos de competitividad en las relaciones en evolución	• Enfoques emergentes, no probados suficientemente
Planificación y mitigación	• Las prácticas recomendadas no se amplían	• Enfoques emergentes, no probados suficientemente
Análisis de incidentes	• Las prácticas recomendadas no se amplían	• Podría responder a una solución técnica
Recuperar		
Planificación de la recuperación y mejoras	• Falta de interoperabilidad entre los subsistemas IoT • Las prácticas recomendadas no se amplían	• Enfoques emergentes, no probados suficientemente • Podría responder a una solución técnica
Recurrir a un sistema «estúpido»		• No viable técnicamente
Comunicaciones de recuperación (p. ej., Relaciones públicas)	• Las prácticas recomendadas no se amplían	• Podría responder a una solución técnica

*Algunas tecnologías actuales podrían no ser viables en dispositivos de baja potencia

Enfoques de la evaluación de riesgos

Las metodologías existentes de evaluación de riesgos se establecieron antes de que se desarrollara el IIoT y es poco probable que puedan afrontar la complejidad, el dinamismo y la generalización de este sistema automatizado de sistemas. Mientras los planteamientos actuales requieran la identificación de los activos que se tienen que proteger y el ámbito del sistema, la identificación del ámbito y los límites de los sistemas de IIoT complejos resultará cada vez más difícil. Además, el dinamismo de los entornos del IIoT conllevará la rápida obsolescencia de los panoramas estáticos. Si las organizaciones utilizan los métodos actuales y estáticos para evaluar los riesgos en el IIoT, podrían pasar por alto los nuevos riesgos que surgen en este ecosistema. Se necesita una supervisión más dinámica del riesgo por medio de datos en tiempo real.

Se necesita un cambio colectivo que abandone las evaluaciones de riesgos basadas en el cumplimiento normativo (usando conjuntos de controles, normas y marcos recomendados), algo que no resulta apropiado ni práctico para el IIoT. Se necesitan enfoques de garantía más orientados a los resultados, que empiecen por considerar los posibles resultados para una industria concreta (los perjuicios y los riesgos) y retrocedan para establecer los requisitos del control de riesgos.

Las organizaciones que son dependientes, o codependientes, e interoperables con otras tienen que poder obtener garantías de que los componentes y servicios que compran son fiables y seguros. Pero esto resulta complicado debido a las implicaciones (lo que podría significar que las organizaciones ni siquiera estén seguras de cuáles son sus dependencias) y a los distintos requisitos de garantía entre las distintas partes interesadas. Actualmente no hay una solución obvia para ello, pero en la sección de recomendaciones de este informe se sugieren formas de avanzar.

Procesos de defensa operacional

La variedad de enfoques existentes para la defensa operativa no será suficiente en los entornos del IIoT a gran escala y de rápida evolución. Muchos de los procesos implicados ya constituyen un reto. Por ejemplo, un estudio sobre los procesos de mantenimiento y aplicación de parches de 2019, realizado en 1821 redes de producción, concluyó que el 71 % de los sitios utilizaban sistemas Windows sin asistencia (incluido Windows 7, sin asistencia desde enero de 2020), o que iban a quedarse sin asistencia en breve. Un 62 % utilizaba programas muy obsoletos: Windows 2000 y XP[18]. Es probable que la actualización del firmware se vuelva incluso más difícil de gestionar en entornos del IIoT distribuidos a gran escala, y que los enfoques de actualización existentes no resulten lo bastante eficientes como para satisfacer los requisitos de funcionalidad de, por ejemplo, los sistemas críticos para la seguridad. Se necesitará una nueva ola de mejora continua y procesos dinámicos de seguridad cibernética para identificar los activos, flujos de datos y vulnerabilidades; diseñar arquitecturas seguras y mantener la seguridad de sus sistemas; llevar a cabo la autenticación y el control del acceso; supervisar las redes de IIoT y detectar actividades anómalas; y realizar investigaciones forenses para responder a incidentes.

Procesos de recuperación centrados en los seres humanos

La industria podría estar llegando a un momento crítico para la recuperación después de un incidente de seguridad. Los requisitos de resiliencia, seguridad y protección exigen soluciones alternativas eficaces y, en la mayor parte de los sistemas IIoT actuales, se puede conseguir un mecanismo de seguridad analógico o humano. Los componentes analógicos todavía pueden conseguir una parte suficiente de las funciones inteligentes para mantener los sistemas en funcionamiento, y las personas todavía pueden hacer funcionar los sistemas manualmente en caso necesario, con el fin de mantener un nivel de funcionalidad. Esto se demostró, por ejemplo, en 2017 con la recuperación del ataque con ransomware WannaCry que sufrió el Servicio de Sanidad Nacional (NHS, por sus siglas en inglés) del Reino Unido[20]. A medida que el IIoT vaya avanzando y ampliando su alcance, los sistemas analógicos y los seres humanos dejarán de tener la capacidad de realizar esas complicadas funciones y, en particular, la capacidad de restablecer complicados sistemas de sistemas y entornos de redes. Las soluciones alternativas y recuperaciones manuales podrían dejar de ser una opción para la industria, y el enfoque de la recuperación tendrá que cambiar, aprovechando soluciones automatizadas eficaces.

Tecnologías defensivas

Muchos de los dispositivos terminales de baja potencia que se están incorporando como sensores y controladores a los entornos del IIoT no son adecuados para ejecutar los protocolos criptográficos actuales y, por consiguiente, no satisfarán los requisitos de seguridad de las comunicaciones y de confidencialidad de los datos. El NIST está impulsando el trabajo de normalización de la criptografía ligera y la criptografía poscuántica, pero no está claro en qué grado los usuarios y los productores de dispositivos IoT estarán listos (o tendrán capacidad) para pasar a la fase de los dispositivos y el software listos para la era cuántica. Las arquitecturas emergentes del IIoT también presentan un reto para otros enfoques defensivos técnicos ya existentes, como la segmentación de las redes y las brechas de aire. La separación lógica de los entornos de TI y TO en los sitios y las organizaciones, y entre ellos, podría constituir un conflicto con el estímulo para aprovechar las ventajas de la interoperabilidad y podría generar una falsa sensación de seguridad allí donde sí existan (como sucede en el ejemplo del ataque con Stuxnet[19] en la página siguiente).

Ejemplo: Stuxnet
Stuxnet es un malware descubierto en 2010, desplegado en un ataque contra Irán auspiciado por el estado. Stuxnet atacó los controladores lógicos programables de un modelo específico de centrifugadora utilizada para separar el material nuclear, lo que provocó el suministro de lecturas falsas mientras se activaba la maquinaria para que funcionara fuera de su tolerancia (de forma que las centrifugadoras giraran con demasiada rapidez y se rompieran). Este fue el primer ataque cibernético importante que dio lugar a daños físicos y, además, consiguió «cruzar la brecha de aire», ya que se instaló en una memoria USB manipulada en máquinas que no estaban conectadas a internet.

Deficiencias crecientes en habilidades y concienciación

A medida que las industrias y sus sistemas vayan logrando un alto nivel de conexión por primera vez, mantener su seguridad cibernética se convertirá en una parte crítica de la responsabilidad de una amplia y cada vez mayor parte del personal. Estará incluido el personal que desempeñe funciones que previamente quizás no exigieran contar con competencias en seguridad cibernética. Será necesario invertir más recursos que nunca en la creación de competencias y conocimiento sobre seguridad cibernética (y para algunas organizaciones tal vez se trate del primer esfuerzo conjunto). Los enfoques del conocimiento y la formación tendrán que ampliarse, mejorando los canales de personas que entiendan la seguridad cibernética en el espacio industrial, para abarcar toda la variedad de aplicaciones del IIoT. Una comprensión global de cómo encajan los sistemas IoT en la misión de la organización resulta difícil de enseñar; aun así, es vital que el personal pueda responder de forma apropiada. Esto incluye, por ejemplo, decidir qué sistemas se dejan operativos y cuáles se dejan fuera de línea en caso de producirse un incidente de seguridad cibernética. Los nuevos conceptos constituirán un reto: por ejemplo, el personal de TO y la dirección suelen estar acostumbrados a pensar en las instalaciones físicas, mientras que los límites de las redes (y, por lo tanto, el riesgo) pueden ser difíciles de definir en el IIoT.

En el informe Brecha del personal en seguridad cibernética[21] del Centro de Estudios Estratégicos e Internacionales de 2019, más del 70 % de los empleadores ya afirmaban que la brecha de competencias en seguridad cibernética ya afectaba de manera significativa a sus organizaciones, y el problema seguirá creciendo con la adopción del IIoT. Ya hay algunos ejemplos de ofertas de formación y certificación profesional en este ámbito[22], pero las necesidades de formación en evolución del personal en una gran variedad de industrias, teniendo en cuenta factores como las distintas prioridades comerciales y la diversidad de conocimientos básicos, todavía no se están abordando de manera exhaustiva. Preocupa el hecho de que este reto sea particularmente acuciante en los países en vías de desarrollo, algunos de los cuales están adoptando rápidamente el IIoT en la actualidad, omitiendo algunos de los adelantos tecnológicos de los últimos años y, por lo tanto, sin haber creado necesariamente una base suficiente de personal de seguridad cibernética.

Interdependencia de los controles de riesgos

Hay una gran variedad de brechas previstas allí donde los controles de riesgos y capacidades existentes no se trasladen eficazmente al IIoT (véase la tabla 1, páginas 34–35). El problema es más complicado que simplemente plantearse si las clases individuales de control darán la talla en el IIoT. La deficiencia de cualquier tipo de control podría tener consecuencias para otras personas (y, posiblemente, muchas personas) porque, como se refleja en la figura 12, los controles de seguridad cibernética son interdependientes. La figura 13 representa la cadena de efectos posteriores del fallo de un solo control fundamental. Todas las clases de control dependen, en cierta medida, de tener un inventario de dispositivos, pero es probable que los enfoques actuales del inventario de dispositivos tengan dificultades para hacer frente a la expansión, el dinamismo y la complejidad del IIoT.

Los controles de riesgos se han diseñado sobre todo para un mundo en el que las responsabilidades están claras, donde alguien puede tomar medidas. Esto ya se está complicando en los entornos operativos interconectados modernos y podría empeorar con la proliferación de modelos de datos / dispositivos / servicios compartidos, que son posibles en el IIoT.

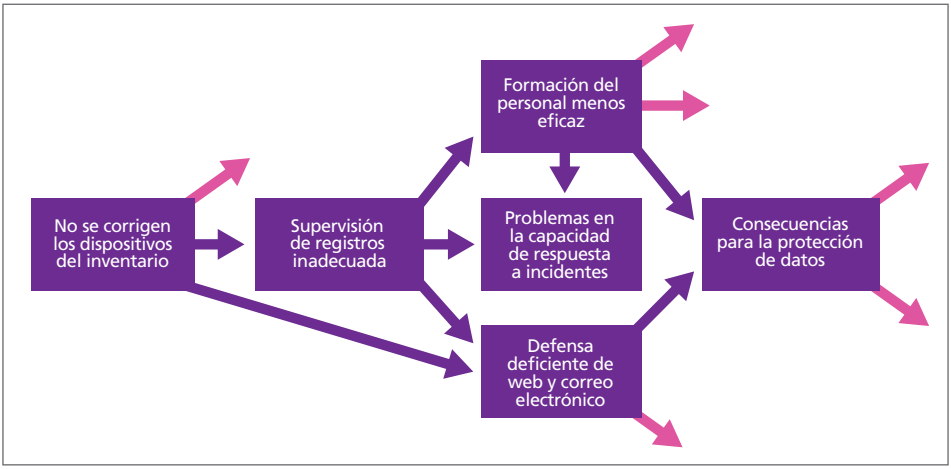


Figura 13: Ejemplo de la cadena de dependencias entre las medidas de control de seguridad cibernética

Práctica de seguridad cibernética: Desafíos para la mentalidad, la reglamentación y los seguros

La reglamentación, los requisitos de los proveedores de ciberseguros y la adopción de una mentalidad de seguridad cibernética en las organizaciones podrían impulsar el progreso de forma que se eliminen las deficiencias en capacidad operativa y se desarrollen controles de riesgos que se puedan trasladar eficazmente al IIoT. Pero esas influencias afrontan unos retos fundamentales.

La reglamentación, los ciberseguros y la adopción de una mentalidad de seguridad cibernética podrían impulsar el progreso de forma que se eliminen las deficiencias en capacidad operativa y se desarrollen controles de riesgos

Mentalidad

En muchas industrias del IIoT, una mentalidad de seguridad cibernética sigue sin ser habitual, lo que constituye un punto de partida complicado desde el cual se puedan lograr esas capacidades operativas. Una mentalidad de seguridad frente a protección (en particular, en las industrias que tradicionalmente han tenido una sólida cultura de cumplimiento de las normas de seguridad) significa que los requisitos de protección suelen salir perdiendo con respecto a los requisitos de seguridad. Asimismo, la mentalidad de seguridad cibernética entra en conflicto con las prioridades de disponibilidad. Por ejemplo, a nivel de liderazgo, si evitar tiempo de inactividad es el objetivo principal, se podría incentivar el mantenimiento en línea de sistemas en riesgo (por ejemplo, para evitar tener que desconectar una central eléctrica). A nivel operativo, es probable que los nuevos sistemas IIoT se gestionen, al menos al principio, mediante equipos de TO, que podrían carecer de un enfoque en seguridad (en particular, en la integridad y la confidencialidad). Suele haber un sesgo cultural que tiende a mantener los sistemas en funcionamiento (aunque sean sistemas heredados o presenten otros problemas de seguridad). Esto podría generar soluciones para mantener y restablecer funciones del sistema que presten muy poca atención a la seguridad.

Mentalidad: Los retos singulares del sector marítimo
Los ingenieros locales de los barcos están acostumbrados a tener mucha independencia y a «resolver los problemas con una llave inglesa y cinta adhesiva». Es posible que sean ingenieros de redes con talento, pero que no tengan necesariamente una mentalidad de seguridad. Por ejemplo, se cuentan historias de ingenieros que «optimizan» la velocidad de una red instalando un parche que elimina la segregación por seguridad. Este reto se agrava porque los barcos pueden recoger piezas de repuesto y nuevos tripulantes en cualquier lugar del mundo.

Convencer a los directivos de una organización de que inviertan en los recursos y el personal necesarios para abordar los retos en seguridad cibernética es un problema constante. Y es un problema particularmente acuciante en las organizaciones que empiezan a convertirse en empresas tecnológicas o de datos conectadas a internet, en las que invertir en recursos de seguridad cibernética no había tenido prioridad hasta ahora. Hay signos de que la mentalidad ya ha empezado a cambiar, y que el conocimiento y la «paranoia» sobre seguridad cibernética en el espacio industrial están aumentando, potenciados por los informes de incidentes de seguridad de IIoT a gran escala, como el ataque de ransomware al productor de aluminio Norsk Hydro en 2019 (se pueden consultar otros ejemplos en la figura 9 de la página 22).

Estos problemas que aparecen internamente en las organizaciones hacen que sea todavía más importante que los enfoques externos eficaces incentiven los avances necesarios en capacidad. La reglamentación y el ciberseguro son dos ejemplos muy importantes, pero también afrontan retos.

Reglamentación

Hay un número creciente de industrias en las que será necesaria la reglamentación sobre seguridad cibernética; es posible que algunas de ellas no hayan sido objeto de reglamentación sobre seguridad cibernética con anterioridad. La reglamentación tendrá que abordar los requisitos tanto de seguridad como de protección de manera integrada (sin que resulten onerosos ni contradictorios), sobre todo en las aplicaciones en las que la seguridad y la protección se solapan. Ya hay varios ejemplos en el sector de la aviación, como la aviónica, que debe contar con seguridad cibernética para poder obtener la certificación de seguridad[23, 24]. La forma en que se han regulado internet y la tecnología hasta ahora es demasiado estática, prescriptiva y reactiva como para ser eficaz en el IIoT, lo que podría obstaculizar la realización de beneficios que sus nuevos modelos de negocio pueden aportar.

Las complicadas interdependencias entre las organizaciones del IIoT, así como la creciente dependencia de las organizaciones con respecto a los proveedores de servicios, generan ambigüedades con respecto a la responsabilidad de proteger los sistemas. Estas, a su vez, generan retos para poder entender cómo se debe regular en este espacio[25]. Por ejemplo, hay opiniones contrapuestas sobre la necesidad de que la reglamentación transfiera del consumidor al fabricante la responsabilidad de la configuración segura de un dispositivo (por ejemplo, contraseñas seguras) y de su integración, ya que los dispositivos conectados a internet se están implementando en aplicaciones cada vez más críticas[26]. Por último, la desintegración de internet en enclaves separados (por ejemplo, con la adopción por parte de China y Rusia de una posición cada vez más fuerte en la política internacional) podría llevar la reglamentación en nuevas direcciones y es necesario tener en cuenta la situación geopolítica.

Reglamentación: ¿Quién toma la decisión?
Una compañía aérea comercial no utiliza enlaces de datos comerciales, que se pueden usar para transmitir mensajes de control operativo de la compañía aérea y para que la tripulación del avión permanezca en contacto con los controladores aéreos. Utiliza 3G en tierra y radiofonía; no utiliza enlaces de datos en el aire porque el otro sistema es más barato. Esto genera riesgos que la compañía aérea acepta. ¿Dónde queremos (las industrias, los gobiernos o la sociedad) permitir que las organizaciones tomen decisiones de este tipo?

Fotografía de Nur Andi Ravsanjani Gusma, de Pexels

Ciberseguro

La industria de los ciberseguros afrontará retos a la hora de evaluar el riesgo cibernético para todo el conjunto de TI y TO de complejos sistemas IIoT, al identificar todos los posibles perjuicios a gran escala y que podrían propagarse, derivados de un incidente cibernético, y al decidir quién es el responsable principal de los incidentes ocurridos en sistemas interdependientes. Existe la percepción de que la provisión existente para ciberseguros para el IIoT no es óptima. El riesgo cibernético marítimo, por ejemplo, se puede asegurar, pero no cubre la TO en toda su extensión ni el valor de la carga perdida o dañada.

El problema del «silencio cibernético» ya existe allí donde, debido a recortes cibernéticos en diversos silos asegurables, se producen pérdidas relacionadas con el aspecto cibernético que se derivan de políticas tradicionales no diseñadas para cubrir el riesgo cibernético. Existe la opinión de que este reto se podría agravar, ya que los límites y las responsabilidades no quedan claras en el IIoT, lo que impide contar con la claridad necesaria para crear políticas eficaces.

Conclusiones estratégicas y recomendaciones

El ritmo actual de cambio en la seguridad cibernética operativa simplemente no es suficiente para satisfacer las probables demandas de un IIoT futuro

El ritmo actual de cambio en la seguridad cibernética operativa simplemente no es suficiente para satisfacer las probables demandas de un IIoT futuro. Se requieren esfuerzos conjuntos por parte de una diversidad de grupos, desde directivos de empresas hasta fabricantes de dispositivos, pasando por las autoridades reguladoras y los gobiernos, para abordar los riesgos emergentes y ampliar las deficiencias en capacidad. Han surgido diversos temas comunes que constituyen la base de las recomendaciones de esta evaluación:

- Los líderes de las organizaciones que utilizan el IIoT deberán actuar para garantizar que cuentan con las prácticas de gestión de riesgos adecuadas para proteger sus sistemas y servicios.
- Investigar las vulnerabilidades y las soluciones de seguridad para muchos entornos de IIoT en vivo no resulta práctico y es potencialmente peligroso. Es necesario poder investigar cómo se puede proteger el IIoT en un entorno seguro y sin consecuencias.
- La interconectividad y la interdependencia cada vez mayores de las organizaciones del IIoT, así como el potencial riesgo compartido y sistémico, darán lugar a retos complejos para decidir quién debe asumir la responsabilidad principal de la seguridad cibernética.
- El IIoT abarcará las cadenas de suministro de dispositivos y la prestación de servicios de terceros en todo el mundo, y se necesitarán enfoques de garantía de seguridad que generen confianza a nivel internacional.

Las recomendaciones se dividen en dos partes: próximos pasos prácticos para los usuarios del IIoT y recomendaciones para realizar más investigación y estudios. El informe finaliza con una llamada a la acción, sugiriendo áreas en las que la Lloyd's Register Foundation y la comunidad en general podrían querer centrar la atención para generar impacto con este informe.

Todas las recomendaciones siguientes se sustentan en un conjunto de principios rectores que todas las partes interesadas del ecosistema del IIoT deberían adoptar para ayudar a crear un entendimiento común de cómo se pueden abordar el riesgo, la responsabilidad y la resiliencia.

- Dar por sentado el fallo como base para la planificación de las situaciones posibles de riesgo, la arquitectura y el desarrollo de estrategias de seguridad.
- Dar por sentado la amenaza interna en los sistemas y las cadenas de suministro.
- Dar por sentado el potencial de riesgo sistémico y buscar formas de identificar y realizar pruebas allí donde pudiera aparecer; y métodos para limitar la propagación del perjuicio.

Mirar hacia el futuro

Internet se ha construido sobre varias tecnologías fundamentales: los paquetes de información se envían a través de una red, usando convenciones TCP/IP relativas a las direcciones (por ejemplo, IPv6) y un conjunto de convenciones de nomenclatura de dominios supervisadas por ICANN. En conjunto, estas tecnologías son muy flexibles y resilientes, pero no se diseñaron teniendo en cuenta la seguridad cibernética.

No está previsto que los sistemas en los que se sustentan cambien rápidamente; esos sistemas son la plataforma sobre la que se ha construido toda la nueva tecnología digital en la actualidad.

En estos momentos, la posibilidad más importante de que haya interrupciones proviene de la informática cuántica. Es posible que, algún día, sea necesario optimizar internet y la tecnología correspondiente para que sean compatibles con los algoritmos y aplicaciones cuánticos, algo que podría alterar de manera fundamental los sistemas existentes. De manera realista, esto solo ocurriría si la industria o la sociedad cambiaran de forma generalizada a un paradigma de informática cuántica (un plazo de tiempo que va mucho más allá del ámbito de este informe). Sin embargo, existe la posibilidad de que los ordenadores cuánticos rompan los mecanismos de protección criptográfica que se usan en la actualidad, lo que exigiría un replanteamiento de los supuestos habituales de seguridad, y es posible que esto se produzca en un plazo de diez años.

Siguientes pasos prácticos para los usuarios del IIoT

Para las organizaciones que utilizan el IIoT en la actualidad, hay varias medidas que deben tener en cuenta al planificar sus operaciones de seguridad o al desarrollar productos y servicios a corto y largo plazo. En general, las organizaciones deberían intentar pasar de una gestión de riesgos basada en el cumplimiento normativo a una gestión basada en los resultados.

1. **Al planificar la gestión de riesgos, siempre hay que tener en cuenta las consecuencias de los perjuicios**. Es posible que, en el futuro, los dispositivos y las tecnologías que ya se están utilizando revelen vulnerabilidades que se puedan explotar y puedan introducir un riesgo. Esto es cierto para todas las tecnologías; sin embargo, es probable que la situación se vuelva más compleja con el IIoT, ya que el potencial de conectividad de las arquitecturas IoT conlleva que el perjuicio tenga más vectores para propagarse. Por consiguiente, a la hora de diseñar arquitecturas de seguridad, será necesario tener en cuenta la posible conectividad, y no simplemente la conectividad que se utiliza hoy en día. Suponer que la conectividad estará limitada a lo que se utiliza actualmente no constituirá una estrategia viable.

2. **Tener en cuenta los posibles fallos de los controles de seguridad a medida que aumente el uso de dispositivos IoT**. Las tecnologías que ayudan a implementar los controles de seguridad se exponen a tantos riesgos como cualquier otra tecnología IoT. Teniendo en cuenta la complejidad de la planificación para posibles futuros, sería prudente identificar los puntos flexibles, los lugares en los que podrían fallar los controles de seguridad y las medidas para identificar las situaciones que se estén aproximando a esos puntos en los que se vaya a producir un fallo. Un buen ejemplo de ello sería poner en marcha mecanismos de detección de activos IoT no incluidos en la arquitectura de seguridad, o que se estén utilizando de una forma no prevista cuando se diseñó esa arquitectura de seguridad. Esto forma parte de la capacidad de conocimiento de la situación de la organización y constituirá una parte necesaria para garantizar que su conjunto de controles siga siendo adecuado para su finalidad.

3. **Usar técnicas que puedan aportar a una organización una evaluación continua de su posición (prácticamente en tiempo real), en lugar de evaluaciones periódicas**. La dinámica del IoT podría dejar rápidamente desfasados los supuestos de amenazas, vulnerabilidades y probabilidades de riesgos. Avanzar hacia la capacidad de mantener el conocimiento de la situación del riesgo conforme va cambiando no solo conllevará un cambio de ritmo en las decisiones sobre seguridad, sino que también permitirá supervisar el cumplimiento de las normas de seguridad y protección más cerca del tiempo real.

4. **Tener en cuenta cómo usan el IoT las cadenas de suministro: considerar que, si fracasan al mantener la seguridad cibernética, generarán un riesgo para los planes de gestión de riesgos para la seguridad**. Una organización debe tratar de lograr el máximo nivel de comprensión y de visibilidad en tiempo real de su cadena de suministro, organizando su seguridad cibernética a lo largo de la cadena y asegurándose de abordar toda vulnerabilidad restante mediante sus controles de riesgos.

5. **Invertir en procesos forenses de preparación**. Este aspecto se considera una práctica recomendada para que las organizaciones se aseguren de estar preparadas para un incidente en cualquier sistema crítico. En un entorno IoT, este requisito se agudiza, ya que la información que se debe recopilar, registrar, proteger y auditar estará más distribuida y ubicada en más dispositivos. Cuando un ciberseguro se utilice como medio para compartir o transferir el riesgo, sería prudente planificar la captura de datos e información junto con los proveedores de seguros, con el fin de garantizar la obtención de la evidencia apropiada para maximizar las pérdidas que se puedan recuperar.

6. **Incluir el planteamiento de posibles situaciones futuras en las evaluaciones de riesgos** (no solamente la posición actual), para intentar obtener algún tipo de medida de protección para el futuro. Dado que la arquitectura IoT se ha diseñado inherentemente para que sea flexible y ampliable (en ambas direcciones), y permita adoptar nuevos análisis y tecnologías, las organizaciones deberían asegurarse de que sus evaluaciones de riesgos no se limiten a sus sistemas tal como están constituidos hoy en día. Se deben considerar los futuros posibles y probables.
   Los planes de gestión de riesgos podrían someterse a pruebas de estrés planteando casos difíciles, por ejemplo:
   - Falta de mantenimiento de los perímetros de seguridad (p. ej., porque el IoT introduzca una cantidad incontrolable de superficie de ataque vulnerable).
   - Superficies de ataque basadas en el personal con presencia en todo el entorno (¿qué pasaría si el IoT permitiera a un atacante desplegar aprendizaje automático para generar ataques muy específicos a compañeros de trabajo?).
   - Base de activos imprevista (cuando los activos conectados a internet no quedan registrados ni documentados al instalarlos, y sobre todo si se encuentran en zonas muy protegidas).
   - Fallo de los controles de seguridad (cuando aumenta la capacidad de las amenazas del IoT y otras tecnologías relacionadas; por ejemplo, si la criptografía no cuenta con suficiente resistencia, los cortafuegos no son eficaces o la formación sobre resistencia a la ingeniería social es ineficaz).

7. **Invertir en formación del personal sobre normas y prácticas recomendadas para IoT:** en particular, sobre los temas relacionados con la seguridad cibernética y los aspectos de seguridad de las tecnologías planificadas o utilizadas. Es importante que una organización lleve a cabo las prácticas recomendadas y las opciones de control, pero no hay una forma «correcta» de impartir formación. Las organizaciones deberían ser conscientes de que es posible que no exista una formación relevante (y que los paquetes de formación existentes podrían resultar inadecuados), y que el aprendizaje más valioso puede obtenerse hablando con compañeros. Las organizaciones más maduras en seguridad cibernética tienden a estar dispuestas a hablar de sus dificultades, en lugar de tratarlas como si fueran secretos comerciales u obstáculos para un ascenso. Lo más importante es garantizar que los empleados entiendan las prioridades operativas y su función en ellas, de forma que puedan tomar buenas decisiones en situaciones complicadas. Las personas deben entender qué se les exige para poder suministrar una política de la organización.

Más investigación y estudios

Está claro que es improbable que el mercado realice el cambio necesario sin que antes se hagan esfuerzos concertados para entender mejor los retos y probar las posibles soluciones. Este informe propone una serie de recomendaciones para realizar más investigación y estudios. Esta lista es deliberadamente breve y va dirigida a aquellos que pueden influir de manera significativa en las limitaciones previsibles de la seguridad cibernética operativa para el IIoT.

Desarrollar un simulador del IIoT y capacidad para realizar ensayos de investigación

La falta de instalaciones de simulación adecuadas significa que las comunidades investigadoras y operativas no pueden explorar todos los posibles fallos o las opciones de recuperación. Por ejemplo, en la aviación civil, un equipo académico tenía varias ideas interesantes sobre la vulnerabilidad de la seguridad, pero no pudo probarlas; no conseguía encontrar un simulador adecuado y no podía permitirse probar las ideas en un avión real, ya que no podía financiar los miles de libras que costaba modificar, reemplazar y volver a certificar el avión después.

Las comunidades investigadoras y operativas necesitan urgentemente la capacidad de generar conocimiento sobre el impacto de la dinámica del IoT en los resultados para la seguridad y la protección cibernéticas, en un entorno que pueda aportar una base de evidencia para innovar en soluciones nuevas para los riesgos.

Existe una profunda necesidad de explorar la gran variedad de fallos y opciones de recuperación posibles en un entorno sin consecuencias. La realización de pruebas con las capacidades y los supuestos de seguridad, así como la realización de pruebas con vulnerabilidades, no resulta práctica y tiene muchas implicaciones para la seguridad en muchos entornos IIoT reales. Los sitios web son el único caso en los que hay una combinación particular de dispositivos y proveedores, pero no se pueden dejar fuera de línea simplemente para experimentar. Entre las preguntas que un simulador y un entorno de ensayos de investigación podrían estudiar se incluyen las siguientes:

- Cómo introducir cortafuegos en las redes: el valor de volver a introducir componentes no inteligentes, soluciones basadas en hardware y componentes centrados en las personas.
- Enfoques de control de las arquitecturas de red y limitación de las amenazas y la propagación de los perjuicios.
- Enfoques del inventario dinámico de dispositivos en sistemas distribuidos a gran escala, y la supervisión y la evaluación dinámicas del riesgo mediante datos en tiempo real.
- El valor de la descentralización y las estrategias de heterogeneidad.
- El impacto de la interdependencia de los controles, la centralidad y criticidad de los nodos y la formación de modelos del contagio resultante.
- Cómo aportar un nivel óptimo de inmunidad y resiliencia frente a una amenaza, incluyendo las estrategias de gestión de parches, pero también el impacto de la formación y los cambios de mentalidad.

- Enfoques eficaces de la recuperación automatizada en caso de producirse un incidente y estudio de la necesidad de conservar posiciones alternativas manuales.
- Normas sobre el cambio de comportamiento y medidas de resiliencia relativa.

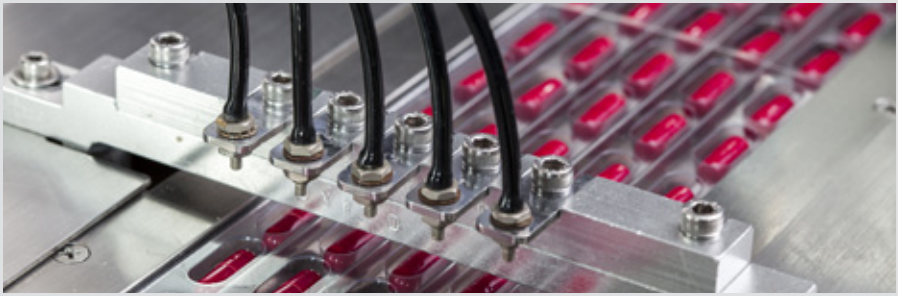
También se podría utilizar como base para probar las técnicas de garantía (incluyendo la comprobación del valor de los programas de garantía que aprovechan la IA) frente a la hiperconectividad, sus tecnologías instrumentales (incluyendo 5G y la virtualización de las redes) y los riesgos generados por su interacción con otras tecnologías emergentes, entre las que se encuentran la IA y la informática cuántica.

Ejemplo: Simulación para el sector marítimo
Una simulación en la industria marítima combinaría una gran cantidad de sistemas marítimos conectados que se encuentran en un barco real y en su ecosistema extendido (proveedores independientes, incluidos los proveedores de la nube), con el fin de analizar las vulnerabilidades de seguridad cibernética de cada uno de los componentes y del sistema en su conjunto.

Pensando en un futuro cercano, con barcos que puedan funcionar de manera autónoma (posiblemente sin personas) y por control remoto, las nuevas amenazas para la seguridad cibernética provienen de la transferencia de datos a través de enlaces con satélites para la detección remota y las optimizaciones del rendimiento, o para realizar el mantenimiento preventivo de los componentes supervisados.

Como ejemplo concreto, teniendo en cuenta los objetivos climáticos de la Organización Marítima Internacional relacionados con el desperdicio de combustible y la reducción de emisiones de gases de efecto invernadero, es razonable esperar que el análisis del desperdicio de combustible que se puede evitar se base en modelos desarrollados con datos recopilados a bordo y que se transfieren a tierra (a un banco de pruebas o un centro de operaciones). Un simulador podría investigar la naturaleza y la extensión de las amenazas para la seguridad cibernética que provienen de esa transferencia de datos y de ese enlace remoto.

Ejemplo: Investigación para el sector de la producción
Con unos procesos de producción que cada vez dependen más de los dispositivos IIoT y del suministro de datos (por ejemplo, la gestión de inventarios justo a tiempo), se ha complicado la creación de modelos de impacto de los distintos tipos de ataques. Si se amplía la investigación, se podría estudiar cómo cuantificar los riesgos emergentes del aumento de la interdependencia, y también cómo se pueden gestionar dinámicamente esos riesgos en tiempo real. Asimismo, en el caso de los procesos de producción que requieren garantías (por ejemplo, la producción farmacéutica), la creación de modelos podría evaluar si esas garantías se pueden mantener frente a un sistema dinámico a gran escala con muchas aportaciones imprevisibles.



Mayor estudio de los modelos de responsabilidad, los aspectos prácticos y las implicaciones para los mercados del IIoT

Si el perjuicio derivado de una falta de seguridad cibernética en el IIoT aumenta de forma significativa, también lo hará la presión para plantear un modelo de responsabilidad, para los proveedores de tecnologías y servicios y para los usuarios de los dispositivos IoT. Anticipando este posible futuro, vale la pena seguir estudiando las formas que esos modelos podrían adoptar, cuál sería su impacto en los mercados, cómo se pondrían en marcha y, en particular, qué modelos se deberían desarrollar que pudieran sustentar un ejercicio de evaluación de costes y beneficios. Este estudio no solo debería tener en cuenta las opiniones nacionales sobre el IoT, sino los mercados internacionales que dependen de los flujos de datos y los posibles códigos de conducta que surgirán con el funcionamiento del IIoT, así como las tecnologías y los servicios de los que dependerán esas infraestructuras.

Explorar enfoques para desarrollar confianza en la cadena de suministro del IIoT, incluyendo la colaboración internacional

El IIoT abarcará las cadenas de suministro de dispositivos (tanto las cadenas de suministro que aportan los dispositivos IIoT como las cadenas de suministro que se basan en esos dispositivos IIoT) y la prestación de servicios de terceros en todo el mundo. Esta colaboración conlleva un riesgo inherente y la comunidad necesita métodos para generar una confianza sólida en las cadenas de suministro y en los servicios compartidos. Este informe recomienda que se lleve a cabo un esfuerzo internacional por explorar vías que den lugar a una plataforma sostenida para esa confianza.

Entre las vías que podrían plantearse se encuentran las siguientes:

- El valor de los programas de certificación de la integridad de los componentes y servicios, y cómo llevar a cabo una supervisión significativa para generar confianza. Esto podría consistir en estudiar cuál sería el nivel mínimo necesario de supervisión de los productos y servicios para establecer la garantía de la cadena de suministro.
- Si se debe utilizar, y cómo, la gobernanza del código abierto como medio para aportar integridad sin que ello también suponga exponer una vulnerabilidad.
- Colaboración entre los fabricantes de dispositivos IIoT para establecer un protocolo de interfaz de los dispositivos con el fin de compartir información sobre seguridad. Esto debería permitir la detección rápida y el seguimiento de la aparición y propagación de riesgos, y permitiría plantear, de forma rápida y prácticamente en tiempo real, el cumplimiento normativo y el riesgo cibernético. Idealmente, los fabricantes deberían superar los formatos y normas de datos de TI y TO.
- El desarrollo de un código de conducta internacional sobre seguridad y protección cibernéticas para entornos del IIoT, que pueda garantizar el cumplimiento de las normas en todas las cadenas de suministro y que dé lugar a una cultura que pueda aportar fiabilidad (teniendo en cuenta cómo se puede regular o autorregular un sistema de este tipo).
- Formas de intentar alinear las culturas de seguridad de TO y TI, para evitar una monocultura, pero desarrollando una interfaz significativa entre las dos que pueda facilitar una gestión de riesgos conjunta.
- Planteamiento de un observatorio de prácticas recomendadas en seguridad cibernética para el IIoT y de la forma en que un esfuerzo global de este tipo podría recopilar datos para sintetizar y compartir el conocimiento, y facilitar un mayor intercambio de datos sobre la eficacia de los controles de riesgos.
- Exploración de la posibilidad de establecer alianzas precompetitivas en torno a una amenaza crítica para la protección y la seguridad; intercambio de información y presentación de informes sobre las vulnerabilidades y la eficacia de los controles, que podrían sustentar el intercambio de información y la distribución de las prácticas recomendadas.

Llamada a la acción

Entender el potencial riesgo sistémico en el IIoT

Teniendo en cuenta la dinámica del IoT, existe una posibilidad muy real de que los ecosistemas del IIoT se desarrollen con un potencial inherente de riesgo sistémico. Cuando las cadenas de suministro abarcan todo el planeta y las organizaciones IIoT tienen un carácter multinacional, ese riesgo sistémico también puede ser mundial. La comunidad de partes interesadas del IIoT necesita, con cierta urgencia, desarrollar la capacidad de predecir los posibles resultados, evaluar las estrategias de respuesta en caso de que surja un riesgo, detectar el riesgo en cuanto surja e, idealmente, planificar soluciones de prevención y disuasión. Existe una necesidad urgente de un programa de estudio que combine los conocimientos especializados relevantes para desarrollar los modelos en un primer momento, luego las capacidades analíticas y, posteriormente, las capacidades informáticas para realizar dichos análisis y comenzar a dar forma a los conocimientos colectivos en este espacio. Una labor de este tipo debe incluir a partes interesadas de todos los sectores relevantes y podría beneficiarse de las aportaciones de expertos de otras industrias con experiencia en la identificación y la mitigación de riesgos sistémicos. Debería tratar de generar información que se pueda llevar a la práctica para la comunidad que investiga y desarrolla tecnología, incluyendo las comunidades internacionales que elaboran las políticas, las autoridades reguladoras, los organismos que elaboran las normas y las compañías de seguros.

Demostradores conceptuales para los entornos emergentes del IIoT

El IoT se va a convertir en una tecnología capaz de sustentar tanto el crecimiento económico en las naciones más pobres como el desarrollo de soluciones para algunos de los problemas más importantes del mundo (calentamiento global, seguridad alimentaria, etc.). Las cadenas de suministro serán globales y el fomento de la seguridad cibernética en el IIoT y las prácticas de seguridad en todo el mundo puede ayudar a desarrollar resiliencia en el sistema. Este informe prevé que valdría la pena contar con capacidad de demostración en la que se implique la industria, pero neutral para los proveedores y dirigida a desarrollar capacidad en las comunidades globales de usuarios y proveedores del IIoT. Esto podría unir a los innovadores en productos y servicios y a los proveedores y usuarios de las infraestructuras de IoT, así como a los representantes de la sociedad civil, con el fin de generar conocimiento sobre los requisitos, los obstáculos y las soluciones.

Apéndice A: Referencias

1 Desai, N. (27 de abril de 2016). **IT vs. OT for the industrial internet – Two sides of the same coin?** [publicación en blog] https://www.globalsign.com/en/blog/it-vs-ot-industrial-internet [consultado el 10 de junio de 2020]

2 Leal-Ayala, D; Castañeda-Navarrete, J; Carlos López-Gómez, C. (2019). **OK computer? The safety and security dimensions of Industry 4.0.** Universidad de Cambridge. https://www.ciip.group.cam.ac.uk/reports-and-articles/ok-computer-safety-and-security-dimensions-industr/download/OK_Computer.pdf [consultado el 10 de junio de 2020]

3 Foro Económico Mundial (2020). **Informe de Riesgos Globales de 2020.** http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf [consultado el 10 de junio de 2020]

4 Tech Pro Research (2019). **The rise of Industrial IoT: Industrial sector leverages IIoT uses.** https://www.techrepublic.com/resource-library/downloads/research-why-industrial-iot-deployments-are-on-the-rise/ [consultado el 10 de junio de 2020]

5 IBM (11 de febrero de 2020). **IBM X-Force: Stolen credentials and vulnerabilities weaponized against businesses in 2019**. https://newsroom.ibm.com/2020-02-11-IBM-X-Force-Stolen-Credentials-and-Vulnerabilities-Weaponized-Against-Businesses-in-2019 [consultado el 10 de junio de 2020]

6 Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) (nd). **Cybersecurity Framework**. https://www.nist.gov/cyberframework [consultado el 10 de junio de 2020]

7 Center for Internet Security (2019). **CIS Controls.** https://www.cisecurity.org/controls/ [consultado el 10 de junio de 2020]

8 ISO (nd). **ISO/IEC 27001 Information security management**. https://www.iso.org/isoiec-27001-information-security.html [consultado el 10 de junio de 2020]

9 National Cyber Security Centre (nd). **Cyber Essentials**. https://www.cyberessentials.ncsc.gov.uk/ [consultado el 10 de junio de 2020]

10 Industrial Internet Consortium (2019). **IoT security maturity model: Description and intended use.** https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_FINAL_Updated_V1.1.pdf [consultado el 10 de junio de 2020]

11 Industrial Internet Consortium (2019). **The Industrial Internet of Things, managing and assessing trustworthiness for IIoT in practice.** [Artículo] https://www.iiconsortium.org/pdf/Managing_and_Assessing_Trustworthiness_for_IIoT_in_Practice_Whitepaper_2019_07_29.pdf [consultado el 10 de junio de 2020]

12 Agencia Europea de Seguridad de las Redes y de la Información (ENISA) (2018). **Good practices for security of Internet of Things in the context of smart manufacturing.** https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot/at_download/fullReport [consultado el 10 de junio de 2020]

13 IoT Security Institute (nd). **Smart cities & critical infrastructure framework.** https://iotsecurityinstitute.com/iotsec/index.php/artefacts [consultado el 3 de julio de 2020]

14 Fagan, M; Megas, KN; Scarfone, KA; Smith, M. (2020). **NIST 8259A, IoT device cybersecurity capability core baseline.** NIST 8259A. National Institute of Standards and Technology. Mayo de 2020. https://csrc.nist.gov/publications/detail/nistir/8259a/final [consultado el 10 de junio de 2020]

15 Fagan, M; Megas, KN; Scarfone, KA; Smith, M. (2020). **Foundational cybersecurity activities for IoT device manufacturers.** NIST 8259. National Institute of Standards and Technology. Mayo de 2020. https://csrc.nist.gov/publications/detail/nistir/8259/final [consultado el 10 de junio de 2020]

16 Agrafiotis, I; Creese, S; Goldsmith, M; Nurse, J; y Upton, D. (2016). **The relative effectiveness of widely used risk controls and the real value of compliance.** Universidad de Oxford. https://www.cs.ox.ac.uk/files/8869/The_Relative_Effectiveness_of_widely_used_Risk_Controls_and_the_Real_Val....pdf [consultado el 10 de junio de 2020]

17 Ponemon Institute (2019). **The fourth annual study on the cyber resilient organization.** https://www.ibm.com/account/reg/uk-en/signup?formid=urx-37792 [consultado el 10 de junio de 2020]

18 CyberX (2020). **2020 global IoT/ICS risk report.** https://cyberx-labs.com/resources/risk-report-2020/ [consultado el 10 de junio de 2020]

19 Karnouskos, S. (noviembre de 2011). **Stuxnet worm impact on industrial cyber-physical system security.** In *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society* (págs. 4490–4494). IEEE. https://ieeexplore.ieee.org/document/6120048 [consultado el 10 de junio de 2020]

20 National Audit Office (2018). **Investigation: WannaCry cyber attack and the NHS.** Report by the Comtroller and Auditor General, UK Department of Health. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [consultado el 10 de junio de 2020]

21 Crumpler, W y Lewis, JA. (2019). **The cybersecurity workforce gap.** Center for Strategic and International Studies, Washington, DC. https://www.csis.org/analysis/cybersecurity-workforce-gap [consultado el 3 de julio de 2020]

22 IoT Security Institute (nd). **Smart cities & critical infrastructure professional certification.** https://iotsecurityinstitute.com/iotsec/index.php/iotsi-certified [consultado el 10 de junio de 2020]

23 UK Civil Aviation Authority (2019). **The cyber security oversight process for aviation (CAP 1753).** http://publicapps.caa.co.uk/docs/33/CAP1753%20OCT2019.pdf [consultado el 10 de junio de 2020]

24 Bellamy, W. (1 de marzo de 2019). **EASA proposes new aircraft cybersecurity certification amendments.** *Avionics International.* https://www.aviationtoday.com/2019/03/01/easa-proposes-new-aircraft-cyber-security-certification-amendments/ [consultado el 10 de junio de 2020]

25 Brass,I; Carr, M; Kruakae, P; y Tanczer, L. (2019). **Cyber security of the Internet of Things.** PETRAS Stream Report. https://www.researchgate.net/publication/335175129_Standards_Governance_and_Policy_Cybersecurity_of_the_Internet_of_Things_IoT_PETRAS_Stream_Report [consultado el 10 de junio de 2020]

26 Wheeler, T. (2020). **Big Ideas: Placing a visible hand on the digital revolution.** Brookings Institution. https://www.brookings.edu/policy2020/bigideas/placing-a-visible-hand-on-the-digital-revolution/ [consultado el 10 de junio de 2020]

Apéndice B: Colaboradores

Andrés Andreu
Director General de Tecnología, Bayshore Networks

Gerry Bonner
Director General de Servicios de flota, China Navigation Company

Martin Borrett
Ingeniero distinguido de IBM; Director General de Tecnología y Ejecutivo Técnico IBM Security Europe

Hugh Boyes
Ingeniero principal de WMG Cyber Security Centre y Director de Bodvoc Ltd

Ruth Boumphrey
Directora de Investigación, Lloyd's Register Foundation

Elisa Cassi
Directora de ciberproductos, Nettitude

Lizzie Coles-Kemp
Profesora de Seguridad de la información, Royal Holloway University of London

Ben Densham
Director General de Tecnología, Nettitude

Duncan Duffy
Responsable de Sistemaselectrotécnicos, Lloyd's Register Marine & Offshore

Taylan Durmus
Asociada, CyLon

Kevin Forshaw
Director de Colaboraciones industriales y estratégicas, Universidad de Plymouth

Derwen Hinds
Asesor técnico estratégico independiente en Tecnologías futuras y emergentes. Profesor honorario, UCL STEaPP, e Investigador docente principal honorario, ISST, Imperial College London

Paul Hopkins
Responsable global de Arquitectura de seguridad, Vodafone

Mohammad Jbair
Asesor senior de Seguridad de SCI, Airbus CyberSecurity

Chronis Kapalidis
Líder de Prácticas de seguridad cibernética, Europa, HudsonAnalytix; Investigador, Universidad de Warwick

Jens-Peter Kjær Jensen
Director senior de Programas, Force Technology

Srinivas Kumar
Director General de Productos, Mocana

Irving Lachow
Vicedirector, Ciberestrategia y ejecución, MITRE

Kenny Lee
Director Técnico, División de Servicios técnicos, Electrónica / Automoción / Inalámbrico, Bureau Veritas

Phil Litherland
Energía y servicios básicos de ICN, PwC

Ross McKerchar
Director General de Seguridad de la información, Sophos

Andrew McKinven
Asesor

Daniel Ng
Consejero Delegado, CyberOwl

Ng Soon Lee
Vicepresidente, Servicios de productos, TÜV SÜD PSB Singapur

Gbenga Olugbodi
Gerente de Programa, Lloyd's Register Foundation

Raghav Pant
Investigador posdoctoral senior, Universidad de Oxford

Jan Przydatek
Director de Tecnologías, Lloyd's Register Foundation

Stuart Quick
Líder del Cibercentro de Excelencia, AXIS Capital

Tim Rawlins
Director y Asesor senior, NCC Group

Simon Reeve
Director de Relaciones comerciales, Lloyd's Register Foundation

Siraj Shaikh
Profesor de Seguridad de sistemas, Institute for Future Transport and Cities (IFTC), Universidad de Coventry; y Director Científico, CyberOwl

Greg Shannon
Director Científico, Carnegie Mellon University CERT

Christina Skouloudi
Ejecutiva de Seguridad de las redes y la información, Agencia Europea de Seguridad de las Redes y de la Información (ENISA)

Matt Smith
Investigador, Universidad de Oxford

Joel Snape
Analista de investigación senior, Nettitude

William Tanuwijaya
Director de Desarrollo comercial, Beckhoff Automation Pte. Ltd.

Jacqui Taylor
Fundadora, Consejera Delegada, FlyingBinary LTD; Smart City Tsar; Asesora experta de la Secretaría del G20 (G20SS) en Economía digital

Vincent Turmel
Vicepresidente de Ingeniería de campo, Bayshore Networks

Janne Uusilehto
Director del Programa de privacidad, Google

Cheryl W
HMG UK

Carolin Weisser Harris
Responsable de Operaciones internacionales, Global Cyber Security Capacity Centre, Universidad de Oxford

Tarah Wheeler
Investigadora en Políticas de seguridad cibernética,New America Foundation

Zhang Yiran
Asesor, Servicios de seguridad cibernética, TÜV SÜD PSB Singapur

Apéndice C: Glosario

5G	La tecnología de quinta generación estándar para las redes de telecomunicaciones móviles. En comparación con las redes actuales, la tecnología 5G permitirá que una mayor cantidad de datos se transmita más rápida y fiablemente, permitirá que se unan más dispositivos a la red y permitirá que las organizaciones segmenten y supervisen su red de comunicaciones de nuevas maneras. 5G es una tecnología fundamental e importante para el IoT.
Abrevadero	Tipo de ataque cibernético en el que un objetivo (habitualmente un sitio web) queda infectado con malware, con la finalidad de infectar a los visitantes de ese objetivo. Por ejemplo, los atacantes podrían infectar o suplantar el sitio web de un proveedor legítimo de la industria nuclear, para infectar los ordenadores de los empleados de la industria nuclear que visitan el sitio web.
Accidente	Un suceso desafortunado que se produce de forma imprevista e involuntaria, y que, por lo general, provoca daños materiales o lesiones (en algunos ámbitos, los accidentes se limitan específicamente a las lesiones sufridas por seres humanos). La distinción importante a efectos de este informe es que los «accidentes» no conllevan intencionalidad. Véase también incidente.
Activo	Un elemento, material, virtual o inmaterial, que tiene valor para una organización.
Actor de la amenaza	El actor de la amenaza puede ser una persona o un grupo de personas que trabajan juntos. Un actor de la amenaza con intención maliciosa se suele considerar un atacante (cuando la amenaza se materializa en forma de ataque), pero los actores de la amenaza también podrían introducir el riesgo de forma no intencionada.
Amenaza	Todo aquello que pueda provocar daños en activos (hardware, software, datos, organización social, etc.). Las amenazas pueden ser intencionadas (p. ej., atacantes) o no intencionadas (catástrofes naturales, casualidad, etc.). Véase también riesgo.
Aprendizaje automático	Conjunto de técnicas utilizadas para permitir que los algoritmos informáticos mejoren automáticamente, «aprendiendo» mediante la iteración, para optimizar la trayectoria basada en reglas hacia cualquier objetivo que se haya establecido. El aprendizaje automático se describe con frecuencia como aprendizaje «supervisado» (que requiere la intervención humana directa) o «no supervisado» (que requiere poca o ninguna intervención humana). Véase también IA.
Aprendizaje de confrontación	Técnica utilizada por los atacantes para provocar que los sistemas de aprendizaje automático generen un resultado erróneo, mediante la alteración de las entradas de una forma calculada para confundir al sistema.

Atacante	Persona u organización que lleva a cabo acciones contundentes, físicas o no físicas, para perjudicar a otra persona u organización. En el contexto de la seguridad cibernética, el atacante es una persona o un grupo que actúa con la intención de provocar perjuicios, robar datos, etc. Fuera del contexto de un ataque concreto, también se conoce como actor de la amenaza.
CID	Confidencialidad – Integridad – Disponibilidad. Tríada de principios que constituyen la base de las cuestiones relativas a la seguridad de la información. Confidencialidad: los datos, objetos y recursos solamente pueden ser consultados por las entidades autorizadas. Integridad: los datos son fiables y correctos, y están protegidos para impedir su manipulación. Disponibilidad: los usuarios autorizados pueden acceder a los sistemas y recursos que necesitan.
CSC	Controles críticos de seguridad del Centro para la Seguridad de Internet, para una defensa cibernética eficaz. Publicación de 20 pautas sobre prácticas y controles recomendados para la seguridad informática. Más información: https://www.cisecurity.org/controls/
Cyber Essentials	Programa de certificación realizado por el Centro Nacional de Seguridad Cibernética (NCSC, por sus siglas en inglés) del Reino Unido, con el fin de ayudar a las empresas a protegerse de las amenazas cibernéticas más habituales y demostrar su compromiso con la seguridad cibernética.
Edge computing	Informática «de periferia» que tiene lugar en la fuente de los datos, o cerca de esta: en muchas redes de IoT, los datos son recopilados por dispositivos de baja potencia y se envían a través de la red a un recurso informático central para su tratamiento, lo que posiblemente da lugar a que ese tratamiento se vuelva a enviar a los dispositivos de baja potencia que se encuentran en la «periferia» de la red, para realizar acciones. El modelo de edge computing empuja una mayor parte del cómputo hacia los dispositivos de la periferia, con frecuencia para minimizar la latencia (el tiempo que tardan las señales en enviarse y regresar). Este modelo requiere que los dispositivos periféricos tengan más capacidad computacional y da lugar a diversos retos para la seguridad, ya que los datos se conservan o comparten en distintos lugares de la red. Por lo general, resulta más complicado proteger esas redes, pero depende del tipo de amenaza esperada.
ENISA	Agencia Europea de Seguridad de las Redes y de la Información (por sus siglas en inglés). ENISA trabaja estrechamente con los Estados miembros de la UE y otras partes interesadas para aportar asesoramiento y soluciones, además de mejorar sus capacidades en seguridad cibernética. Apoya el desarrollo de una respuesta cooperativa a los incidentes o crisis de seguridad cibernética transfronterizos y a gran escala, y prepara los programas de certificación en seguridad cibernética. Más información: http://www.enisa.europa.eu/

Firmware	Software básico y de bajo nivel que da instrucciones al hardware. Por ejemplo, indica a un semáforo que encienda las distintas bombillas para que la luz cambie de color, o indica a una radio que transmita en una frecuencia concreta. En los dispositivos con pocos recursos (frecuentes en el IoT), es posible que el firmware sea el único software ejecutado en el dispositivo.
Hardware	Partes físicas de un ordenador o dispositivo, según el caso, como la unidad central de procesamiento (CPU, por sus siglas en inglés), almacenamiento de datos informáticos, placas base y equipos de comunicación (radio, puertos, etc.). Por lo general, el hardware es dirigido por el software para ejecutar cualquier comando o instrucción.
IA	Inteligencia artificial El término abarca una variedad de técnicas de informática, estadística e ingeniería de la información que permiten que los ordenadores perciban su entorno y den pasos para lograr los objetivos que se les han fijado. Véase también aprendizaje automático.
ICANN	Corporación para la Asignación de Nombres y Números en Internet. Consorcio mundial que supervisa la coordinación del sistema mundial de nombres de dominio, que es el sistema que vincula las direcciones IP legibles por ordenador con las direcciones de dominios en formato legible para las personas, y que ejecuta eficazmente la «guía telefónica para internet» (por ejemplo, vincula http://icann.org con la dirección legible por ordenador 192.0.32.7). ICANN participa en varias iniciativas importantes de gobernanza de internet.
IIoT	Internet industrial de las cosas. Este término se puede utilizar de forma diferente en las distintas comunidades; a efectos de este informe, se interpreta como «las aplicaciones industriales de las tecnologías IoT». Esto abarca tanto los SCI con conexión a internet como los dispositivos más pequeños (a veces incluye los dispositivos IoT para consumidores).
Incidente	Un incidente es un suceso que interrumpe las operaciones normales y que debe notificarse. Un incidente de seguridad es un suceso que podría indicar que los sistemas o datos de una organización han sido objeto de una vulneración o que las medidas aplicadas para protegerlos han fallado. Un incidente puede conllevar intencionalidad, a diferencia de un accidente.
Infraestructura crítica	Término utilizado para describir los activos que se consideran esenciales para el funcionamiento de una sociedad y una economía: la electricidad, el agua y las comunicaciones son infraestructuras críticas clásicas. Este término suele aparecer en el contexto de una infraestructura crítica nacional, pero las redes de activos pueden trascender las fronteras nacionales (como sucede con las redes de energía multinacionales o con la red de transporte marítimo).

IoT	Internet de las cosas. La red de tecnologías que está interconectada y funciona a través de internet y los correspondientes protocolos de comunicación, en gran medida sin intervención de los seres humanos. Con frecuencia (pero no siempre) se trata de un conjunto de dispositivos pequeños y de baja potencia, diseñados para funcionar como parte de un sistema coordinado para la recopilación y el análisis de datos. Entre los dispositivos IoT habituales se incluyen los sensores con conexión a internet (p. ej., medidores de temperatura o de la calidad del aire), balizas (p. ej., etiquetas que transmiten la ubicación) y actuadores (p. ej., motores que abren y cierran las puertas a voluntad). Estos sistemas son diseñados y utilizados por los seres humanos; por lo tanto, cualquier debate sobre IoT debería incluir los sistemas sociotécnicos correspondientes, la formación, las condiciones psicológicas, las interfaces de usuario, etc.
IP	Protocolo de internet (por sus siglas en inglés) (véase también TCP/IP). El protocolo de comunicación principal del paquete de protocolos de internet para comunicarse a través de los límites de la red. Su función de direccionamiento permite la interconexión y, básicamente, establece internet.
IPv6	La versión 6 del Protocolo de internet es la versión más reciente y define las formas en las que los ordenadores pueden establecer direcciones. Véase también: ICANN.
ISO 27001	Organización Internacional de Normalización. La norma de seguridad ISO 27001 especifica un sistema de gestión para conseguir que la seguridad de la información cuente con un control de la gestión y define requisitos específicos. Las organizaciones que reúnan los requisitos podrán obtener la certificación de un organismo acreditado, tras la realización de una auditoría con buenos resultados. Más información: https://www.iso.org/isoiec-27001-information-security.html
Macrodatos	El significado de este término se está ampliando a medida que se desarrolla la ciencia de los datos, pero habitualmente se refiere a conjuntos de datos variados, extremadamente grandes, y a los procesos que permiten entenderlos, con frecuencia mediante IA, aprendizaje automático o métodos estadísticos.
Malware	Software malicioso diseñado para interrumpir, dañar u obtener acceso no autorizado a un sistema informático. Los virus, gusanos, troyanos, adware, spyware y ransomware son tipos de malware.

NIST CSF	Marco de seguridad cibernética del NIST. Aporta un marco de políticas sobre pautas de seguridad informática para que las organizaciones del sector privado puedan evaluar y mejorar su capacidad para prevenir, detectar y responder a los ataques cibernéticos. Más información: https://www.nist.gov/cyberframework. El NIST es el Instituto Nacional de Normas y Tecnología de EE: UU. Forma parte del Departamento de Comercio de EE. UU. y define las normas industriales, por ejemplo, para los procesos y la planificación de seguridad cibernética. Más información: https://www.nist.gov/
Nube	Término utilizado generalmente para describir los centros de datos disponibles para muchos usuarios a través de internet, donde otra persona aloja «sus» datos. Suele adoptar la forma de servicios de suscripción: Gmail, Amazon Web Services, Dropbox, SAP y Oracle son proveedores de servicios en la nube.
Persona interna	Sujeto con acceso legítimo a una red o un sistema. El término «amenaza interna» se puede aplicar a cualquier persona física o jurídica de una organización que genere una amenaza, independientemente de que sea intencionada o no.
Phishing	Son mensajes de correo electrónico fraudulentos que intentan conseguir que los destinatarios visiten sitios web maliciosos, descarguen software malicioso o revelen datos personales (contraseñas, números de tarjetas de crédito, etc.). El phishing se suele describir en las amplias categorías siguientes: • Con un objetivo muy preciso (p. ej., un mensaje que afirma que proviene del director de finanzas de una empresa concreta, indicando a un empleado que debe realizar una transacción financiera urgente). • Con un objetivo preciso (p. ej., envío de un mensaje de correo electrónico a todos los empleados de una empresa concreta, pidiéndoles que hagan clic en un enlace para conseguir un descuento en una cafetería cercana). • Sin objetivo (un mensaje enviado al azar a un gran grupo de direcciones de correo electrónico). Véase también spear phishing.
Ransomware	Un tipo de malware que bloquea el acceso a un ordenador o un activo, hasta que se paga un rescate. Con frecuencia, el ransomware cifra los datos y ofrece a las víctimas la clave de descifrado si pagan el rescate.
Redes definidas por software	Las primeras redes se solían definir por el hardware: los dispositivos estaban conectados físicamente para formar una red. Las redes contemporáneas se definen cada vez más por el software, con un núcleo central que controla la lista de los dispositivos que están dentro y fuera de la red (es decir, se pueden comunicar directamente entre ellos) en cualquier momento.

RGPD	Reglamento general de protección de datos. El marco jurídico de la UE para gestionar y hacer cumplir la protección de datos en relación con los datos almacenados sobre los ciudadanos de la UE (independientemente del lugar del mundo en el que se conserven esos datos).
Riesgo	Posibilidad de que se produzca la pérdida incontrolada de algo de valor: la intersección de activo, amenaza y vulnerabilidad.
SCADA	Sistema de Control, Supervisión y Adquisición de Datos (por sus siglas en inglés). Se trata de sistemas informáticos que recopilan y analizan los datos en tiempo real de los procesos industriales. Subconjunto de sistemas de control de procesos, que garantizan que los procesos funcionen dentro de unos límites normales, los sistemas SCADA se utilizan para supervisar y controlar una planta o unos equipos en sectores como los de telecomunicaciones, control de agua y residuos, energía, refinamiento de petróleo y gas y transporte. Véase también SCI.
SCI	Sistema de control industrial. El SCI abarca el amplio conjunto de sistemas de control, instrumentos y otro hardware utilizado para automatizar o controlar a distancia los equipos industriales. Los subconjuntos de SCI incluyen los sistemas de control de procesos (sistemas automatizados para garantizar que los procesos funcionen dentro de unos límites normales), sistemas de control distribuidos (en los que hay controladores autónomos distribuidos por todo el sistema) y SCADA (controlados más centralmente, que se utilizan habitualmente para automatizar los sistemas que requieren una supervisión continua).
Seguridad cibernética	Este término se utiliza de formas distintas en las diversas subcomunidades, pero habitualmente se utiliza para abarcar la práctica de reducir el riesgo de que se produzca un incidente cibernético. Conlleva la defensa de ordenadores, servidores, dispositivos móviles, sistemas electrónicos, redes y datos contra ataques maliciosos, pero también puede abarcar la formación y el desarrollo de sistemas nuevos (tanto sociales como técnicos), con el fin de ayudar a minimizar la superficie de ataque o activar la resiliencia en caso de ataque.
Seguridad cibernética operativa	La seguridad operativa clásica (OPSEC) se desarrolló en el contexto militar y se centra en tener en cuenta los objetivos y las capacidades del adversario, con el fin de ayudar a aclarar los requisitos de defensa. En el contexto de la seguridad cibernética, esto conlleva centrarse en los modelos de amenaza y utilizar contramedidas para reducir o eliminar la capacidad del adversario para provocar daños.
Software	Conjunto de datos o instrucciones informáticas que indican al ordenador lo que debe hacer. Véase también hardware.
Spear phishing	Otro término para referirse al phishing con objetivos precisos, en el que el atacante intenta obtener acceso a una persona u organización específica.

Superficie de ataque	La suma de distintos puntos de ataque en un sistema, conceptualizada en términos de vulnerabilidades específicas que se pueden explotar. Por lo general, el objetivo es mantener la superficie de ataque lo más pequeña posible. Esto se consigue limitando el acceso al software y los sistemas confidenciales (p. ej., mediante el control físico o digital del acceso) y manteniendo actualizado el software en la medida de lo posible.
TCP/IP	Protocolo de control de transporte y Protocolo de internet. En conjunto, este grupo de reglas regula la forma en que los ordenadores pueden conectarse a internet, con datos divididos en paquetes y encaminados a través de la red hacia su destino, donde los paquetes se vuelven a reagrupar para restablecer los datos originales. Véase también IP.
TI	Tecnología de la información. Uso de ordenadores para almacenar, obtener, transmitir y manipular datos o información. La TI se suele utilizar en el contexto de las operaciones comerciales (con los ordenadores, bases de datos y software que se utilizan en un entorno típico de oficina). La definición de TI no incluye (habitualmente) la TO.
TO	Tecnología operativa. El hardware y el software que detectan o provocan cambios por medio de la supervisión directa o el control de los dispositivos físicos. Por lo general, su definición es distinta a la de TI.
Vulnerabilidad	Debilidad que un atacante puede explotar para obtener acceso no autorizado a un sistema informático o realizar acciones no autorizadas en ese sistema. Las vulnerabilidades pueden influir en cualquiera de las consideraciones CID, permitiendo a los atacantes que ejecuten código, accedan a la memoria de un sistema, instalen malware, roben, destruyan o modifiquen datos, etc.