ISO focus
#132
Su acceso a las Normas Internacionales

Secretos cibernéticos

#132

ISO focus

Enero-febrero 2019

42-45 Sesenta años de seguridad contra incendios

Presentación de ISO 55002 sobre la gestión de activos

El Foro Mundial de Inversiones: escaparate de las normas ISO

Hablamos de inodoros con Bill Gates

2-3 Confianza en seguir dando frutos

Comentario de John Walter.

4-5 El cambio se nota en el aire

La Cuarta Revolución Industrial ya está inmersa en la sociedad.

6-11 Cómo afrontar los riesgos actuales de seguridad de TI

ISO/IEC 27000, nuestra ciberdefensa colectiva.

12-13 Arremetida contra el ciberdelito

ISO/IEC 27001 está contraatacando.

14-23 El diseño de un futuro conectado

ISO/IEC 30141 : fundamentos inteligentes para un mundo virtual.

24-31 La búsqueda de la ciberconfianza

¿Cómo nos afecta el riesgo digital ?

32-33 Plataforma para el desempeño

Cibernormas para un mundo más seguro.

34-41 Cinco cosas que no sabía que se pueden hackear

Atención: usted podría ser la próxima víctima...

46-49 El viaje de los datos, posible gracias a ISO/IEC 20000-1

Por qué la gestión de servicios de TI es importante.

ISOfocus Enero-febrero 2019 – ISSN 2310-7987

ISOfocus, la revista de la Organización Internacional de Normalización, se publica seis veces al año. Usted puede descubrir mayor contenido en nuestro sitio Web en **iso.org/isofocus**, o manteniéndose conectado con nosotros en:

Jefa de Comunicación | **Katie Bird**

Redactora Jefa | **Elizabeth Gasiorowski-Denis**

Redactor | **Barnaby Lewis**

Escritores contribuyentes | **Robert Bartram, Rick Gould**

Editora y correctora | **Vivienne Rojas**

Diseñadores | **Xela Damond, Pierre Granier, Alexane Rosa**

Traductora | **Alexandra Florent**

Traducción al español | **COPANT (Comisión Panamericana de Normas Técnicas)**
www.copant.org

Suscripciones y ediciones anteriores

Si le gusta *ISOfocus*, puede descargar el archivo pdf de manera gratuita o suscribirse para recibir los números impresos a través de nuestra página web **iso.org/isofocus**. También puede ponerse en contacto con nuestro servicio de atención al cliente en **customerservice@iso.org**.

Contribuciones

Usted puede participar en la creación de esta revista. Si cree que su contribución puede aportar un valor añadido a cualquiera de nuestras secciones, póngase en contacto con **isofocus@iso.org**.
Las opiniones expresadas son las de los respectivos contribuyentes y no son necesariamente las de ISO o las de cualquiera de sus miembros.

MIXTO Papel procedente de fuentes responsables FSC® C008839

Esta revista está impresa en papel certificado FSC®.

myclimate neutral Printed Matter 01-14-277370 myclimate.org

Confianza
en seguir dando frutos

***John Walter**, Presidente de ISO.*

Ahora que cumplo un año como Presidente de ISO, siento un profundo orgullo y la satisfacción del deber cumplido. Al volver la vista al último año –de hecho, a la última década– salta a la vista todo lo que ha logrado ISO y la eficacia con la que lo ha hecho. Este desempeño no solo se centra en nuestros sólidos procesos de desarrollo de normas y nuestros documentos, sino también en cómo hemos logrado ofrecer asistencia y guía a muchos de nuestros miembros de todo el mundo.

Me habrán oído decir en varias ocasiones que los desarrolladores de normas de todo el mundo son los mejores ejemplos de amistad, cooperación, confianza y relaciones de trabajo de igual a igual. Abrimos puertas y construimos puentes. Hacemos amigos y fomentamos la confianza. Respetamos y valoramos a cada persona y a todos los organismos nacionales de normalización. No discriminamos contra ninguna persona, organización o nación. Acogemos y aceptamos a todos los participantes por su compromiso sincero con las Normas Internacionales y el uso de estas normas en beneficio de nuestra aldea global. El mundo necesita más ISO.

Por ello, todos estamos obligados a mantener y desarrollar ISO como una organización plena de vida y vigor. El mundo no espera menos de nosotros. Cuando me he reunido con líderes industriales y gubernamentales de todos los rincones del planeta, siempre me he sentido bienvenido. Todos buscan activamente soluciones a desafíos serios y críticos. Con frecuencia describimos y abordamos las opciones que nos ofrecen las Normas Internacionales. Al final de estas sesiones, todos han expresado su deseo unánime de trabajar con ISO para colaborar, cooperar y apoyar. Este compromiso me llena de inspiración y es uno de los motivos por los que el Secretario General Sergio Mujica y yo proseguimos con nuestras fructíferas conversaciones con los principales líderes mundiales.

Sin embargo, tenemos que hacer más : tenemos que llegar más lejos y llamar a la acción ; seguir aportando soluciones. El futuro de nuestro mundo puede depender de nosotros.

Generar valor para nuestros miembros es un objetivo clave que Sergio y yo compartimos. Estoy encantado de cómo hemos hecho honor a nuestro compromiso y cómo hemos conectado con la comunidad global. Sergio habla con conocimiento, inteligencia y autoridad acerca de todas las partes de la organización y todas las regiones del mundo. Contamos con el apoyo incondicional de todos los miembros del Consejo de ISO, con una participación y un compromiso crecientes con nuestros procesos de gobierno revisados. Este compromiso redundará sin duda en beneficio de ISO.

El compromiso con las organizaciones internacionales ha sido una parte crucial de nuestro trabajo. El año pasado, como Presidente de ISO, me comprometí ante ustedes a crear lazos más fuertes con nuestra organización hermana, la Comisión Electrotécnica Internacional (IEC). Me emociona y complace ver cómo la cooperación y la colaboración aumentan entre las dos organizaciones. Buena parte de este éxito se debe al impulso y el liderazgo de un amigo duradero y fiable, el Presidente de la IEC Jim Shannon.

De cara al futuro, tendremos que redoblar nuestros esfuerzos para apoyar la Agenda 2030 para el Desarrollo Sostenible de Naciones Unidas, diseñada para reconducir nuestro mundo por un camino más resiliente y próspero. Es importante que empleemos bien nuestro tiempo y avancemos con la máxima decisión y agilidad. Con solo 11 años por delante, nuestro compromiso con la ONU debe ser más sólido que nunca ; seguiremos dándolo todo para ayudar al mundo a lograr los 17 Objetivos de Desarrollo Sostenible.

Estos esfuerzos son solo una parte de nuestra labor –si bien una parte importante– para afrontar los enormes desafíos mundiales. Personalmente, lo que más me preocupa es la ciberseguridad, sin duda una de las cuestiones más candentes del mundo moderno. Si permitimos que las ciberactividades disruptivas y dañinas interrumpan o alteren nuestras interconexiones globales, todos nuestros procesos y desvelos quedarán en nada. La conectividad digital tiene un papel central en liberar la innovación y la prosperidad para la humanidad. No obstante, las crecientes amenazas cibernéticas suponen un escollo en nuestro camino común hacia el progreso, y los gobiernos y la industria deben desarrollar sus capacidades en esta área. Rápido, además.

Atrás quedaron los días en que las empresas podían confiar cualquier quebradero de cabeza de ciberseguridad al departamento de TI. Son cuestiones que hoy son ya un problema de sostenibilidad y supervivencia del negocio. Las Normas Internacionales son esenciales para garantizar unos programas rigurosos y eficaces en materia de ciberseguridad. Como he declarado ante gobiernos y líderes de la industria de todo el mundo, ISO está en una magnífica posición en esta era de transformación masiva del ciberespacio ; estamos creando una cartera de normas de primera clase que las organizaciones pueden integrar en sus procesos de negocio y sus productos.

Al afrontar un nuevo año, no sabemos a ciencia cierta qué esperar en cuanto a ciberseguridad. ¿ Qué nos deparan los cibercriminales para 2019 ? ¿ Qué debemos hacer para protegernos de ellos ? Espero que este número de *ISOfocus* dé respuesta para algunas de estas cuestiones. En nuestra frágil realidad sobre ciberseguridad, las Normas Internacionales gozan de mayor demanda que nunca.

A título personal, pienso que quienes participamos en el sistema de Normas Internacionales tenemos la obligación moral de dejar de lado nuestras diferencias, olvidar rencillas y abrazar la globalización. Aislarnos y construir muros entre nosotros supondría un enorme fracaso institucional y ambiental y nos llevaría al desastre. Como miembros de esta civilización internacional, podemos y debemos abordar juntos los desafíos que afronta nuestro planeta. ¿ Desea alguno de ustedes dejar en herencia a sus hijos un planeta invivible por meros intereses personales o negligencia ? Las normas ISO ya están ayudando a abordar y superar desafíos globales y debemos asegurarnos de que siga siendo así en el futuro. Hay demasiado en juego. Sigamos progresando juntos. ■

El cambio se nota en el aire

#4thindustrialrevolution

CITA Bertrand Piccard
Lo que opina la figura estelar detrás de Solar Impulse sobre el papel de las normas en el mundo

Para resaltar la importancia de las normas para la Cuarta Revolución Industrial, ISO desarrolló una campaña en sus plataformas de redes sociales entre el 12 y el 26 de octubre de 2018. Tras el lanzamiento con ocasión del Día Mundial de la Normalización, nos centramos en cómo las normas ISO que apoyan la adopción de sistemas ciberfísicos supondrán un beneficio para la vida diaria de las personas en áreas como salud y seguridad, transporte, protección de datos personales y biotecnología.

MÁS DE
3 300 000
IMPRESIONES

CAMPAÑA
La campaña reunió a miembros de ISO, expertos de la industria y otras partes interesadas, que hablaron sobre la necesidad de desarrollar normas que permitan garantizar una adopción integral de las tecnologías emergentes en nuestra vida diaria

MÁS DE
500 CONTRIBUCIONES
A NUESTRA CAMPAÑA

THINGLINK Las Normas Internacionales y la Cuarta Revolución Industrial
Visión general de algunos ISO/TC relacionados

VÍDEO Normas e inteligencia artificial Parte 1
Entrevista con Wael William Diab, Presidente del ISO/IEC JTC 1/SC 42

VÍDEO Normas e inteligencia artificial Parte 2
Entrevista con Wael William Diab, Presidente del ISO/IEC JTC 1/SC 42

MÁS DE
15 500
VISUALIZACIONES
DE VÍDEOS

MÁS DE
1 700 000
USUARIOS
DESTINATARIOS

VÍDEO Normas y cadena de bloques
Entrevista con Philippa Ryan, ISO/TC 307/WG 3, *Contratos inteligentes y sus aplicaciones*

CÓMO AFRONTAR

LOS RIESGOS ACTUALES DE SEGURIDAD DE TI

Foto: Kevin Ku/Unsplash

por Barnaby Lewis

Expertos de la industria estiman que las pérdidas anuales debidas a ciberdelitos podrían llegar a los USD 2 billones el año próximo [1]. Un sinfín de nuevos objetivos se suman cada día, especialmente dispositivos móviles y « cosas » conectadas. Por ello, es esencial un planteamiento conjunto.

El atractivo del ciberdelito para los ciberdelincuentes es evidente : entramado de interacciones, sanciones relativamente leves, enfoques dispares sobre el blanqueo de capitales y ganancias potencialmente enormes. La clave es la preparación y prever las vulnerabilidades, además de la resiliencia, en las interacciones con los sistemas de gestión generales ; es aquí cuando entra en acción la norma ISO/IEC 27001 sobre sistemas de gestión de seguridad de la información (SGSI).

Se trata del buque insignia de la familia de normas ISO/IEC 27000 publicada por primera vez hace más de 20 años. El comité técnico conjunto ISO/IEC JTC 1 de ISO y la Comisión Electrotécnica Internacional (IEC) fue creado para proporcionar un punto para la normalización formal de la tecnología de la información. Con el tiempo, se ha actualizado y ampliado continuamente hasta incluir más de 40 Normas Internacionales que abarcan todo lo relativo a la creación de un vocabulario común (ISO/IEC 27000), gestión de riesgos (ISO/IEC 27005), seguridad en la nube (ISO/IEC 27017 y ISO/IEC 27018) y técnicas forenses para analizar pruebas digitales e investigar incidentes (ISO/IEC 27042 e ISO/IEC 27043, respectivamente).

Estas normas no tratan solo de gestionar la seguridad de la información, sino también a ayudar a identificar a los criminales y llevarlos ante la justicia. Por ejemplo, ISO/IEC 27043 ofrece directrices que describen procesos y principios aplicables a diversos tipos de investigación, entre otras : acceso no autorizado, corrupción de datos, fallos del sistema y violaciones de la seguridad de la información en empresas, así como otras investigaciones digitales.

1) Steve Morgan, “ Cyber Crime Costs Projected To Reach $2 Trillion by 2019 ”, Forbes Online

La clave es la preparación y prever las vulnerabilidades.

Sacar ventaja en el terreno de juego

Que esta familia se pueda aplicar a las necesidades de las empresas grandes y pequeñas mediante la evolución constante es una gran responsabilidad del subcomité SC 27 de ISO/IEC JTC 1 sobre técnicas de seguridad de TI. En gran parte, hay que agradecer el aporte de personas como el profesor Edward Humphreys, quien dirige el grupo de trabajo encargado de desarrollar los SGSI, que siguen siendo una de las herramientas de gestión de riesgos para combatir los miles de millones de ataques anuales [2] que, de otra manera, seguirían ampliando sus objetivos y métodos.

Conversé con el profesor Humphreys, un especialista en seguridad de la información y gestión de riesgos con más de 37 años de experiencia en el mundo académico y de consultoría. Comencé preguntándole sobre los principios básicos de los SGSI. ¿ Cómo pueden adelantarse a los delincuentes para proteger tanto a empresas como a consumidores ?

2) “ Internet Security Threat Report ”, Volumen 23, Symantec, 2018

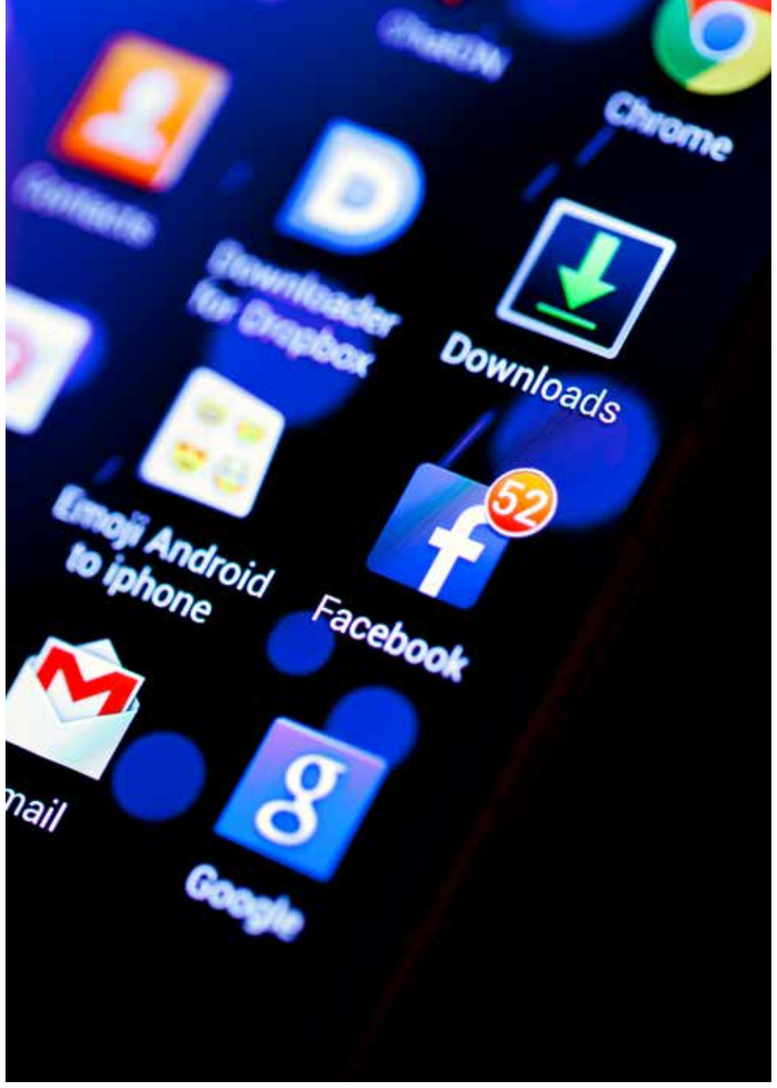
« Es cierto que los peligros que amenazan la información, procesos de negocio, aplicaciones y servicios evolucionan continuamente. ISO/IEC 27001 es una norma que mejora continuamente, por lo que el proceso de gestión de riesgos integrado permite que las empresas estén actualizadas en su lucha contra el ciberdelito ».

Según el profesor Humphreys, que la norma ISO/IEC 27001 mejore continuamente implica que una organización puede evaluar sus riesgos, poner en marcha controles para mitigarlos y, después, monitorear y revisar dichos riesgos para mejorar la protección según se requiera. Así, siempre se está listo y preparado frente a ataques : « Si se usan adecuadamente, con los SGSI la organización puede sacar ventaja en el terreno de juego al adaptarse al entorno de riesgo en evolución que suponen Internet y el ciberespacio ».

De amenazas a oportunidades

En el plano empresarial, dar forma y mitigar las amenazas que se ciernen desde todos los ángulos es una tarea formidable. Existe una necesidad clara de usar un sistema de seguridad unificado e integrado en todo el negocio y, dada la complejidad de las interrelaciones, pregunté al profesor Humphreys si los SGSI se pueden aplicar a empresas pequeñas y medianas (pymes). « Los SGSI se pueden aplicar a cualquier tipo de organización y actividad comercial, incluidas las pymes. Muchas pymes forman parte de cadenas de suministro, por lo que es esencial que controlen y gestionen la seguridad de su información y ciberriesgos para protegerse tanto ellos mismos como a otras personas ». El profesor Humphreys aclara que las obligaciones de una empresa se suelen definir en acuerdos de nivel de servicio (ANS) –contratos entre miembros de la cadena de suministro– que detallan los requisitos y obligaciones del servicio, además de establecer responsabilidades legales, y es aquí donde los SGSI suelen ser una parte fundamental de tales acuerdos.

Naturalmente, existen desafíos adheridos al negocio en línea de las pymes, compensados con creces por el gran potencial que ha desplegado Internet. Se podría alegar que las empresas más pequeñas han sido las que más beneficio han obtenido de la tecnología, una cuestión planteada recientemente por el embajador Alan Wolff de la Organización Mundial del Comercio. En la Asamblea General de ISO de 2018, Wolff afirmó que « cualquiera –con un diseño, con una simple computadora, que se pueda meter en la red, que tenga acceso a una plataforma– puede formar parte del comercio internacional ».



Puede que la vida privada sea menos compleja que el comercio mundial, pero también está en juego.

Las ventajas del desarrollo social y económico son enormes : Internet aporta presencia global a cada vez más personas y comunidades que antes estaban aisladas. Sin embargo, se necesita un planteamiento demostrado y sensato como los SGSI para reducir los aspectos negativos. Tal y como me recuerda el profesor Humphreys, « un ciberataque a una parte de la cadena de suministro podría perjudicar a toda la cadena » y los impactos alcanzarían mucho más que a nuestro propio negocio, incluso a clientes directos. Tan cierto para fabricantes de juguetes artesanales de Bali como para sistemas nacionales de salud de Europa.

Derecho a la privacidad y necesidad de confianza

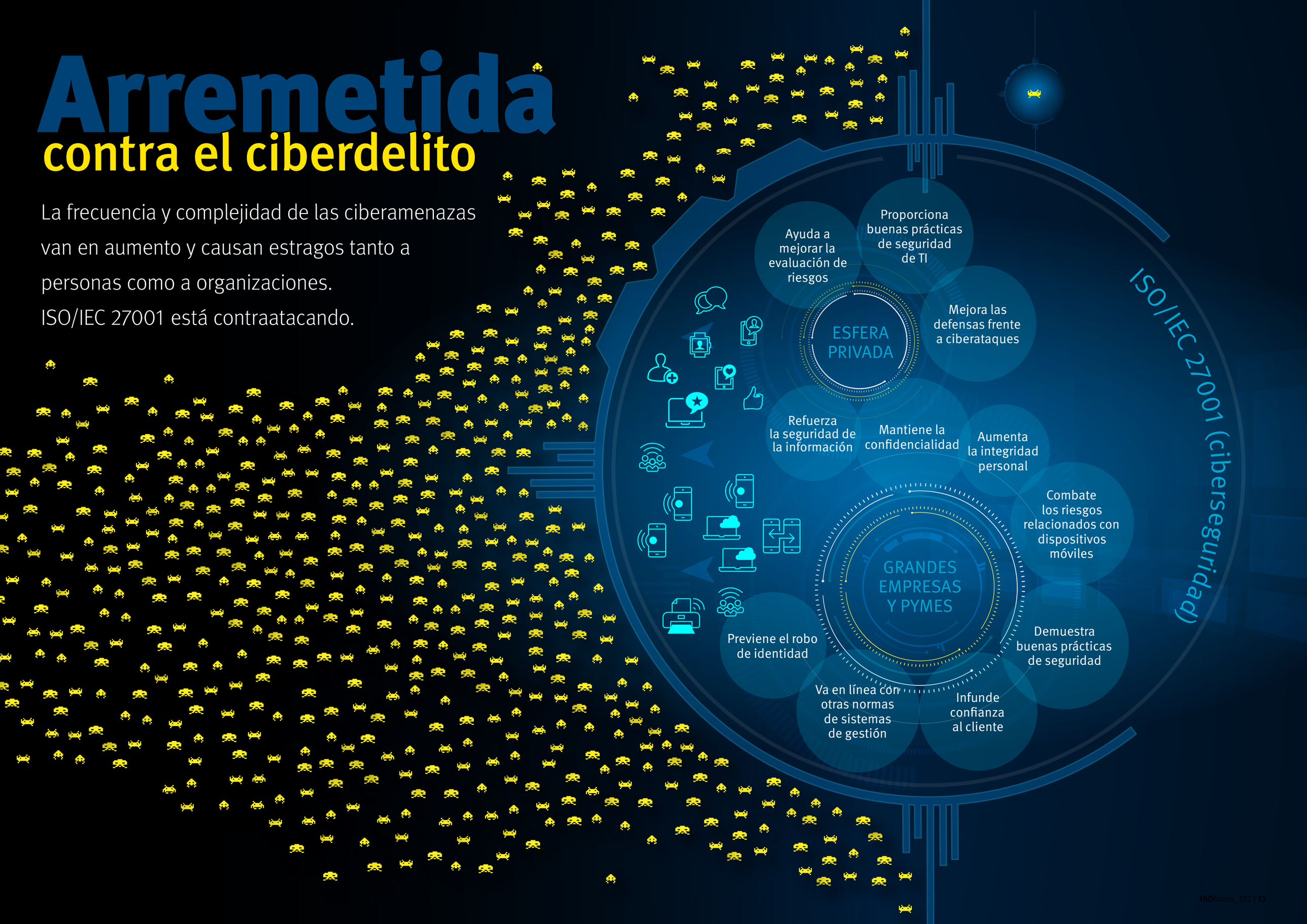
Puede que la vida privada sea menos compleja que el comercio mundial, pero también está en juego. Para la mayoría de nosotros, seguir buenas prácticas en las contraseñas y las actualizaciones de seguridad (y recordar que, si algo parece sospechoso o demasiado bueno para ser verdad, probablemente así sea) debería mantenernos a salvo de ciberdelincuentes la mayoría del tiempo. Sin embargo, cada vez se hacen más preguntas sobre cómo las instituciones y empresas conservan, analizan y monetizan las ingentes cantidades de datos que cedemos más o menos voluntariamente.

Le pregunté al profesor Humphreys si la familia ISO/IEC 27000 ofrece respuestas a estas incógnitas. « Hace poco, el subcomité SC 27 se embarcó en otro proyecto de desarrollo, ISO/IEC 27552, que amplía aún más ISO/IEC 27001 para abordar necesidades específicas de la privacidad ». El documento, actualmente en fase de borrador, especifica los requisitos y brinda asesoramiento para establecer, implantar, mantener y mejorar continuamente la gestión de la privacidad en lo referente a la organización.

La amenaza contra la privacidad, las finanzas y la reputación individual o corporativa mina la confianza e influye en nuestro comportamiento en línea y en la vida real. El papel de la familia ISO/IEC 27000 es crucial para poder seguir avanzando. Tenemos muchos motivos para preocuparnos, puesto que casi todos los aspectos de nuestra vida están digitalizados, pero tranquiliza saber que hay una familia de normas con la que contar para los sistemas de gestión de seguridad de la información, además de un grupo internacional de expertos que, como el profesor Humphreys, trabajan para que vayamos un paso por delante. ■

Arremetida
contra el ciberdelito

La frecuencia y complejidad de las ciberamenazas van en aumento y causan estragos tanto a personas como a organizaciones. ISO/IEC 27001 está contraatacando.



El diseño
de un futuro conectado

por Rick Gould

En 2018, ISO, junto con la Comisión Electrotécnica Internacional (IEC), publicó ISO/IEC 30141, la primera arquitectura de referencia normalizada centrada en la Internet de las Cosas (IdC) – esa compleja fusión de miles de millones de dispositivos inteligentes conectados por Internet. La aplicación de la norma creará una IdC más eficaz, segura, resiliente y mucho más protegida.

La IdC es una red de dispositivos computarizados y, con frecuencia, inalámbricos que permiten a las personas y las máquinas ver, sentir e incluso controlar gran parte del mundo.

En los dos años transcurridos desde el primer artículo sobre la Internet de las Cosas (IdC) en la *ISOfocus* allá por 2016, han ocurrido muchas cosas. En primer lugar, se creó un nuevo subcomité centrado enteramente en desarrollar normas para este sector en rápida expansión, por ejemplo, ISO/IEC 30141. En segundo lugar, varios ataques a gran escala en la IdC han demostrado de forma patente la necesidad vital de estas normas.

Ya son más de 20 años desde que el pionero tecnológico británico Kevin Ashton creara la expresión « Internet de las Cosas » durante su trabajo en Procter & Gamble. Ashton demostró en una presentación cómo la empresa podría usar la identificación de radiofrecuencia (RFID) –la tecnología inalámbrica ampliamente presente hoy en el pago sin contacto y las tarjetas de identificación inteligentes– para el control y seguimiento de productos. La expresión sin duda dejó huella.

La definición oficial de la IdC formulada por ISO y la Comisión Electrotécnica Internacional (IEC) es « una infraestructura de entidades, personas, sistemas y recursos de información interconectados, junto con servicios que procesan y reaccionan a información proveniente del mundo físico y del mundo virtual ». Sin embargo, en palabras sencillas, la IdC es una red de dispositivos computarizados y, con frecuencia, inalámbricos que permiten a las personas y las máquinas ver, sentir e incluso controlar gran parte del mundo que nos rodea, ya sea a título individual o a una escala mayor y mundial.

De hecho, los dispositivos y sistemas de la IdC se han hecho un hueco en la mayoría de los aspectos de la vida moderna, si no en todos. Algunos ya son bien conocidos y son de uso común en los mercados doméstico y de consumo, aunque los mayores usuarios de la IdC operan en la industria, la salud, la gestión municipal y la agricultura. En términos simples, cualquier tecnología calificada como inteligente es, probablemente, parte de la creciente familia de la IdC ; por ejemplo, contadores inteligentes, coches inteligentes, tarjetas inteligentes, dispositivos inteligentes para deporte, ciudades inteligentes, teléfonos inteligentes, relojes inteligentes, servicios públicos inteligentes, agricultura inteligente, salud inteligente y hasta la fabricación inteligente, que se considera una nueva revolución industrial.

Tecnología que nos acerca

En conjunto, la IdC puede hacer que estemos más conectados e informados, seamos más eficaces y eficientes y generemos menos residuos. Sin embargo, si la manejamos mal, puede perjudicar la seguridad y resiliencia de nuestras redes informáticas y nuestros datos. No en vano, la relativa simplicidad de los dispositivos de la IdC es la que plantea tantos desafíos como oportunidades. « Las ventajas son numerosas, pero, al mismo tiempo, los mayores riesgos son la resiliencia y la seguridad », recalca Francois Coallier, Presidente del comité técnico conjunto ISO/IEC JTC 1, *Tecnologías de la información*, subcomité SC 41, *Internet de las Cosas y tecnologías relacionadas*. ISO e IEC fundaron el JTC 1/SC 41 para centrarse en las normas de la IdC, mientras que el JTC 1 en sí es responsable de la normalización internacional en el campo de las TIC y supera ampliamente las 3 000 normas publicadas desde sus inicios en 1987.

Los desafíos de la interoperabilidad –es decir, la capacidad de los dispositivos de la IdC para conectarse de manera integrada entre ellos y a otros sistemas– y la seguridad están interrelacionados. « Se desarrollan nuevas tecnologías constantemente, y a un ritmo rápido », agrega Coallier, « por lo que su incorporación a la red se ha producido con rapidez y muchas veces a medida que aparecían nuevas tecnologías ». El crecimiento de la IdC es exponencial y se le atribuye un potencial de hasta 50 000 millones de dispositivos de IdC conectados de aquí a 2020 y un valor de mercado de billones de dólares estadounidenses.

NUBE DE VENTAJAS...

« Ya existen muchas normas publicadas sobre resiliencia, protección y seguridad, pero ISO/IEC 30141 proporciona la arquitectura de referencia para aplicarlas. »

François Coallier, Presidente del ISO/IEC JTC 1, *Tecnologías de la información*, subcomité SC 41, *Internet de las Cosas y tecnologías relacionadas*.

El año de la bombilla

2016, el mismo año en el que nació el JTC 1/SC 41, fue también el año de la bombilla para la Internet de las Cosas, en sentido tanto literal como figurado, debido a varios ataques a gran escala contra las redes a través de la IdC. Por ejemplo, en marzo de ese año, el ataque conocido como « Mirai Botnet » paralizó gran parte de Internet en la costa oriental de los EE. UU., en lo que constituye el mayor incidente de Internet hasta la fecha. A muchas personas les sorprendió la rapidez con la que se propagó el código malicioso y lo fácil que le resultó al hacker entrar en redes en apariencia seguras. Pero ¿cómo ocurrió ? Se trató de un caso del eslabón más débil de la cadena, en este caso, los dispositivos IdC situados en el borde de la red.

« El creador de Mirai Botnet atacó dispositivos tales como cámaras de CCTV inalámbricas y televisores inteligentes vendidos con un número limitado de nombres y contraseñas de administrador predeterminados », explica Coallier. El fabricante produjo millones de estos dispositivos. « El botnet atacante probó cada combinación de nombre de administrador y contraseña en secuencia hasta que pudo acceder y tomar el control del dispositivo », afirma. « Tras hacerse con el control de más de cien mil de estos dispositivos, el atacante fue capaz de generar fuertes ataques de denegación de servicio que lograron tumbar temporalmente parte de Internet en los EE. UU.».

En otro ataque bien documentado, una fábrica fue objeto de sabotajes por métodos de ingeniería social contra los equipos personales (PC) administrativos. « En este caso, parece que desde tales PC se tenía acceso a los sistemas de producción industriales, algo que se habría evitado si estos sistemas hubieran tenido una segmentación de red correcta para aislarlos de los equipos administrativos expuestos a Internet », agrega Coallier. Lo que es más importante, la red habría sido mucho más segura si simplemente se hubieran aplicado procesos y procedimientos bien documentados y ya descritos en numerosas normas, por ejemplo, la serie ISO/IEC 27033 sobre técnicas de seguridad informática, una de las normas que exigen la segmentación de las redes para una mayor seguridad.

Foto : Kaur Kristjan/Unsplash

A muchas personas les sorprendió la rapidez con la que se propagó el código malicioso y lo fácil que le resultó al hacker entrar en redes en apariencia seguras.

El mismo año del Mirai Botnet, un grupo de investigadores israelíes demostraron el riesgo de hackeo de las redes de iluminación mediante un dron volador modificado y explotando la vulnerabilidad de una popular bombilla inteligente. Bastaba con derrotar a las medidas de seguridad de una sola lámpara para infectar y dominar las adyacentes. Los investigadores informaron de que, si una ciudad tenía suficientes bombillas inteligentes con los mismos protocolos de comunicación, el ataque malicioso era capaz de infectar toda la red de bombillas en minutos. Aunque sea un escenario extremo, este ejercicio demostró el posible alcance de los ataques masivos maliciosos en redes aparentemente seguras, tan solo aprovechando vulnerabilidades imprevistas de los dispositivos sencillos situados en el borde de la red.

Las normas para la IdC al rescate

Aquí estriba el desafío de los dispositivos IdC : en su simplicidad, unida a una implementación poco cuidadosa y a que los usuarios prestan poca atención a su seguridad. Muchos de estos dispositivos son minicomputadoras simplificadas y de baja potencia dotadas de sistemas operativos compactos basados en Linux, un sistema omnipresente y popular entre los hackers. Significa que los dispositivos IdC tienen requisitos distintos de los de otros equipos ; si sus usuarios no aplican unas normas rigurosas para su seguridad, estos factores convierten a la IdC en el blanco de los ataques. « La IdC es cuestión de yin y yang : ofrece oportunidades, pero tenemos que equilibrarlas con una implementación cuidadosa y prestar mucha más atención a la seguridad », observa Coallier.

Las normas de la Internet de las Cosas establecen un marco común.

Aquí es donde las Normas Internacionales reforzarán la operabilidad y la resiliencia de la IdC. ¿ De qué modo pueden hacerlo ? La serie de normas ISO/IEC 29192, por ejemplo, define técnicas de criptografía liviana ideal para los dispositivos sencillos y de baja potencia. En el ejemplo de la bombilla, los investigadores israelíes recomendaron una técnica de seguridad concreta descrita en ISO/IEC 29192-5 y que especifica tres funciones de troceado adecuadas para aplicaciones que requieran implementaciones criptográficas livianas. Sin embargo, como en cualquier otro campo en desarrollo, también necesitaremos nuevas normas, y aquí es donde entra en juego el JTC 1/SC 41, cuya misión bien definida abarca la interoperabilidad y, sobre todo, la seguridad.

El subcomité JTC 1 ha publicado hasta la fecha 18 documentos centrados ante todo en las redes de sensores. Entre ellos está también una nota de orientación en la forma del informe técnico ISO/IEC TR 22417, *Tecnologías de información – Casos de uso de la Internet de las Cosas (IdC)*, que proporciona un contexto para los usuarios de normas de la IdC. Esta guía abarca aspectos importantes, tales como los requisitos básicos, la interoperabilidad y las normas aplicadas por los usuarios. Lo que es más importante, los ejemplos que aporta aclaran en qué casos entran en juego las normas existentes y resaltan dónde se requiere una mayor normalización.

Construimos los fundamentos

Las normas de la Internet de las Cosas establecen un marco común en temas tales como terminología o arquitecturas de referencia que ayudarán a los desarrolladores de productos a implantar un sistema interoperable. La ISO/IEC 30141 sienta las bases y el marco de referencia para las muchas normas aplicables producidas por el JTC 1/SC 41. « Vimos la necesidad de una arquitectura de referencia para maximizar los beneficios y reducir los riesgos », explica Coallier, Presidente del subcomité de ISO. Otra norma fundamental es ISO/IEC 20924, *Tecnologías de la información – Internet de las Cosas (IdC) – Definición y vocabulario*. « Es importante que quienes trabajan con la IdC hablen un mismo lenguaje », agrega Coallier. ISO/IEC 20924 e ISO/IEC 30141 proporcionan el lenguaje necesario.

El grupo de trabajo que desarrolló la ISO/IEC 30141 estuvo encabezado por la Dra. Jie Shen de China y contó con el apoyo de dos coeditores, concretamente Wei Wei de Alemania y Östen Frånberg de Suecia. En conjunto, los responsables del proyecto acumulan muchas décadas de experiencia en este campo, complementada por un equipo de más de 50 especialistas que contribuyeron directamente a la norma. « La IdC conlleva un sinfín de riesgos y oportunidades », informa la Dra. Jie Shen, que agrega : « necesitamos diseñar el mecanismo de mantenimiento perfecto para superar estos riesgos y la clave está en los detalles ».

Gran parte de los detalles ya están presentes en las muchas normas publicadas por los subcomités del JTC 1, y ISO/IEC 30141 las dota de una arquitectura de referencia común y se suma a las nuevas normas que el JTC 1/SC 41 está desarrollando. « ISO/IEC 30141 proporciona un marco común para los diseñadores y desarrolladores de la IdC », explica Coallier. « La norma describe las características principales de la IdC, además de un modelo conceptual y una arquitectura de referencia », agrega. Las descripciones vienen acompañadas de numerosos ejemplos.

MODELO DE SEIS DOMINIOS DE LA ARQUITECTURA PARA LA IdC

ISO/IEC 30141

Una cadena de seis dominios

ISO/IEC 30141 también refleja una estructura nueva e innovadora que se conoce como el modelo de seis dominios para la arquitectura de referencia de la IdC. Proporciona un marco que permitirá a los diseñadores de sistemas integrar toda la variedad de dispositivos y operaciones dentro de la IdC. El equipo del proyecto comprobó que los planteamientos convencionales no son adecuados para las redes más simples. La Dra. Jie Shen explica: «Es más complicado construir el ecosistema en la IdC para conectar muchas entidades heterogéneas: usuarios humanos, objetos físicos, dispositivos, plataformas de servicios, aplicaciones, bases de datos, herramientas de terceros y otros recursos. Comprobamos que el modelo de referencia convencional por capas aplicado tradicionalmente a los sistemas de TI resultaba insuficiente». El modelo de seis dominios, por otro lado, puede ayudar a subdividir el ecosistema de la IdC con toda claridad y guía a los usuarios al establecer el nuevo modelo de negocio de esta Internet. El modelo en sí será aún más eficaz si se sustenta en la cadena de bloques, la técnica altamente segura empleada cada vez más en las transacciones financieras.

La norma también describe en profundidad la interoperabilidad –o cómo hacer posible una comunicación fluida entre tipos diversos de dispositivos– y el concepto de confiabilidad en la IdC. Esta última, a su vez, se define como el grado de confianza que los usuarios pueden tener en que un sistema funcione del modo previsto, pero garantizando la protección, seguridad, privacidad, confiabilidad y resiliencia ante disrupciones tales como desastres naturales, fallas, error humano y ataques. «Ya existen muchas normas publicadas sobre resiliencia, protección y seguridad, pero ISO/IEC 30141 proporciona la arquitectura de referencia para aplicarlas», informa Coallier. Al mismo tiempo, a medida que la Internet de las Cosas sigue evolucionando y creciendo, el JTC 1/SC 41 está desarrollando otras nueve normas para la IdC que permitirán avanzar en confiabilidad, interoperabilidad, seguridad y especificaciones técnicas. ■

LA BÚSQUEDA DE LA **ciber confianza**

Foto : Ludovic Toinel/Unsplash

por Robert Bartram

Con una tecnología cada vez más sofisticada y que ofrece a partes iguales mayores oportunidades y nuevas vulnerabilidades y amenazas, las organizaciones de todo tipo corren riesgo de dejar la puerta abierta a ataques maliciosos o brechas de seguridad a gran escala. Es por ello que la gestión de riesgos es tan indispensable en el ciberespacio como lo es en la vida real. ¿En qué consisten estos ciberriesgos? ¿Cómo pueden ayudar las Normas Internacionales a reducirlos? ¿La única solución es una tecnología aún más sofisticada?

La definición del Diccionario de la Lengua Española es bastante clara: el «riesgo» es la «contingencia o proximidad de un daño». Es necesario correr riesgos para lograr resultados, pero también es necesario gestionarlos para conseguir resultados positivos y evitar consecuencias negativas.

El riesgo es inevitable. Debemos correr riesgos; son una parte inevitable y necesaria de nuestras vidas, tanto en la esfera personal como en la profesional. De hecho, si alguna empresa u organización de algún sector del mundo enormemente competitivo de hoy en día finge que no corrió ningún riesgo –o que tal riesgo no existió– además de incumplir sus obligaciones legales y estatutarias, quebraría y se perdería de vista rápidamente.

No obstante, el riesgo también puede ser una fuerza positiva. Gestionar riesgos correctamente puede generar resultados positivos; es necesario que las empresas corran riesgos para lograr sus objetivos. Es natural que las organizaciones necesiten un grado de certidumbre antes de tomar decisiones estratégicas importantes; además, es fundamental comprender que el riesgo se trata del impacto probable de incertidumbre en dichas decisiones. En resumen, el riesgo gira en torno a tomar decisiones en un mundo cada vez más complejo, volátil y ambiguo.

Amenaza digital

Ante todo, en el ámbito del ciberriesgo. En el ciberespacio, la existencia de altos niveles de incertidumbre suele deberse a cuestiones de seguridad nacional y corporativa. La amenaza no proviene del contexto y las circunstancias del mercado, sino de «autores de amenazas», aquellos que tratan de realizar actos delictivos. De hecho, son invisibles y, como los fantasmas y espectros de las tradiciones folclóricas, su invisibilidad apenas acentúa la sensación de amenaza. Los autores de amenazas tienen la intención y la capacidad de hacer daño; además, son ágiles y se adaptan.

Es más, la tecnología se vuelve más sofisticada cada día que pasa, incluso a cada hora que pasa. Antaño, un delincuente industrial tenía suerte si lograba sustraer un maletín lleno de documentos importantes olvidado sobre una mesa. Ahora, con las memorias USB o vulnerabilidades de exfiltración, ese mismo delincuente puede robar gigabytes de información que, en hojas de papel apiladas, podría llegar hasta la Luna. No es solo que el almacenamiento de datos se haya vuelto extremadamente sofisticado –del papel a digital–, sino que la naturaleza y los fines de los datos también han cambiado. Si un criminal se propone robar productos médicos protegidos, por ejemplo, ya no necesita descerrajar un almacén: le basta con copiar los datos en formato digital y clonar el producto en una impresora 3D.

Es un sine qua non que las organizaciones de todo cariz necesitan «ciberprotección» de un tipo u otro. Pero no solo eso: también necesitan un sistema lo suficientemente robusto para alertarles de cualquier ataque –real o percibido– con la máxima rapidez. Las amenazas en el ciberespacio encajan en dos categorías: internas y externas. Para diseñar y ejecutar con éxito un sistema de protección frente a las amenazas externas, el énfasis debe estar en las intenciones y capacidades de los actores maliciosos externos: lo que buscan, por qué lo buscan y de qué tecnologías disponen.

Sin embargo, las organizaciones también necesitan prepararse para la amenaza desde dentro y los descuidos del personal que dejan el sistema expuesto a posibles daños. Un uso poco cuidadoso de los datos personales puede exponer a una persona al chantaje y la captación por organizaciones de intenciones aviesas. Una organización puede tener el mejor cortafuegos del mundo, pero este no sirve para nada si hablamos de una persona de dentro con altos niveles de acceso y capaz de sustraer información en el anonimato.

La tecnología se vuelve más sofisticada cada día que pasa, incluso a cada hora que pasa.

Lo que realmente importa

Entonces ¿cómo se protegen los gobiernos, las empresas y las personas ante estas amenazas? El comité técnico ISO/TC 262, *Gestión del riesgo*, ha producido la norma ISO 31000 sobre gestión del riesgo, que crea un marco de principios y un proceso para la gestión del riesgo en su conjunto. Jason Brown es Presidente del ISO/TC 262 y, entre otras labores, fue responsable de gestionar la evaluación y protección de ciberseguridad del Departamento de Defensa de Australia. Resalta que, al igual que con cualquier gestión de riesgos, si una organización se toma en serio la protección ante los ciberriesgos, necesita «volver a los objetivos de la empresa y decidir qué cosas importan de verdad, conocer sus auténticos tesoros. En otras palabras, conozca cuáles son sus joyas de la corona digitales.»

Las empresas y los gobiernos necesitan evaluar cuidadosamente el valor y la naturaleza de aquello que es realmente valioso. Por ejemplo, si el papel de una organización es proteger una propiedad intelectual técnica del máximo nivel en forma de datos, resulta obvio que la fuga o sustracción de tales datos les supondrá consecuencias enormes. Sin embargo, las consecuencias serán más graves si esta información en su custodia pertenece a otros que dependen de esa organización como parte de una cadena de suministro, dado que una brecha en el sistema supondría la rotura de toda la cadena. Lo que importa en primera línea, por tanto, es una visión sistémica y estratégica, y no una evaluación de la tecnología en sí misma.

Google devuelve más de 6,5 millones de coincidencias en 0,54 segundos cuando buscamos «ISO 31000» en su motor de búsqueda.

Este planteamiento concuerda con el del Dr. Donald R. Deutsch, Vicepresidente y Responsable Jefe de Normalización de Oracle en California, además de Presidente del comité técnico ISO/IEC JTC 1, *Tecnologías de la información*, subcomité SC 38, *Computación en la nube y plataformas distribuidas*, un grupo de expertos que trabaja con el patrocinio conjunto de ISO y la Comisión Electrotécnica Internacional (IEC). La nube y su posición en la jerarquía del riesgo tienen quizá la máxima importancia inmediata para el consumidor común. Si usamos una computadora en la actualidad, es altamente probable que también usemos la nube. En el caso de la «computación en la nube, es más una cuestión de implantación y estrategia de negocio que de estrategia tecnológica», afirma el Dr. Deutsch. Sin duda existen mejoras tecnológicas recientes que conllevan sus propios riesgos –tales como el aprovisionamiento automático de recursos informáticos compartidos por múltiples usuarios– pero «los riesgos son bastante parecidos a los que tendríamos en cualquier entorno informático, aunque exacerbados y amplificados por la escala».

El precio de la resiliencia

Las Normas Internacionales sustentan este planteamiento estratégico en materia de ciberriesgo. Como recuerda Jason Brown, a la hora de abordar los ciberriesgos, la serie ISO 31000 también se debe evaluar conjuntamente con la serie ISO/IEC 27000 sobre sistemas de gestión de seguridad de la información, o SGSI en abreviatura. Este planteamiento da igual peso a la tecnología y al «factor humano». ISO/IEC 27000 ayudará a las organizaciones a evaluar sus necesidades puramente tecnológicas, mientras que ISO 31000 ayudará a comprender el valor de la información o los productos que guardan en el ciberespacio y, por tanto, el grado de protección tecnológica que necesitará para prevenir posibles ataques. En otros términos: una evaluación exhaustiva del riesgo según ISO 31000 podría evitarle a cualquier organización un desembolso económico considerable si hablamos de seguridad tecnológica. Hacer caso omiso del riesgo puede llevar por igual a gastar demasiado en un sistema de protección o a no invertir lo suficiente.

No obstante, estas dos series de normas no son en absoluto las únicas que pueden ayudar a mitigar los riesgos cibernéticos. La ciberseguridad también se debe examinar en términos de continuidad del negocio; es exactamente a lo que dedica la serie ISO 22301 sobre gestión de la continuidad del negocio. Esta serie hace posible un «sistema de gestión documentado para protegerse de [...] incidentes disruptivos cuando se producen» y permite a las organizaciones evaluar si su sistema de información y telecomunicaciones apoya sus objetivos y qué consecuencias tendría su caída. La inversión de una organización en ciberseguridad puede regirse por el nivel de dependencia que tiene en el sistema; una organización pequeña puede seguir utilizando (o retomar) los recibos en papel, mientras que un gigante como Amazon depende literalmente de la conectividad.

De modo parecido, el trabajo de ISO/IEC JTC 1/SC 38 ayuda a los productores –y en último término a los consumidores– a hablar un lenguaje común en cuanto a computación en la nube. Un hecho crucial es que la exigencia de este conjunto de normas no emana de los productores o vendedores en sí mismos, como suele ocurrir, sino de los clientes y compradores. Tanto gobiernos como corporaciones resaltaron que cada productor usaba su propia terminología, lo que hacía imposible la comparación de productos y una elección informada. A su vez, esto llevó a la publicación de ISO/IEC 17789, *Tecnología de la información – Computación en la nube – Arquitectura de referencia*, que estableció una arquitectura de referencia y un marco de vocabulario común. El subcomité SC 38 también supervisó la creación de ISO/IEC 19086, una norma en cuatro partes dedicada a los acuerdos de nivel de servicio entre proveedores de la nube y sus clientes y que aún tiene dos partes en desarrollo.

La computación en la nube, es más una cuestión de implantación y estrategia de negocio que de estrategia tecnológica.

CIBERSEGURIDAD

HECHOS Y CIFRAS

92 %
del malware se sigue enviando por correo electrónico

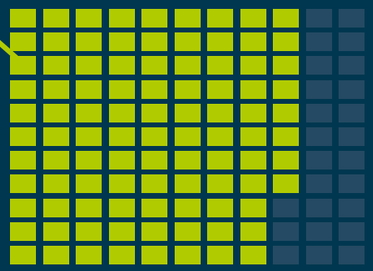
VULNERABILIDAD DE LOS SISTEMAS DE CONTROL INDUSTRIALES

UN **54%**
DE LAS EMPRESAS EVALUADAS SUFRIERON UN INCIDENTE DE SEGURIDAD RELACIONADO CON EL SISTEMA DE CONTROL INDUSTRIAL EN LOS ÚLTIMOS 12 MESES

UN **16%**
HA SUFRIDO TRES O MÁS INCIDENTES

ATAQUES EXITOSOS EN 2017

EL **77 %**
de ellos fue sin archivos



Fuente: Top cybersecurity facts, figures and statistics for 2018
www.csoonline.com

Un salto de gigante

No hay duda alguna del impacto positivo que todas estas normas tuvieron en la ciberseguridad en general y los ciberriesgos en particular. Ya son cerca de 40 países los que han adoptado ISO 31000 como su sistema nacional de gestión del riesgo. Por si esto fuera poco, Google devuelve más de 6,5 millones de coincidencias en 0,54 segundos cuando buscamos «ISO 31000» en su motor de búsqueda.

No obstante, dado que la tecnología evoluciona a un ritmo cada vez mayor, las normas internacionales deben mantenerse al día. Las herramientas que funcionan hoy día tal vez no sirvan en el futuro. Por ejemplo, a medida que el aprendizaje automático se adentra en la Inteligencia Artificial, es probable que lleguemos a sistemas con capacidades de aprendizaje adaptativas y «filosóficas» impensables en la actualidad. Las capacidades de análisis de datos se están desarrollando hasta el punto que será posible analizar cantidades ingentes de datos para detectar problemas emergentes que de lo contrario pasarían desapercibidos. Por otra parte, la llegada de la computación cuántica también aumentará exponencialmente la velocidad de la computación. La combinación de estos tres cambios en el mundo cibernético será «probablemente el cambio más transformador que hayamos visto desde el descubrimiento de la electricidad o el átomo», afirma Jason Brown. Y todo ello sin tomar en cuenta las nanotecnologías ni la creciente interconectividad de todo tipo de elementos.

Cuando un día todos estos factores se combinen, se acelerará drásticamente el entorno competitivo para hacerse con la ventaja en los negocios, entre países y también entre distintos agentes del mercado. Se llegará hasta un punto en el que la intervención humana seguirá marcando el nivel de riesgo en los objetivos, pero la capacidad humana real para tratar con el ciberespacio podría llegar a ser insignificante. El ISO/TC 262 está examinando en la actualidad un área etiquetada como «Gestión de riesgos emergentes» y que se centra en los riesgos que, probablemente, serán más disruptivos. Como aclara Brown, tanto los consumidores como los productores necesitan abordar el futuro de forma diferente y todos «tendremos que estar mucho más abiertos a este mundo altamente volátil y ambiguo». ■

Plataforma para *el desempeño*

ISO/IEC 27001 (seguridad de la información)

ISO/IEC 29192-1 (criptografía liviana)

ISO/IEC 27002 (controles de seguridad de la información)

ISO/IEC JTC 1/SC 27 *Técnicas de seguridad de TI*

ISO/IEC 27042 (análisis de pruebas digitales)

ISO/IEC 27032 (interacción más segura con el ciberespacio)

Serie ISO/IEC 27033 (seguridad de la red)

ISO/IEC 27043 (investigación de incidentes)

ISO/IEC 27005 (gestión de riesgos de ciberseguridad)

Futura ISO/IEC 27552 (necesidades específicas de privacidad)

ISO/TC 262 *Gestión del riesgo*

ISO 31000 (gestión de riesgos para organizaciones)

Futura ISO 31050 (gestión de riesgos emergentes)

ISO/IEC 31010 (técnicas de evaluación de riesgos)

Futura ISO 31030 (gestión de riesgos al viajar)

Futura ISO 31022 (gestión de riesgos jurídicos)

Futura ISO/IEC 20924 (vocabulario para la IdC)

ISO/IEC 30141 (arquitectura de referencia para la IdC)

Futura ISO/IEC 30149 (marco de confiabilidad de la IdC)

ISO/IEC JTC 1/SC 41, *Internet de las Cosas y tecnologías relacionadas*

ISO/IEC TR* 22417 (Casos de uso de la Internet de las Cosas)

ISO/IEC 27035 (preparación para la continuidad del negocio)

Serie ISO/IEC 27035 (respuesta ante ciberataques)

ISO/TC 292 *Seguridad y resiliencia*

ISO/IEC 27017 (controles de seguridad de la información para computación en la nube)

ISO/IEC 19944 (uso de datos en servicios en la nube)

Serie ISO 22301 (gestión de la continuidad del negocio)

ISO/IEC 27018 (protección de datos personales en nubes públicas)

ISO/IEC JTC 1/SC 38 *Computación en la nube y plataformas distribuidas*

ISO/IEC 20933 (sistemas de acceso)

Serie ISO/IEC 19086 (marcos de acuerdo de nivel de servicio)

ISO/IEC 17789 (arquitectura de referencia para computación en la nube)

* TR : informe técnico

Foto: Hal Gatewood/Unsplash

5 cosas que no sabía que se pueden hackear

Foto: James Hicks/Unsplash

por Elizabeth Gasiorowski-Denis y Vivienne Rojas

Cada vez se conectan más objetos cotidianos, lo que no solo nos facilita las cosas a nosotros: también a los hackers. Ser conscientes de los peligros de los dispositivos conectados a la red es el primer paso para mantener a raya a los intrusos.

Los bebés, en el punto de mira de los hackers. Quizá se pregunte: ¿cómo es posible que un hacker pueda meterse en el cuarto de mi bebé? Por desgracia, la inmunidad de algunos dormitorios de bebés está expuesta a atacantes al acecho desde fuera del hogar. La moraleja de esta historia no es que puedan hackear su monitor de bebés: es que prácticamente cualquier elemento «conectado» está expuesto a los hackers.

Gartner, Inc. prevé que habrá 20 400 millones de dispositivos conectados en uso de aquí a 2020. El segmento de consumidores es el mayor usuario de dispositivos conectados, con 5 200 millones de unidades en 2017, nada menos que un 63 % del número total de aplicaciones en uso. En este mismo momento, muchos hogares cuentan con docenas de elementos conectados. Hablamos de equipos informáticos, teléfonos celulares y tabletas, pero también muchos electrodomésticos tradicionales, tales como frigoríficos, televisores y sistemas de seguridad.

En un estudio sobre la exposición de los dispositivos de la Internet de las Cosas al hackeo, los investigadores de la Universidad Ben-Gurion de Beersheba en Israel concluyeron que muchos fabricantes de dispositivos y propietarios se lo ponen muy fácil a los hackers. Hay bastantes fabricantes que usan las mismas contraseñas predeterminadas para el mismo tipo de dispositivo y los usuarios no suelen cambiarlas. Significa que, si tiene diez dispositivos conectados a la red y no toma precauciones en uno de ellos, toda la red está en peligro. Terrorífico, ¿no es cierto?

Es un hecho que los hackers «profesionales» pueden hackear y explotar prácticamente cualquier cosa que tenga una conexión estable a wifi. A no ser que el dispositivo esté totalmente aislado de Internet, es posible introducirse en él de una forma u otra. El problema afecta a una variedad enorme de objetos. Repasamos aquí cinco cosas expuestas a los hackers.

Monitores para bebés y cámaras

Para eso se inventaron los monitores para bebés: para monitorear a los niños pequeños. Por eso es tan peligroso cuando alguien hackea o explota uno de estos dispositivos. Los bebés y los niños de corta edad pueden ser vistos desde lugares preocupantes y por cualquiera capaz de hacerse con el control de los aparatos. De un modo similar, son muchas las cámaras de seguridad que se conectan hoy a

Es un hecho que los hackers «profesionales» pueden hackear y explotar prácticamente cualquier cosa que tenga una conexión estable a wifi.

Internet para poder observar lo que ocurre desde fuera del hogar. El Departamento de Consumo de Nueva York emitió una advertencia sobre la seguridad de los monitores para bebés tras varios incidentes muy difundidos en los que se escuchaban voces extrañas a través de ellos.

Impresoras y faxes

Muchas impresoras tienen su propia conexión a Internet para poder hablar con otros dispositivos de su hogar u oficina, con frecuencia por wifi. Esta conexión constituye el primer paso para el acceso remoto de cualquier hacker a su red. Basta con salvar cualquier control de seguridad para hackear su impresora y cualquier dispositivo conectado a ella. Las vulnerabilidades de las impresoras están bien documentadas: un hacker en particular alardeó de haberse metido en 150 000 impresoras para poner de relieve su vulnerabilidad.

Los hackers también pueden infiltrarse en su red doméstica enviando un simple fax. Dado que la mayoría de los aparatos de fax están integrados hoy en equipos multifunción conectados a una red wifi o una línea telefónica, es posible hackearlas fácilmente enviando un archivo de imagen diseñado para contener código malicioso. Al convertirlo en datos para su transmisión por la red informática interna, el código oculto puede tomar el control de su aparato de fax, robar sus contraseñas y datos bancarios y secuestrar otros dispositivos.

Foto : Hal Gatewood/Unsplash

Los comercios ya han tenido que retirar numerosos juguetes « conectados » o « inteligentes » tras hallar fallas de seguridad.

Juguetes infantiles

Sí, ese osito de peluche con wifi tan ideal es todo un campo de juegos para los hackers. Al parecer, cada vez que sale al mercado un nuevo dispositivo conectado a Internet, es pasto de los hackers. Entre ellos están muchos objetos y aparatos que no solemos asociar a este tipo de tecnología… por ejemplo, los juguetes. Cualquier juguete conectado a Internet y que tenga un micrófono, una cámara o seguimiento de localización puede poner en riesgo la privacidad o seguridad de los niños. Podría tratarse de una muñeca parlante o una tableta infantil. Los comercios ya han tenido que retirar numerosos juguetes « conectados » o « inteligentes » tras hallar fallas de seguridad en sus protocolos de Bluetooth y wifi que podrían permitir a un extraño hablar con los menores o escuchar conversaciones. En todos estos juguetes, la conexión a Bluetooth no estaba protegida : para introducirse en ellos, el atacante ni siquiera necesitaba una contraseña, un código PIN ni ninguna otra autenticación.

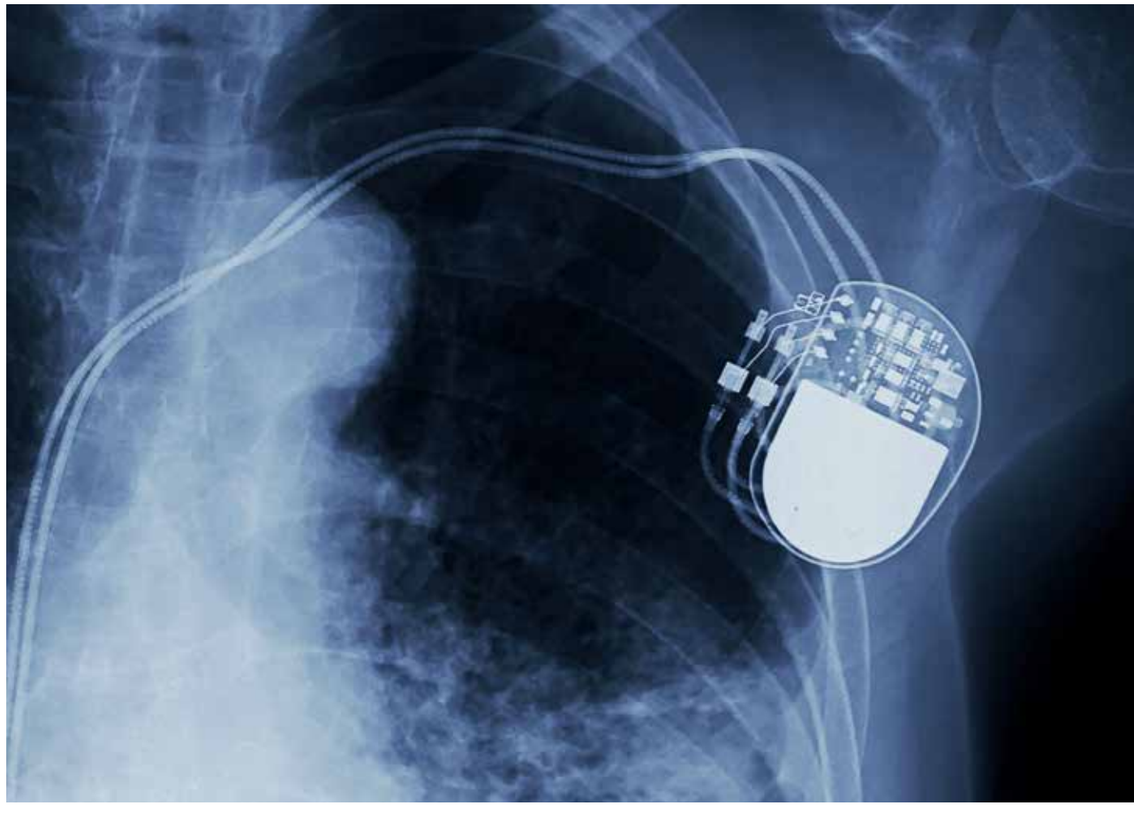
Aparatos inteligentes

Su frigorífico podría ser el peor enemigo de su seguridad. El frigorífico que le permite enviar la lista de la compra directamente a su smartphone puede estar configurado de modo que permite a cualquiera encontrar sus credenciales de Google. Cualquier dispositivo o aparato de su hogar que esté conectado puede ser la puerta de entrada a toda su red. Por muy práctico que sea poder controlar la temperatura de su hogar desde otro lugar –quizá para subirla a la hora en que sale del trabajo–, los hackers pueden capturar el control del termostato y crear un ambiente insoportable hasta que se paga un rescate. Las cafeteras son otro objetivo clave de las intrusiones cibernéticas. Cualquier defecto en la aplicación móvil que controla su cafetera podría ser la puerta a la vulneración de su privacidad si los hackers se hacen con su contraseña de wifi y filtran los datos que pasan por su red.

La Administración de Alimentos y Medicamentos de los EE. UU. retiró 465 000 marcapasos por temor a problemas de seguridad.

Marcapasos e implantes

¿Hackear su corazón ? ¡Ya está ocurriendo ! La Administración de Alimentos y Medicamentos (FDA) de los EE. UU. retiró 465 000 marcapasos en 2017 por temor a problemas de seguridad con los que un atacante malicioso podría cambiar el ritmo cardíaco de los pacientes e incluso provocar su muerte. ¿ Y la estimulación cerebral profunda, que alimenta diminutos pulsos eléctricos de alta precisión a su cerebro para controlar una epilepsia o los temblores del Parkinson ? Este control exacto del cerebro es todo lo que los hackers necesitan para lograr « hazañas » mayores que el simple control de las bombas de insulina o los implantes cardíacos. Un ataque específico contra los implantes cerebrales, o « brainjacking », podría perjudicar a las funciones motoras, alterar el control de impulsos, modificar las emociones o los afectos, inducir dolor y modular el sistema de recompensa. La pregunta sigue abierta : cuando los implantes cerebrales inalámbricos sean la norma, ¿ cómo permitir el acceso a los médicos, pero no a los cibercriminales ?



¿ LO SABÍA?

Si tiene diez dispositivos conectados a la red y no toma precauciones en uno de ellos, su seguridad puede estar en peligro.

El segmento de consumidores es el mayor usuario de dispositivos conectados, con 5 200 millones de unidades en 2017.

Apuesta por la seguridad

Existen otras muchas formas en apariencia improbables en que un hacker podría acceder a su sistema. Por mucho que protejamos la puerta principal de Internet, alguien podría infiltrarse por una puerta trasera. ¿Qué significa para nuestro futuro? ¿Cuánto deben alarmarnos todos estos productos inteligentes conectados a Internet? La respuesta es mucho. No tenemos que esperar hasta 2020 para experimentar estas vulnerabilidades de seguridad.

Proteger nuestro ciberespacio es un asunto urgente y uno que requiere una atención inmediata y continua. En muchos casos, unas medidas de seguridad correctas desaniman a los hackers expertos y mantienen a raya a los oportunistas; con frecuencia, las Normas Internacionales son nuestra primera línea de defensa. Normas como ISO/IEC 27001 e ISO/IEC 27002 aportan un lenguaje común para abordar aspectos de gobierno, riesgos y cumplimiento normativo relacionados con la seguridad de la información; ISO/IEC 27031 e ISO/IEC 27035 ayudan a las organizaciones a responder eficazmente ante los ciberataques, difundirlos y recuperarse de ellos. Existen otras muchas normas que definen mecanismos de encriptación y firma que pueden integrarse a los productos y aplicaciones para proteger las transacciones online, el uso de tarjetas de crédito y los datos almacenados.

No obstante, las normas solo son buenas en la medida en que se aplican. La próxima vez que adquiera un monitor para bebés o cualquier otro dispositivo conectado, pregúntese: ¿Pensó el fabricante en la exposición a los hackers? ¿Implementó la empresa las Normas Internacionales adecuadas? Si la respuesta es negativa en ambos casos, quizá le convenga reconsiderar su elección. ■

SESENTA AÑOS DE
SEGURIDAD CONTRA INCENDIOS

Aprovechando la oportunidad de su reunión plenaria anual, el comité técnico ISO/TC 92, *Seguridad contra incendios*, celebró en 2018 su 60.º aniversario : seis décadas de triunfos en la producción de normas aceptadas internacionalmente sobre ensayos contra incendios, medición de parámetros de incendios, ingeniería de seguridad contra incendios y otros temas relacionados. La reunión, celebrada el pasado octubre en Delft, Países Bajos, contó con NEN como anfitrión, el miembro de ISO en el país. La organización de normas neerlandesa recibió elogios por su excelente organización del evento, que incluía bombones y pastelitos elaborados especialmente para la ocasión.


Foto : NEN

Delegados del ISO/TC 92 frente al «Het Meisjeshuis» de Delft, un antiguo orfanato para niñas renovado y reinaugurado en la primavera de 2005 como centro cultural.

El colofón de los festejos fue una cena de celebración a la que asistió incluso la alcaldesa de Delft, Marja van Bijsterveldt. Pronunció un inspirador discurso con muchas referencias a las normas ISO en el que subrayaba la importancia de la normalización en los esfuerzos de mejora de la seguridad contra incendios. Más adelante, se galardonó a Patrick van Hees, Presidente del ISO/TC 92, con un certificado de méritos por parte del Director de NEN, Rik van Terwisga, para conmemorar este hito emblemático.

Las celebraciones no dejaron el trabajo normas en segundo plano ; el ISO/TC 92 y sus cuatro subcomités progresaron considerablemente en sus distintas áreas de especialidad. Durante los encuentros, el ISO/TC 92 debatió sobre su posible expansión a nuevos terrenos tales como grandes incendios al aire libre, túneles y construcciones subterráneas y salud y seguridad de bomberos : un signo infalible de que el comité estará presente durante muchos años.

ISO/TC 92 desea agradecer a Efectis, FTT-Fire Testing Technology, Kingspan, Etex Group y DGMR que hayan patrocinado estos encuentros.

EL FORO MUNDIAL DE INVERSIONES :
ESCAPARATE DE LAS NORMAS ISO

Para mayor información :

http://worldinvestmentforum.unctad.org/iso

En el último Foro Mundial de Inversiones de la UNCTAD, celebrado en Ginebra (Suiza), ISO se unió a innovadores, bancos de desarrollo, interesados del sector privado y representantes líderes de la industria y de gobiernos de todo el mundo para resaltar la importancia de las normas ISO.

Más de 80 participantes asistieron a la sesión informativa bajo el nombre « Normas ISO : la ayuda para que la Agenda 2030 sea una realidad », cuyo objetivo era exponer el papel de las normas en el logro de los Objetivos de Desarrollo Sostenible (ODS), la agenda de las Naciones Unidas para garantizar la paz y la prosperidad mundiales antes de 2030. Con un programa interactivo que incluía un panel y un debate, el evento además brindó una plataforma para intercambiar experiencias en áreas como el comercio internacional y los desafíos de las políticas públicas. Las organizaciones y empresas que quieran contribuir a los ODS descubrirán que las Normas Internacionales brindan herramientas eficaces para ayudarlas a afrontar este desafío.

La sesión de ISO se encontraba entre los 60 eventos, entre los que había tres cumbres, cinco mesas redondas ministeriales, debates moderados para el sector privado y varias ceremonias de entrega de premios. El objetivo global este Foro, que organiza la UNCTAD cada dos años, es fortalecer la cooperación transfronteriza en aras de promover la inversión internacional y su contribución al crecimiento y desarrollo económicos.

PRESENTACIÓN DE ISO 55002
SOBRE LA GESTIÓN DE ACTIVOS

La nueva edición de ISO 55002 se presentó oficialmente en Amersfoort, Países Bajos, por parte del ISO/TC 251, el comité técnico de ISO sobre la gestión de activos. La presentación fue oficial cuando Rhys Davies, Presidente del Comité, y el Coordinador Ton van Wingerden hicieron una presentación simbólica del ejemplar inaugural a Anton van der Sanden, Director de Royal HaskoningDHV NL. La sede central de esta consultoría de ingeniería albergó este encuentro del ISO/TC 251, que duró una semana, con la responsabilidad de desarrollar el conjunto de normas ISO 55000 sobre sistemas de gestión de activos.

Siendo una parte esencial de la serie, ISO 55002 orienta sobre la aplicación de un sistema de gestión de activos de acuerdo con ISO 55001. Las observaciones y experiencia de los primeros en adoptar la norma fueron los cimientos de esta importante revisión, que ofrece una guía para crear un plan de gestión de activos estratégico, procesar el riesgo en la gestión de activos y aplicar ISO 55001 en organizaciones de todos los tamaños. Elaborado por un grupo de expertos internacionales de 30 países – muchos de los cuales fueron imprescindibles en la redacción de ISO 55001 –, este documento concluyente se mantiene fiel al espíritu de los requisitos originales, mientras que genera observaciones globales sobre cómo se usa la norma..

Publicado por primera vez en 2014, la serie ISO 55000 incluye tres normas cuya relevancia y popularidad se han hecho evidentes con creces. En relación al éxito de la serie, Rhys Davies afirmó que ISO 55000 explica « por qué » una organización necesita un sistema de gestión de activos, ISO 55001 se encarga de « qué » es necesario para ajustarse a la norma e ISO 55002 orienta sobre « cómo » cumplir con los requisitos de la norma. Considera que la actualización de ISO 55002 promoverá considerablemente la adopción de este sistema de gestión en todo el mundo.


Foto : NEN

***Rhys Davies** Presidente del ISO/TC 251,* (derecha) ***y Ton van Wingerden**, Coordinador,* (izquierda) *presentan el primer ejemplar de ISO 55002:2018 a **Anton van der Sanden**, Director de Royal HaskoningDHV NL.*

EMPODERAR A FILIPINAS

El Secretario General de ISO, Sergio Mujica, se unió al Bureau of Philippine Standards (BPS), miembro de ISO en Filipinas, en la celebración de la Semana Nacional de las Normas en Manila. Celebrada de forma que coincidiese con el Día Mundial de la Normalización, al que se consagra el 14 de octubre como tributo a los esfuerzos colectivos de los expertos de todo el mundo que redactan Normas Internacionales, la semana arrancó con un concurso de escritura de ensayos sobre las normas y otro sobre creación de pósteres en los que participaron 150 estudiantes de institutos de toda la capital.

En su presentación informativa, Mujica resumió la historia y el sistema de normalización de ISO y habló sobre las numerosas ventajas que reportan las normas a los gobiernos, la economía y los consumidores, así como del impacto constructivo en el progreso tecnológico. Señaló la poca participación de Filipinas en los programas de normalización de ISO por la falta de recursos y concluyó con un poderoso mensaje dirigido a los estudiantes : convertirse en los profesionales de la normalización del mañana.

Durante su visita de dos días a Manila, el Secretario General de ISO se reunió con miembros del Congreso filipino y destacados profesionales de la normalización para debatir sobre la propuesta de una infraestructura nacional de calidad, respaldada ampliamente por el BPS y que ayudaría al país en su desarrollo económico futuro.


Foto : BPS

*El Secretario General de ISO, **Sergio Mujica**, toma un « groufie » (selfie en grupo) con estudiantes en Manila.*

HABLAMOS DE INODOROS

CON BILL GATES

« Las Normas Internacionales son fundamentales para el progreso de nuevas tecnologías de saneamiento y el desarrollo de una industria que salve vidas », afirmó Sergio Mujica en la Reinvented Toilet Expo, celebrada el pasado octubre en Pekín (China). El Secretario General de ISO se dirigió al público en un panel de alto nivel que contaba con Bill Gates, Copresidente de la Fundación Bill & Melinda Gates, y el doctor Jim Yong Kim, Presidente del Banco Mundial, además de otras personalidades reconocidas de la industria y del gobierno.

La cumbre de tres días, promovida por la Fundación Gates, abordó las perspectivas globales de saneamiento sin drenaje : una novedosa tecnología de inodoros independientes que tratan los residuos de forma segura sin tener que conectarlos a la red de saneamiento tradicional. El surtido de propuestas de la Expo iba desde inodoros con procesos biológicos y químicos hasta membranas que filtran líquidos ; diseños que permiten que más personas de regiones en desarrollo puedan ir al baño con seguridad y dignidad.

Emprender esta revolución no es tarea fácil. Sin embargo, hoy en día la tecnología puede verse respaldada por nuevas Normas Internacionales especializadas en sistemas de saneamiento sin drenaje. Gracias a que ofrece requisitos de seguridad y rendimiento para unidades de tratamiento integradas, ISO 30500 no solo facilita la fabricación eficaz, también contribuye al desarrollo del sector en su conjunto, lo que garantiza que miles de millones de personas consigan el saneamiento seguro que necesitan para dar el paso hacia una vida sana y productiva.

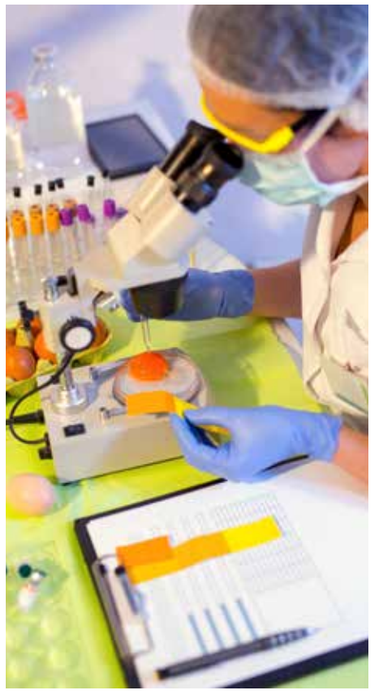
***Bill Gates** comparte escenario con un frasco de heces humanas para demostrar los beneficios de las nuevas tecnologías de inodoro.*

MAYOR COOPERACIÓN ENTRE ISO Y AOAC

ISO y AOAC INTERNATIONAL (AOAC) anunciaron en 2018 la renovación de su acuerdo de cooperación para el desarrollo y aprobación conjuntos de normas y métodos comunes. Esta colaboración de alto nivel se suscribió por primera vez en 2012 para un periodo de cinco años con AOAC, una organización científica sin ánimo de lucro comprometida con la producción de métodos fiables de análisis químicos. El objetivo es aumentar considerablemente la importancia mundial de ambas organizaciones mediante la adopción de normas comunes aprobadas por el Codex Alimentarius.

A tenor del nuevo acuerdo, AOAC e ISO pueden formar parte del trabajo del otro y participar en el desarrollo de normas comunes mediante grupos de trabajo formados por expertos de AOAC e ISO. AOAC e ISO publicarían las normas resultantes, sometidas a procesos de aprobación paralelos de ambas organizaciones.

La cooperación, centrada en un principio en la leche y los productos lácteos, ampliará sus competencias para abarcar proyectos dentro del alcance del comité técnico ISO/TC 34 , *Productos alimenticios*. Es posible que las futuras prioridades de las normas de AOAC/ISO contengan más tareas sobre el análisis de nutrientes, además de abordar los contaminantes, adulterantes y residuos de pesticidas, por el bien de todos los interesados de la industria alimentaria.



ISO COLABORA CON EL BANCO MUNDIAL

PARA AYUDAR A PAÍSES A FACILITAR EL COMERCIO

ISO colabora con el Banco Mundial con el fin de respaldar a organismos nacionales de normalización miembros de ISO ubicados en países en desarrollo, en función de sus necesidades, con la implementación del Acuerdo sobre Facilitación del Comercio de la Organización Mundial del Comercio. Se incluyen áreas como la aplicación de buenas prácticas en barreras técnicas para comerciar o, especialmente, implementar procedimientos de evaluación de conformidad.

La colaboración se realizó en un taller de cooperación de agencia fronteriza celebrado del 14 al 16 de noviembre de 2018 en Ciudad del Cabo (Sudáfrica), donde ISO acudió como invitado para presentar "Las normas y la facilitación del comercio".

El evento unió a altos representantes de 12 países africanos involucrados en la implementación del acuerdo sobre facilitación del comercio con el fin de compartir experiencias y aprender unos de otros. Los organizadores fueron el Banco Mundial, el Secretariado de la Organización Mundial del Comercio, el Secretariado de la Convención Internacional de Protección Fitosanitaria (IPPC), la Organización Mundial de Sanidad Animal (OIE), la Organización Alimentación y la Agricultura (FAO) y la Organización Mundial de Aduanas (WCO).

El programa de apoyo a la facilitación del comercio del Banco Mundial apoya activamente a países en desarrollo para orientar sus leyes, procedimientos y procesos de facilitación del comercio de forma que permitan la implementación del acuerdo sobre facilitación del comercio.

En la mayoría de países en desarrollo, el miembro de ISO o el organismo nacional de normalización (NSB, por sus siglas en inglés) son el punto de contacto nacional según requiere el Acuerdo sobre Obstáculos Técnicos al Comercio del Banco Mundial, además, también puede ser un proveedor de servicios de evaluación de conformidad.

Durante el evento, ISO se comprometió a proporcionar al Banco Mundial comentarios sobre sus herramientas relacionadas con el acuerdo sobre facilitación del comercio que se aplican a las actividades de los NSB.

ADVANCING THE GLOBAL AGENDA

– CALENDARIO 2019

Los Objetivos de Desarrollo Sostenible (ODS) de Naciones Unidas ofrecen una visión de un mundo más próspero, pacífico y sostenible. Con sus conocimientos expertos y recursos, ISO está bien posicionada para apoyar a sus miembros a lograr los ODS, todos ellos relacionados con la labor de ISO.

Descargue el Calendario ISO 2019 para descubrir cómo las normas ISO contribuyen a los 17 ODS. Diseñado con un formato de 17 meses, presenta muchas de las formas en que ISO puede hacer realidad la Agenda 2030 y que nadie se quede detrás.

El Calendario ISO 2019 ya está disponible para su descarga en iso.org.

El viaje de los datos posible gracias a ISO/IEC 20000-1

Foto: Markus Spiske/Unsplash

Los datos, y la nube que los aloja, tienen un valor casi infinito para las empresas que saben cómo tratarlos, siempre y cuando tengan implementada la estrategia adecuada para liberar su potencial. Orange Business Services ayuda a sus clientes a convertir sus datos en un verdadero activo comercial, gracias a algo de ayuda de la norma sobre gestión de servicios de TI de ISO/IEC.

Como resultado de la evolución digital, las empresas generan cada vez más y más datos. Estos datos no son más que una materia prima, pero si las organizaciones tienen la capacidad de transformarlos en información útil, pueden abrir la puerta a todo un mundo de oportunidades. Gracias a la computación en la nube, las organizaciones pueden acceder a potentes capacidades de TI. Además, disponen de una flexibilidad nunca vista para externalizar la totalidad o parte de sus sistemas de información, espacios de trabajo, servidores, aplicaciones y almacenamiento.

Aunque la nube ya lleva con nosotros algo más de una década, la mayor objeción que sigue poniendo trabas a su adopción es la constante preocupación por la seguridad e integridad de los datos. Los integradores de sistemas que puedan ofrecer eficazmente soluciones de seguridad y control de acceso alojadas en la nube gozarán de una mejor posición para el futuro, con la capacidad de brindar a sus clientes gran variedad de servicios remotos y gestionados y, al mismo tiempo, impulsar el valor global de su empresa.

Orange Business Services es una de estas empresas. Como rama de servicios comerciales del Grupo Orange, que cuenta con 260 millones de clientes en 28 países y una cifra de negocios anual de EUR 41 000 millones, este proveedor global de TIC quiere ser uno de los principales actores del «viaje de los datos». Con su apoyo a las organizaciones en todos y cada uno de los pasos de su transformación digital, ofrece a sus clientes conocimientos en lo que respecta a recopilación, transferencia, seguridad, almacenamiento, tratamiento, análisis y uso compartido de los datos, además de generar valor para ellos. Para poder prestar esta asistencia a tan gran escala, Orange Business Services necesita operar procesos globales fluidos gestionados por medio de un modelo de gobernanza corporativa aplicable en todo el mundo.

La implementación de la norma ISO/IEC 20000-1, *Tecnologías de la información – Gestión de servicios – Parte 1: Requisitos para sistemas de gestión de servicios*, era, por tanto, un objetivo lógico. Desarrollada por ISO y la Comisión Electrotécnica Internacional (IEC), la norma insignia de la familia ISO/IEC 20000 ayuda a las organizaciones a integrar una estrategia de ciclo de vida útil, indicando para ello las buenas prácticas para gestionar su cartera de servicios y que permanezcan al día. La publicación en 2018 de una edición nueva y mejorada nos ha animado a preguntar a Jean-Pierre Girardin, del departamento de Servicios al cliente y Operaciones de Orange Business Services, de qué manera esta reciente actualización va a ayudar a la empresa en su compromiso por mantener unos servicios integrales excelentes, allá donde operen sus clientes.

***ISOfocus*: ¿Qué ha llevado a Orange Business Services a adoptar con entusiasmo ISO/IEC 20000-1?**

Jean-Pierre Girardin: Con más de tres mil empresas multinacionales de renombre a nivel internacional y más de dos millones de profesionales, empresas y comunidades locales en Francia, Orange Business Services se apoya firmemente en normas sobre la seguridad de la información y, además, cuenta con la certificación ISO/IEC 20000-1 desde hace diez años.

Desde el primer momento se decidió intencionadamente introducir la norma de forma progresiva e integrada. Por ello, aprovechamos los sistemas de gestión de la calidad iniciales de la empresa basados en ISO 9001 para mejorar nuestros procesos de gestión de servicios en un marco integrado. Esto nos ha permitido alinear nuestros procesos de servicio en todos nuestros centros operativos de Orange Business Services de todo el mundo.

Como empresa orientada a los servicios comerciales, obtener la certificación ISO/IEC 20000-1 fue una oportunidad de oro. Nos permitió centrarnos en la mejora de nuestros servicios y sacar partido de la virtuosa combinación de tres normas sobre sistemas de gestión (ISO 9001 (calidad), ISO/IEC 20000-1 (servicios de TI) e ISO/IEC 27001[1)] (seguridad de la información)), así como de las posibilidades de mejora continua inherentes a las tres normas.

1) ISO/IEC 27001:2013, *Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requisitos*, se desarrolló junto con ISO y la Comisión Electrotécnica Internacional (IEC).

¿Cuáles son las principales ventajas que ISO/IEC 20000-1 ha brindado a Orange Business Services?

La implementación de ISO/IEC 20000-1 ha supuesto numerosas ventajas clave, a nivel tanto interno como externo. Nuestra triple certificación, que cada año se renueva con nuevas y periódicas ampliaciones del ámbito de aplicación, identifica a Orange Business Services como un colaborador fiable y de confianza y reconoce la calidad de nuestro sistema de gestión a nivel global. Desde entonces hemos incorporado ISO 14001 para la gestión ambiental en tres de nuestros centros. Todos nuestros indicadores demuestran que la satisfacción de los clientes ha aumentado considerablemente como resultado de estos esfuerzos. Es más: el programa de certificación ha demostrado ser una excelente forma de reforzar la cohesión de los equipos en nuestro personal, lo cual nos ha permitido mantener la dinámica con el paso de los años.

La creciente adopción de ISO/IEC 20000-1 no es de extrañar si se tienen en cuenta las preocupaciones por la seguridad hoy en día. ¿Podría por favor explicar los beneficios adicionales relacionados con la seguridad de la norma?

ISO/IEC 27001 para la seguridad de la información cubre un espectro definido de nuestras actividades y entidades (de operaciones, de servicios en la nube...), de modo que tenemos que agradecer a ISO/IEC 20000-1, Párrafo 6.6 sobre la gestión de la seguridad de la información, la protección de todos nuestros procesos y actividades en tres niveles: requisitos en nuestros sistemas, controles de seguridad en nuestras operaciones y una cartera de servicios de seguridad gestionados.
Por ejemplo, supervisamos y respondemos de forma proactiva ante los incidentes de seguridad que pudieran afectar a los activos que se nos confían. Para tal fin, nos aseguramos de que todos los cambios se hayan evaluado antes de la implementación, para impedir cualquier impacto potencial en la protección de la seguridad. También hemos introducido sólidos controles de seguridad en nuestros procesos y procedimientos de trabajo que han resultado ser muy efectivos. Las características de seguridad adicionales de ISO/IEC 20000-1 también ayudan a aumentar la concienciación de la seguridad como una parte integrante de la práctica operativa. Asimismo, los auditores han reconocido el comportamiento ejemplar de nuestro personal a la hora de proteger la integridad de los datos.

¿De qué modo está integrada ISO/IEC 20000-1 en Orange Business Services a nivel de procesos, operaciones y estrategia?

ISO/IEC 20000-1 se integró por completo desde el inicio del proyecto en 2008 en un sistema de gestión de seguridad uniforme y global. Resultó especialmente importante, ya que coincidió con el principio de la certificación ISO/IEC 27001 de nuestro principal centro de servicios de Egipto (en El Cairo), al que siguió más tarde nuestro principal centro de servicios de India (en Gurgaon, cerca de Delhi) y, finalmente, nuestras operaciones en Francia, Brasil y Mauricio. Como resultado, los requisitos de ISO/IEC 20000-1 han pasado a formar parte de todos nuestros procesos y actividades, ya sea en nuestras relaciones con clientes, nuestras actividades con proveedores o en todo el ciclo de vida de los servicios, del pedido al suministro.
A nivel de estrategia, Orange Business Services lleva a cabo análisis de gestión periódicos a escala local, regional y global en los que se supervisan cuidadosamente nuestros resultados de certificación. Nos adelantamos a las expectativas de nuestros clientes y adecuamos el alcance según dicte la actividad.

Foto: Orange Business Services

Ya que habéis tenido tanto éxito con la implementación de ISO/IEC 20000-1 principalmente con recursos internos, ¿podría dar algún consejo a los lectores de *ISOfocus*?

Es importante adoptar un planteamiento paso a paso cuando se persigue la certificación. Empezamos formando un equipo específico, experto y cualificado para gestionar el proyecto. A este respecto, consideramos favorablemente el dominio del marco ITIL, que ayuda a alinear los servicios de TI y las necesidades comerciales. Sentimos que era importante realizar un análisis de lagunas metódico y un estudio de viabilidad antes de introducir un servicio nuevo para certificación. Además, reforzamos nuestro grupo de auditores internos como ayuda para la validación del progreso por medio de auditorías anuales de todos nuestros procesos y entidades.
Para generar una dinámica en el personal, también organizamos sesiones de concienciación sobre ISO/IEC 20000-1 y todos los aspectos relacionados con la certificación y las normas. Nuestro objetivo era transmitir las ventajas de un viaje hacia la certificación, sin perder el pragmatismo, para asegurarnos de que todos comprendieran debidamente el fin que perseguíamos al implementar la norma. El truco no es hablar de los requisitos de la norma, sino centrarse en demostrar lo importante que es aplicarlos por el bien de nuestros clientes, nuestros servicios y nuestros procesos. Toda esta andadura, por supuesto, estuvo refrendada por el equipo directivo, lo cual era vital para que llegase a buen puerto.

Se acaba de publicar una nueva versión de ISO/IEC 20000-1, ¿tiene alguna idea de cómo se plantea el futuro? ¿Próximos proyectos/planes?

La nueva versión de ISO/IEC 20000-1 augura perspectivas alentadoras para Orange Business Services. La norma sigue la línea de la nueva estructura de alto nivel utilizada en todas las normas sobre sistemas de gestión de ISO, incluidas ISO 9001:2015, ISO/IEC 27001:2013 e ISO 14001:2015, por lo que esta versión será incluso más fácil de comprender.
Ya estamos estudiando cómo podemos incorporar los cambios en Orange Business Services; nuestro objetivo es ser una de las primeras empresas en implantar con éxito la nueva edición de la norma. ¡Este será nuestro desafío para 2019! ■


Foto: Orange Business Services

***Jean-Pierre Girardin**, Servicios al cliente y Operaciones, Orange Business Services.*

Gracias a la computación en la nube, las organizaciones pueden acceder a potentes capacidades de TI.