ESPECIAL

# "Futuro y seguridad"

## DE Tecnología & Sentido Común

AGOSTO
2021


El Cibercrimen, **LA GRAN AMENAZA** 06 de la vida digital

**Ransomware** 09 ¿hasta en la sopa?

**Blockchain, más allá de las criptomonedas** 12

**El Esquema Nacional de Seguridad cumple 11 años** 15

**El Tsunami Iot** 18

**El Plan España Digital 2025** 22

25 **Estrategias contra el ransomware**

La pesadilla de la exfiltración de datos 27

**Entendiendo Tor,el Anonimato y la Deep Web** 30

Retos del futuro ante **la computación y comunicación cuántica** 34

ESPECIAL

# "Futuro y seguridad"

## DE Tecnología & Sentido Común


**EQUIPO DIRECTO:**
Javier Peris - Piloto
Manuel D. Serrat - Copiloto
Alberto Rodríguez - Equipo Directo
Juan Carlos Muria - Equipo Directo

**MICRO-ESPACIOS**
Marlon Molina - Es Tendencia
Ricard Martínez - Ojo Al Dato
Catalina Valencia - Ecosistema Emprendedor
Víctor Almonacid - La Nueva Administración
Shirley Villacorta - América Próxima
Fernando Ley - Geo Energía

**PUBLICIDAD Y CONTRATACIÓN**
Carmen Usagre
carmen.usagre@businessandcompany.com
Teléfono: +34 96 109 44 44

**GABINETE JURÍDICO**
Jesús López Peláz

**ATENCIÓN AL LECTOR**
tecnologiaysentidocomun@businessandcompany.com

**EDITA**
Business, Technology & Best Practices, S.L.

Av. San Onofre, 20
46930-Quart de Poblet (Valencia)
Teléfono: 96 109 44 44
Fax: 96 109 44 45
https://businessandcompany.com
soluciones@businessandcompany.com




## MANUEL SERRAT OLMOS

Doctor en Informática por la Universidad Politécnica de Valencia, Master en Dirección de TIC por la UPM, dispone de varias certificaciones internacionales en Operación, Gestión y Gobierno de TI ITIL, PRINCE2 y COBIT5, es escritor técnico, ha sido profesor asociado en la UPV y actualmente dirige el departamento de TI en una organización pública, y Responsable del Comité de la Comunidad Valenciana de itSMF España.

**LinkedIn:**
https://www.linkedin.com/in/manuel-david-serrat-olmos/

**Twitter:**
https://twitter.com/mdserrat

# PREPARA A TU ORGANIZACIÓN PARA RETOS FUTUROS CON ITIL® 4

Los avances tecnológicos han transformado la forma en la que adquirimos e interactuamos con bienes y servicios; creando nuevos comportamientos, expectativas y experiencias.
Pero ¿estás preparado para esos retos?

El mundialmente reconocido ITIL 4, es el método de gestión de servicios que proporciona, a organizaciones y profesionales, un modelo operativo digital / de TI de extremo a extremo para la entrega y operación de productos y servicios habilitados por tecnología y permite a los equipos de TI continuar desempeñando un papel crucial en una estrategia de negocios más amplia.

**¿Quieres conocer más?**

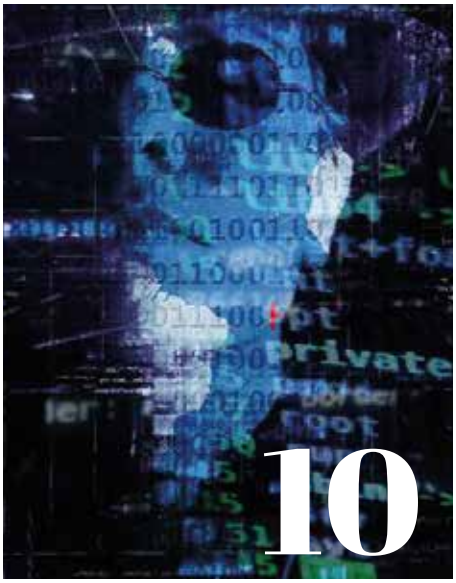
**AXELOS.com/ITIL4-futuro**
(Página en inglés)

ESPECIAL
AGOSTO 2021

#TYSC
TECNOLOGIA Y SENTIDO COMUN

# índice
## DE CONTENIDOS

https://tecnologiaysentidocomun.com


**Ransomware ¿hasta en la sopa?**


**El Esquema Nacional de Seguridad cumple 11 años**


**El Tsunami Iot**


**Entendiendo Tor, el Anonimato y la Deep Web**

# Índice de Contenidos


El Cibercrimen, la gran amenaza de la vida digital ..... 04

Ransomware ¿hasta en la sopa? ..... 06

Blockchain,más allá de las criptomonedas ..... 10

El Esquema Nacional de Seguridad cumple 11 años ..... 14

El Tsunami Iot ..... 18

El Plan España Digital 2025 ..... 22

Estrategias contra el ransomware ..... 26

La pesadilla de la exfiltración de datos ..... 30

Entendiendo Tor, el Anonimato y la Deep Web ..... 34

Retos del futuro ante la computación y comunicación cuántica ..... 38


índice

#TYSC

# El Cibercrimen, LA GRAN AMENAZA de la vida digital

La necesaria Transformación Digital de las economías desarrolladas se encuentra, en este momento de su evolución, ante una situación que amenaza su desarrollo y que puede lastrar gravemente la adopción de nuevas tecnologías o servicios: el cibercrimen, en cualquiera de sus manifestaciones. Crear una Internet segura y que proteja la confianza de los usuarios en los servicios que la puebla será crítico para que esa Transformación siga su curso con éxito.

Hace unos años, los incidentes de seguridad informática los provocaban jóvenes expertos que trataban de probar nuevas técnicas, o de encontrar fallos en sistemas, o simplemente, gamberreaban.. .

Por entonces, se pagaban las llamadas telefónicas a través de un modem para acceder a las clásicas BBS (Bulletin Board System) o a una incipiente Internet fuera del ámbito investigador o militar, y algunos usuarios buscaban formas de ahorrarse esos costes de llamada, intentando engañar a las centrales telefónicas, o usando ilegalmente líneas telefónicas de otros abonados. El modus operandi de este 'ecosistema' se reflejó en una película clásica de los 80, "Juegos de Guerra" [1], obra que ciertamente atrajo a muchos jóvenes de la época hacia los computadores y los videojuegos, pero también, hacia formas ilegales o poco éticas de uso de los recursos tecnológicos. Sin embargo, el impacto de estas actividades era limitado, tanto económica como socialmente hablando, aunque ya hubo casos sonados de hackers capturados, juzgados y condenados en EE.UU., como el ya insigne Kevin Mittnick [2].

Mucho ha llovido desde entonces, y en paralelo a la evolución de los servicios de telecomunicaciones, y en particular, de Internet, las actividades ilegales a través de dichos servicios han cambiado radicalmente. Lejos está aquella imagen romántica del hacker de los 80-90. Hoy en día, se suele mostrar en los medios a los ciberdelincuentes como personas solitarias y encapuchadas, sentadas frente a un ordenador. También esa imagen es una representación distorsionada de la realidad actual. Hoy en día, el cibercrimen es una actividad organizada, a veces incluso, instigada por gobiernos de algunos paises para sabotear a otros, rozando casi el concepto de ciberguerra no declarada. A este respecto, por ejemplo, son públicas las investigaciones sobre grupos de ciberdelincuentes patrocinados desde el gobierno de Corea del Norte [3], o las actividades de empresas como NSO Group [4], que supuestamente sólo venden sus 'armas digitales' a gobiernos.

A estas alturas, Internet es un lugar peligroso, sobretodo, para la actividad económica, incluso sin entrar a valorar todo lo que cualquiera se puede encontrar hoy en día en la Deep Web (o Dark Web) [4]. Y, sin embargo, la mayoría de las personas usan despreocupadamente servicios de todo tipo disponibles en la Red de Redes: correo electrónico, compras, pagos on line, pagos con el móvil, banca on line, formación, búsqueda de emplo, redes sociales,etc. Sin duda, un caldo de cultivo magnífico para el florecimiento de la industria del cibercrimen, que se beneficia además de cuestiones como la transnacionalidad, la anonimidad, el secreto bancario, etc.

Las organizaciones cibercriminales están industrializadas, fijan objetivos, trazan planes, y realizan sus ataques buscando el mayor ratio riesgo/beneficio posible. No son cuatro chavales en un garaje. Son verdaderos profesionales, alojados en edificios de oficinas 'normales', ubicados en países bastante bien determinados. Cuando una organización se convierte en objetivo de uno de estos grupos, y si el 'premio' merece la pena, la amenaza se convierte en persistente y el riesgo alcanza niveles altísimos. Porque además, los profesionales de la seguridad tiene que lidiar con el 'cibercrimen de baja intensidad', formado por otro tipo de cibercriminales de mucho menor nivel pero que armados con scripts y otras técnicas disponibles para cualquiera en la Red, generan tráfico y ruido en los sistemas de control que dificultan la actividad de quienes nos protegen en este ámbito.

**CONTINÚA EN PRÓXIMA PÁGINA**

# Las amenazas del cibercrimen

a nuestra vida digital cubren un amplio abanico de posibilidades, a cual más peligrosa o dañina, pero la ciudadanía en general no está concienciada del riesgo. Los expertos en ciberseguridad consumen gran parte de su tiempo en localizar debilidades de los sistemas antes de que 'los malos' las localicen y exploten, o en construir sistemas que ayuden a proteger las aplicaciones y datos sobre los que residen los servicios que usamos a diario. Incluso hay entidades, como INCIBE [4], que en España realizan una ingente labor de concienciación en ciberseguridad para empresarios y ciudadanos. Sin embargo, el negocio del cibercrimen alcanza cotas insospechadas, gracias a varios factores:

**01** **Usuarios poco sensibilizados**
y más bien confiados, lo que genera poca percepción de riesgo.

**02** **Aplicaciones inseguras**
por diseño.

**03** **Errores de programación**
normales en cualquier producto software.

**04** **Elevada motivación**
de 'los malos'.

**05** **Relativamente reducido coste de explotación**
de un negocio de cibercriminales.

**06** **Bajo riesgo de ser capturados,**
juzgados y condenados.

**07** **Aspectos legales internacionales desfavorables**
A a la investigación del cibercrimen.

**08** **Enorme superficie de exposición al riesgo:**
multiples dispositivos y aplicaciones potencialmente vulnerables.

**09** **Crecimiento de dispositivos inteligentes**
conectados, o Internet of Things (IoT).

**10** **Ingente cantidad de datos disponibles**
para su explotación maliciosa.

**Luchar contra el cibercrimen es tarea de todos. No lo olviden.**

Todos estos factores son de diferente calado, y casi todos de dificultosa resolución. En esta situación, ¿cómo nos podemos estar planteando siquiera 'dar el salto' hacia la economía digital?. Pues posiblemente, porque el camino se hace andando, y normalmente algunos problemas se solucionan o afrontan sólo cuando aparecen. Sin embargo, con ciertas precauciones por parte de todos los agentes implicados en el tema, el impacto de determinadas actividades sería mucho menor. Y pongo como ejemplo el ransomware [7], donde simplemente con determinadas acciones de concienciación de los usuarios de la web y del correo electrónico, que incluyan elevar su desconfianza en determinadas situaciones, se podría reducir bastante el impacto de esta amenaza. Por ejemplo, rechazar los documentos ofimáticos no solicitados, que podrían incluir macros maliciosas; poner la adecuada atención y no clicar sobre enlaces que recibimos a través del correo electrónico sin verificar que efectivamente enlazan a donde dicen enlazar; o no proporcionar datos personales sin ton ni son, todos ellos son consejos que pueden ayudar a evitar un ataque de ransomware a nuestra organización, que podría costarnos desde cientos a millones de euros [8].

## Referencias


[1] https://www.filmaffinity.com/es/film553168.html
[2] https://www.xataka.com/seguridad/kevin-mitnick-genio-o-figura-de-uno-de-los-hackers-mas-famosos-de-la-historia
[3] https://www.technologyreview.com/2020/09/10/1008282/north-korea-hackers-money-laundering-cryptocurrency-bitcoin/
[4] https://es.wikipedia.org/wiki/NSO_Group
[5] https://www.xataka.com/analisis/una-semana-en-la-deep-web-esto-es-lo-que-me-he-encontrado
[6] https://www.incibe.es/
[7] https://www.kaspersky.es/resource-center/threats/ransomware-examples
[8] https://retina.elpais.com/retina/2020/08/20/tendencias/1597917249_738387.html

# Ransomware ¿hasta en la sopa?

Continuamente nos bombardean las noticias acerca de todo tipo de empresas y organizaciones cuyos sistemas quedan inutilizados y bajo el control de ciberdelincuentes, que prometen liberarlos a cambio de una determinada cantidad de dinero en criptomoneda.

En el artículo de este mes de Tecnología y Sentido Común analizamos el fenómeno del ransomware, actualmente la amenaza número uno que afrontan las organizaciones y los individuos en el actual estado de Internet.

En mi artículo del mes de octubre de esta publicación[1] ya citaba el ramsomware como uno de los principales fenómenos actuales del panorama de las amenazas a la ciberseguridad en las redes. También en su artículo en el mismo número de TYSC, nuestro compañero Alberto Rodríguez hacia lo propio con este asunto del ranso- mware. Pero, ¿por qué se considera este tipo de amenaza tan dañina en la actualidad?

Lo primero, es conocer a nuestro enemigo. En su documento "Ransomware: una guía de aproximación para el empresario"[2], el Instituto Nacional de Ciberseguridad de España (INCIBE) define el ransomwa- re como "un tipo de malware que cifra archivos o discos de la víctima, bloqueando sus sistema, y solicitan- do un rescate para recuperar el acceso al sistema y los ficheros".

Esta definición ya no responde totalmente con la reali- dad actual, ya que en estos momentos estamos asistien- do a una serie de campañas de ransomware en las cuales, los ciberdelincuentes, además de exigir el resca- te que consideran oportuno, amenazan a la víctima con publicar la información que han bloquea- do si no paga. Ya no les basta con dejar bloqueada la información, con el daño que eso supone para la víctima que no quiere o no puede pagar, sino que, además, se enfrenta a la posibilidad de sufrir un daño reputacional o industrial si esa información es finalmente publicada[3].

De este comportamiento, el lector podrá deducir que quienes están detrás de estas campañas de ranso- mware no son precisamente hermanitas de la Caridad.

Como muy bien lo define INCIBE[2] "el ransomware (...) es un negocio, ilícito, pero un negocio. Además, no es muy costoso ponerlo en marcha y los benefi- cios son importantes. Están proliferando redes de ciberdelincuentes especializadas en ransomware. En este negocio partici- pan además del creador del ransomware, los que alqui- lan la infraestructura para su distribución o los agentes que lo distribuyen y los servicios para recaudar el rescate". Si en lugar de tratarse de activos digitales lo que se secuestrara fuera una persona, la definición de INCIBE podría cuadrar bastante bien con la de Crimen Organizado.

Otra característica importante del ransomware es que los ciberdelincuentes siempre piden el rescate en criptomonedas, fundamentalmente, en Bitcoins. Esto se debe a la imposibilidad de trazar el dinero del rescate por la utilización de determinados servicios que mezclan los fondos de diferentes cuentas de Bitcoins, realizando realmente un lavado de dinero procedente de actividades presuntamente ilícitas. Como se puede observar, una característica más del Crimen Organizado, equiparable al tráfico de estupe- facientes, de armas o de personas.

Actualmente, conviven dos grandes tipologías de ataques de ransomware: indiscriminados o dirigidos. Las campañas indiscriminadas de ransomware fueron las primeras en aparecer, ya que, como su nombre indica, se basaron en enviar el vector de infección por correo electrónico de forma masiva a una multiplici- dad de direcciones disponibles. Normalmente, en este tipo de campañas el nivel de éxito es bajo, y el coste medio del rescate, también, ya que pueden afectar a hogares y empresas de todo tipo y tamaño. No ocurre igual con los ataques de ransomware dirigidos, en los que los ciberdelincuen- tes se marcan un objetivo que interpretan como lucrativo, recopilan toda la informa- ción que pueden sobre su objetivo, crean una serie de mensajes falsos con un nivel de realismo asombroso, y los envían a su víctima propiciatoria, que acaba infectando a su organización. En estos casos, el nivel de éxito de los ataques es mucho mayor, igual que la recompensa. Recientemente, incluso se ha llegado a ofrecer a un empleado de la empresa a la que se quería atacar una suma importante de dinero si direc- tamente ayudaba a los ciberdelincuentes a meter el ranso- mware en la red de la empresa[4].

CONTINÚA EN PRÓXIMA PÁGINA


Para todas estas campañas se utilizan diferentes técnicas, tanto para realizar la infección, como para engañar a la víctima para que acepte el payload (o carga del código del ransomware).
La forma más habitual es recibir un mensaje de correo de una cuenta que parece legítima y de alguien conoci- do, y que lleva un documento ofimático (casi siempre, en formato Microsoft Word) o un enlace al que se incita a clicar. Si se abre el documento sin las debidas precauciones o se clica en el enlace, la víctima estará sentenciada. Más pronto que tarde, sus ficheros estarán cifrados, y su sistema, a merced de los ciber- delincuentes. En grandes organizaciones, los ciberde- lincuentes esperan a que los sistemas tengan poco uso y poca vigilancia, lo que suele coincidir con los fines de semana, para asegurarse de que todos los recursos posibles se usan en el proceso de cifrado de los fiche- ros y que cuando los usuarios se den cuenta el daño sea ya enorme[5].

Con múltiples grupos de delincuentes creando y distri- buyendo ransomware, y miles de afectados de toda clase a través del globo, es obvio que la "industria del ransomware" se encuentra en pleno florecimiento[6]. La COVI-19 ha supuesto una nueva oportu- nidad de "negocio" para estos ciberdelincuentes, que ni siquie- ra han respetado las instalaciones sanitarias, y a los que ya se les puede incluso imputar al menos un fallecimiento en Alemania. ¿Debemos resignarnos a ser víctimas de este fenómeno? Radical- mente, no. ¿Qué podemos hacer entonces, dada la gravedad potencial de este tipo de amenazas para la supervivencia incluso de determinadas organizaciones?

La medidas de protección frente a la amenaza del ranso- mware pasan por afrontarlo a través de tres líneas de defensa:

**Tecnológicas**, las más básicas de las cuales podrían ser disponer de antivirus de servidor de correo y de estación de trabajo, definir reglas automáticas contra los adjuntos ofimáticos proce- dentes del exterior de la organización, y establecer cierto nivel de vigilancia de enlaces recibidos por correo electrónico. Obvia- mente, la remediación más útil, tras limpiar la infección, es la restauración de las copias de seguridad, para lo cual hay que tenerlas hechas (y comprobadas) con una periodici- dad adecuada. Hay otra técnicas posibles, desde un punto de vista tecnológico, pero exceden el ámbito de este artículo. De nuevo, el documento de INCIBE al que me he referido en varias ocasio- nes[2] es una buena fuente de información al respecto.

**Organizativas**, como la concienciación de los usuarios frente al problema, y la formación de los mismos para que aprendan a identificar este tipo de amenazas cuando las reciben en sus bandejas de entrad de correo.

**Legales**, tales como denunciar tanto las infecciones como los intentos, y apoyar y promover cambios legales internacionales que impidan el lucro de los ciberdelin- cuentes en estos casos.
Recuerden. Luchar contra el cibercrimen, en cuañquei- ra de sus formas, es tarea de todos.

**Referencias**

[1]https://tecnologiaysentidocomun.com/ipages/flipbook/revis- ta-tysc01-octubre-2020 págs. 10-12-
[2] https://www.incibe.es/sites/default/files/contenidos/guias/do- c/guia_ransomware_metad.pdf -
[3] https://www.kas- persky.es/blog/ransomware-data-disclosure/21070/-
[4]https://www.wired.com/story/tesla-ransomware-insider-hack-attempt/-
5]https://www.muyseguridad.net/2019/11/27/ransomware-prosegur/-
[6]https://retina.el- pais.com/retina/2020/08/20/tenden- cias/1597917249_738387.html
[7] https://www.technologyreview.com/2020/09/18/1008582/a-pa- tient-has-died-after-ransomware-hackers-hit-a-german-hospital

**más información en:**
https://javierperis.com/bpm

# Y tú ¿Transformas o Trastornas tu Organización?

## Aprende a:

- ✓ Modelar
- ✓ Mejorar
- ✓ Automatizar Procesos de Negocio

Curso Oficial de Certificación en
**Gestión de Procesos de Negocio**
**ISO/IEC 19510**
**BPM Professional**

Si quieres Aprender, Certificarte, Practicar y recibir posteriormente Ayuda para Liderar con Éxito la Transformación Digital en tu Departamento, Startup, Empresa o Administración, no te quede la menor duda de que este es tu Curso y esta es tu Certificación.

Business&Co.®
Business, Technology & Best Practices, S.L.

# Blockchain, más allá de las criptomonedas

**Uno de los términos más escuchados en el mundillo tecnológico en los últimos tres años es el de blockchain. Pareciera que cualquier sistema tuviera que tener algo de blockchain para 'esta en la cresta de la ola'. En realidad, es un concepto tecnológico en el que se basan ampliamente las monedas virtuales, o criptomonedas, y que aunque puede tener variadas aplicaciones, no es apto para todos los públicos.**

Una cadena de bloques, o *blockchain*, es en esencia una estructura de información compartida en la que su contenido está cifrado y no puede alterarse por un usuario sin conocimiento del resto de usuarios del sistema. Ello la hace especialmente útil para garantizar la adecuada conservación de las anotaciones correspondientes a transacciones, por lo que la primera aplicación practica de este tipo de elemento han sido la pléyade de criptomonedas que pueblan Internet, comenzando con Bitcoin[1].
El funcionamiento, grosso modo, de un sistema blockchain es el siguiente:

1. Cuando un usuario A desea hacer una transacción con un usuario B, solicita su realización a la red blockchain en la que participa.

2. La transacción se transmite a una serie de nodos, que la escriben en el registro de transacciones de la red y la validan mediante una serie de algoritmos propios de la tecnología blockchain utilizda.

3. La transacción validada se une a otras formando un bloque de información, que se cifra y se añade a la cadena de bloques mantenida por la red blockchain, por lo que permanecerá inalterable.

Debemos aclarar que ninguno de los nodos de la red conoce quienes son los usuarios A y B, sólo saben que A ha realizado una determinada transacción con B, porque así está anotado en la cadena de bloques. Los identificadores de los usuarios son los correspondientes a los monederos, o wallets, de cada uno de ellos, que, en el caso de las criptomonedas, es donde termi- narán almacenados esos fondos. El hecho de que los titulares de los monederos virtuales de criptomonedas sean desconocidos ha permitido que éstas hayan sido amplia- mente utilizadas para todo tipo de actividades ilegales, por ejemplo, como comenta- mos en el artículo del mes pasado de TYSC[2], para la recepción de los pagos generados por las campañas de ransomwa- re. Como curiosidad al respecto, reciente- mente se ha vaciado un monedero de bitcoins que estaba durmiente desde 2015 y cuyo valor estimado era de uno mil millones de dólares americanos[3], y que se creía ligado a una red de ciberdelincuencia conocida como Silk Road, desarticulada en 2013. Se desconoce si lo ha vaciado su titular o si alguien ha sido capaz de descifrar la contraseña de cifrado del mismo y se ha hecho con esa ingente cantidad de dinero.

Pero, más allá de los usos de blockchain para las transacciones con criptomonedas, y debido a las propiedades principales de este tipo de tecnologías, se están planteando otros usos mucho más éticos y legales. Al fin y al cabo, se trata de estruc- turas que permiten la confianza distribuida, ya que el diario de operaciones se almacena de forma cifrada y todos los nodos de la red lo conocen y consienten en que lo allí almacenado es cierto. Además, con la inmutabilidad como capacidad de las redes de nodos de una blockchain para prevenir la alteración de transacciones que hayan sido ya confirmadas, puede usarse también para el registro de otros tipos de datos digitales no monetarios.

Por ello, son sistemas apropiados, por ejemplo, para cualquier caso de uso en que se requiera trazabilidad y transparencia. A este respecto, es interesante la iniciativa “Bait 2 Plate” de Treum[4], un sistema que, basandose en una blockchain Ethereum, permite a los consumidores verificar que la captura, procesamiento, y transporte de diferentes tipos de atunes se realiza de forma ética y sostenible, y que e junio de 2017 realizó un piloto con el apoyo de la WWF.

Otro interesante caso de uso de este tipo de tecnologías puede ser, en un futuro más cercano de lo que creemos, la identidad digital autosoberana, es decir, una identidad de una persona que existe independientemente proveedores de identidad, y controlada por la propia persona. Este sistema requiere de una adecuada transparencia de los sistemas y algoritmos de creación y mante- nimiento de esa identidad, de su persistencia en el tiempo y de otras características[5]. De hecho, la Unión Europea admitió a mediados de 2020 que este tipo de sistemas de identificación podrían usarse legalmente en el marco eIDAS de reconoci- miento de identidades electrónicas.

**CONTINÚA EN PRÓXIMA PÁGINA**


de la red, puede falsear rápidamente su contenido para beneficiarse de ella. En redes blockchain públicas, esto es complicado dado el enorme número de nodos, pero si una red blockchain privada con un número relativamente bajo de nodos llega a ser comprometida a través de la agregación de nodos fraudulentos o la toma de control sobre nodos legítimos, los efectos serían devastadores para dicha red.

Pero, a mi juicio, el principal problema de cualquier blockchain no es tecnológico, sino de traslación del 'mundo real' al electrónico. Por ejemplo, si se compra una casa usando criptomonedas, ¿cómo se introduce la transacción de la casa del usuario A al B, y en contrapartida, los fondos del B al A, sin que haya alguien que pueda certificar que ese bien del mundo físico existe, y por tanto, pueda ser objeto de transferencia a través de una transacción blockchain?

Por tanto, antes de lanzarse a llevar la información de su negocio a un soporte basado en blockchain, debe valorarse si se acude a una blockchain pública, en la que los nodos se añaden a la misma sin más que descargar e instalar el software apropiado, o una privada, gestionada por alguna entidad, que es la que permite la agregación de nodos. Pero más importante aún es tener claro si, de verdad, huyendo del *hype* del término blockchain, realmente es adecuada a su caso concreto. No es 'café para todos'.

Uno de los efectos que puede detectarse del uso de blockchain como mecanismo para dar soporte a determinadas operaciones es el de la desaparición de los intermediarios. Por ejemplo, en las redes de criptomonedas no hay ningún intermediario (o banco) que tome el dinero de una cuenta y lo deposite en otra. Son todos los nodos de la red quienes, ante una petición de transferencia de fondos, la aceptan y la anotan, y posteriormente, firman el bloque y lo añaden a la cadena, mediante un consenso definido por el algoritmo de la red.

Sin embargo, y precisamente por el mecanismo de consenso, estas redes son susceptibles ante el conocido como 'ataque del 51%', en el cual si un agente malicioso es capaz de controlar al 51% de los nodos

## REFERENCIAS

[1] https://bitcoin.org/es/

[2] https://tecnologiaysentidocomun.com/ipages/flipbook/revista-tysc02-noviembre-2020

[3] https://arstechnica.com/information-technology/2020/11/someone-has-withdrawn-1-billion-from-a-bitcoin-wallet-dormant-since-2015/

[4] https://www.bbc.com/future/article/20190425-making-sure-fish-is-safe-to-eat

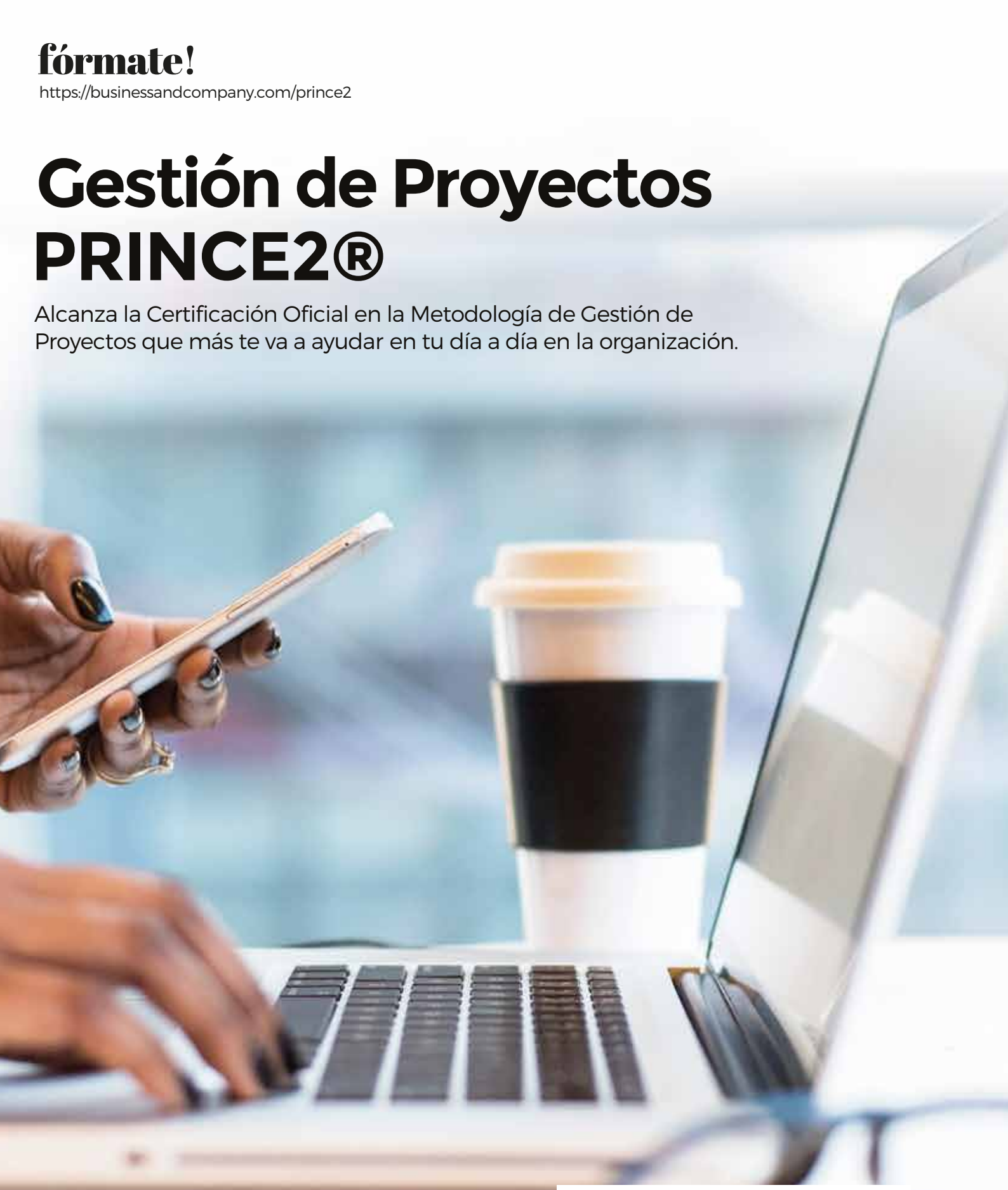
[5] https://blockchainintelligence.es/download/el-uso-de-los-sistemas-de-identidad-auto-soberana-en-el-sector-publico-espanol-y-en-la-union-europea-por-ignacio-alamillo/

fórmate!

https://businessandcompany.com/prince2

# Gestión de Proyectos PRINCE2®

Alcanza la Certificación Oficial en la Metodología de Gestión de Proyectos que más te va a ayudar en tu día a día en la organización.



Business&Co.®
Business, Technology & Best Practices, S.L.

PRINCE2®
ACCREDITED TRAINING ORGANIZATION
PeopleCert ON BEHALF OF AXELOS

# El Esquema Nacional de Seguridad cumple 11 años

**En los días en los que este artículo se publica, el Esquema Nacional de Seguridad está a punto, de cumplir 11 años. Este mes repasamos la importancia de esta norma, no sólo para la Administración Pública, y analizamos las oportunidades que hemos dejado pasar en estos 11 años para mejorar la seguridad de la información y, por qué no decirlo, para generar un nuevo y potente nicho de negocio en el sector TIC nacional.**

Para aquellos que huyen de tener que leer legislación o normativa, quédense tranquilos, y sigan leyendo. Este artículo 'no va de eso', pero es obvio que todo lo que vendrá a continuación emana de un Real Decreto, el 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica[1], el ENS para los amigos. Además de su fecha de aprobación, sólo daré otro dato legal: fue modificado por el Real Decreto 951/2015, de 23 de octubre. Hágame caso, y siga leyendo.

En España solemos pensar que fuera de nuestras fronteras se hacen las cosas mejor, pero en varios aspectos, nuestro país obtiene muy buenos resultados en los rankings internacionales de Desarrollo de Sociedad Digital:

- Ocupa el 2o puesto en servicios públicos digitales.
- Ocupa el 1er puesto en banda ancha ultra-rápida.
- Es mencionada como modelo por nuestra Estrategia Nacional de Ciberseguridad, de la que el ENS es una parte importante.

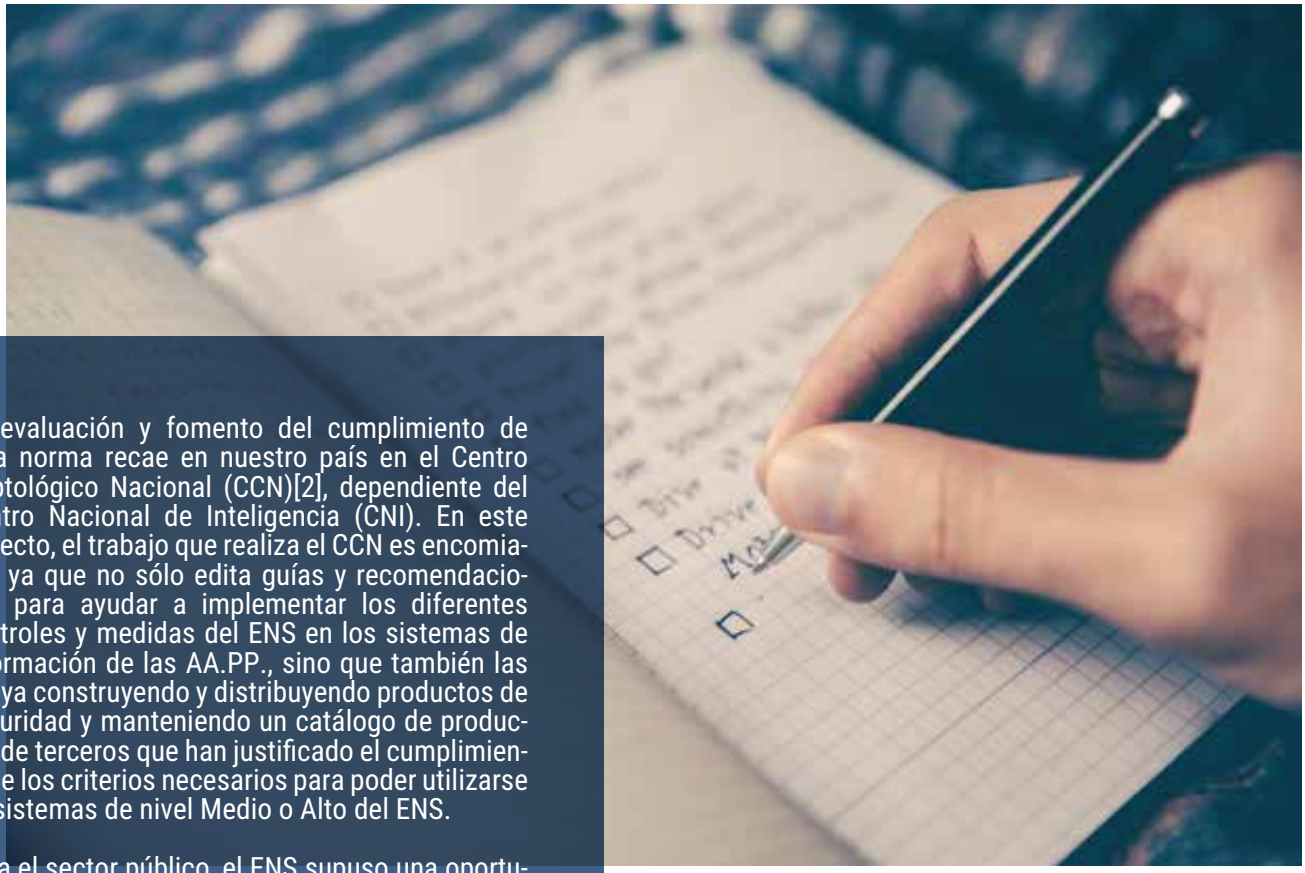
¿Cuál es el objeto de necesitar un Esquema Nacional de Seguridad, que sirva de marco común que deben cumplir todas las AA.PP. y quienes les prestan servicios TIC? Emanado de la extinta Ley 11/2007 de Administración Electróni- ca, la razón de ser del ENS reside en que las Administraciones manejan datos y documentos. Éstos son utilizados para ejercer potestades públicas, y que, por tanto, afectan a derechos de los ciudadanos. Pero, ¿que ocurre con los derechos de un ciudadano o entidad si el dato/- documento en que se basa una decisión de la Administración es erróneo, o peor aún, está mani- pulado maliciosamente? ¿O si todo ese volumen de datos/documentos cae en malas manos? Es obvio que tanto los datos/documentos como los procedimientos para su tratamiento han de ser asegurados, y por ello el legislador pensó en un marco común de aplicación a todos los niveles de la Administración.

Desde un punto de vista muy general, podemos decir que el ENS está ampliamente basado en las normas de la serie ISO 27000, por lo que no puede sino incluir toda una serie de conceptos, controles, medidas, etc. que no están faltos de sentido común, y son ampliamente aceptados por el sector. Es una norma que tenía, y ha mante- nido, 'puntos de contacto' con la normativa de Privacidad y Protección de Datos (LOPDGDD/R- GPD), especialidad de la que en Tecnología y Sentido Común tenemos el honor de contar con el más que experto Ricard Martínez todos los meses.

El ENS establece una serie de cuestiones importantes:

- Define la seguridad como un proceso, integral, y como función diferenciada, basada en las buenas prácticas y los estándares.
- Dibuja un marco organizativo, operacional y de medidas de protección, promoviendo la constitución de un verdadero Sistema de Gestión de la Seguridad de la Información (SGSI).
- Expone la importancia de realizar una adecuada Gestión de Riesgos.
- Categoriza los sistemas de información según el nivel de seguridad que requieran, en Básicos, Medios o Altos, y establece unos requisitos mínimos de seguridad para cada uno de estos niveles, en base a 75 controles.
- Aboga por la concienciación, la formación y la profesionalización del personal de las AA.PP. para una adecuada implantación de las medidas de seguridad, así como por la certifi- cación del nivel de conformidad de productos y servicios con los niveles del ENS.

CONTINÚA EN PRÓXIMA PÁGINA



La evaluación y fomento del cumplimiento de esta norma recae en nuestro país en el Centro Criptológico Nacional (CCN)[2], dependiente del Centro Nacional de Inteligencia (CNI). En este aspecto, el trabajo que realiza el CCN es encomiable, ya que no sólo edita guías y recomendaciones para ayudar a implementar los diferentes controles y medidas del ENS en los sistemas de información de las AA.PP., sino que también las apoya construyendo y distribuyendo productos de seguridad y manteniendo un catálogo de productos de terceros que han justificado el cumplimiento de los criterios necesarios para poder utilizarse en sistemas de nivel Medio o Alto del ENS.

Para el sector público, el ENS supuso una oportunidad para llevar a cabo un proceso de normalización y mejora de sus actividades de seguridad, para la medición de las mismas, y para laconcienciación y profesionalización de su personal. Lamentablemente, el nivel de cumplimiento del ENS es bajo, dado el ínfimo número de AA.PP. que se han certificado en este Esquema, y que según los datos oficiales, de abril de 2020, sólo 496 Entidades Locales han rellenado el Informe INES, de entre las más de 8.000 existentes, de las cuales un 95% tienen menos de 20.000 habitantes y un 83% tienen menos de 5.000.

Para la mayoría de las empresas del sector, estos 11 años del ENS pueden haber pasado casi desapercibidos en cuanto a cifra de negocio, pero las cosas están comen- zando a cambiar, afortunadamente. Las empresas que quieran aprovechar la oportunidad que el ENS les brinda, pueden dedicar sus esfuerzos en ampliar negocio con las AA.P. merced a agregar a su portfolio:

- En el área de Consultoría y Auditoría, ofreciendo servicios de consultoría de adaptación al ENS, certificando el nivel de cumplimiento del ENS de Productos y Servicios de otras compañías, o llevando a cabo Auditorías de Certificación de AA.PP., para lo cual la empresa ha de estar previamente acreditada por ENAC.
- En el área de Servicios, ofreciendo servicios certificados, o seguridad gestionada.
- En el área de Producto, distribuyendo productos certificados para el ENS, o produciéndolos y certificándolos. Se prevé que pronto, lo que ha sido una norma con escaso cumplimiento, va a vivir una auténtica explosión en lo que a negocio se refiere, y sólo las empresas que comprendan el ENS, lo apliquen en sus productos y servicios, y que acompañen a las AA.PP. en su tortuoso camino hacia su digitalización segura, podrán aprovechar este nicho de negocio. Es más, no estar en ese movimiento puede directamente dejarles fuera de la posibili- dad de hacer negocios con la Administración. Para proveedores de bienes y servicios TIC y similares, sería importante en este momento revisar su portfolio de productos y servicios, para adaptarlos de cara a su certificación ENS; incluir en dicho portfo- lio para las AAPP soluciones específicas con ENS (y LOPDGDD/R- GPD) desde el diseño; fomentar que los fabricantes que distribu- yen certifiquen sus productos; y diferenciarse de la competencia, generando confianza y credibilidad con personal experto formado al efecto.

Piénsenlo bien. Esta vez puede tener premio.

**REFERENCIAS**

[1] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-1330
[2] https://www.ccn-cert.cni.es/

fórmate!

https://businessandcompany.com/msp

# Managing Successful Programmes MSP®

## Curso de Gestión de Programas de Proyectos MSP® Fundamentos

MSP®

ACCREDITED TRAINING ORGANIZATION

PeopleCert ON BEHALF OF AXELOS

Business&Co.®

Business, Technology & Best Practices, S.L.

# El Tsunami Iot

**Ya hemos comentado, en artículos anteriores en Tecnología y Sentido Común, la importancia capital que está tomando desde hace algún tiempo la ciberseguridad. Es habitual enfocarse en nuestros ordenadores, redes y servidores cuando pensamos en un entorno seguro. Sin embargo, una verdadera pléyade de nuevas amenazas se pueden materializar a través de un conjunto relativamente nuevo de elementos conectados y con inteligencia, que forman la Internet de las Cosas (IoT). En este artículo trataremos de explicar el porqué de esta gran amenaza que puede impactar en los sistemas de información de las organizaciones y particulares.**

A todo el mundo (o casi) le gustan los altavoces inteligentes/asistentes personales, tales como Alexa o Nest, que han sido regalo habitual desde hace un par de años. Todo el mundo quiere tener una SmartTV en su salón.

El control domótico de las viviendas es fantástico y mejora la comodidad de sus habitantes, con enchufes inteligentes, controles climáticos, cerraduras electrónicas, etc. que podemos gestionar desde nuestro teléfono móvil. Las ciudades quieren ser inteligen- tes y lanzan por doquier proyectos de SmartCities, de mayor o menor calado y ambición. Hay cámaras IP en cualquier lugar, hasta en el más insospechado. Hasta la nevera o el robot de cocina pueden conectarse a Internet para gestionarnos la lista de la compra o descargar nuevas recetas. A todo este universo de elementos que se conectan a Internet de forma autónoma para realizar sus funciones

El enfoque clásico de la seguridad, aunque tenga múltiples capas o facetas, tiene uno de sus principios en el control de la superficie expuesta a las amenazas. "Casa con dos puertas, mala es de guardar", dice el dicho castellano. Una ciudad se amurallaba y se le dejaban dos o cuatro puertas, por lo general. A estas alturas, todos deberíamos saber ya que cualquier producto hardware o software tiene vulnerabilidades, que pueden ser descubiertas y explotadas de las maneras más variadas e imaginativas que se puedan pensar. Estaremos de acuerdo en que, para un sistema compuesto por N elementos, de complejidad CN cada uno de ellos, el número de vulnerabilidades, y quizá su grave- dad, está en función de N y de CN. Por tanto, si a ese sistema se le agregan un número Z de elementos, el riesgo de que exista una vulnerabilidad que se pueda utilizar para afectar gravemente al sistema aumenta.

Asumimos, pues, que existe un riesgo intrínseco en aumentar los elementos que, en una casa, en una empresa o en una administración pública, tenemos conectados a nuestra red. Evidentemente, se pueden poner medidas de seguridad, tales como firewalls, autenticaciones fuertes de doble factor, segmentación de redes, etc. Y seguro que hay alguien que lo hace. Sin embargo, no es el modus operandi habitual. Lamentablemente, son cosas que también pasan en entornos IT y OT[1]: configuraciones de desplie- gue inseguras, contraseñas por defecto o de fabricante, firmwares vulnerables no actualizados, etc. Basta consultar fuentes como SHODAN[2] para hacerse una idea de la cantidad de sistemas que presentan este tipo de problemáticas de ciberseguridad.

En el mundo IoT, cuyo impacto económico la consultora IDC esperaba en 2018 que sea de 1,1 billones de dólares en 2023[3], o se es muy cuidadoso con el despliegue, o puede convertirse en un infierno para todos. Y es muy fácil poner algunos ejemplos:

- Imaginen una casa completamente conectada, que cae en manos de un ciberdelincuente, capaz de subir o bajar la temperatura hasta hacerla inhabitable o averiar la climatización. O que pueda contro- lar al frigorífico y éste comience a hacer compras a diferentes supermercados sin autorización del propietario de la vivienda.

CONTINÚA EN PRÓXIMA PÁGINA


O que bloquee la puerta de acceso a la vivienda, a través de la cerradura inteligente, o juegue compulsivamente con las luces de la casa. Y todo ello, hasta que reciba un pago por liberar nuestro sistema y devolvernos su control. Pago que, por cierto, no garantizará que realmente vuelva a nuestro control. Y si ese es el caso, o inmediatamente se toman las medidas oportunas de seguridad, detectando el origen de la intrusión y solucionando el problema, o al día siguiente podemos volver a tener al mismo intruso, o a otro parecido, pidiendo más dinero.

- Imaginen una ciudad inteligente, con un despliegue de sensores de temperatura, lluvia, viento, contaminación, etc., con sus sistemas de ilumina- ción, señalización y agua potable inteligentes, con cámaras de tráfico y seguridad ciudadana, algunas incluso de acceso público en lugares emblemáticos, drones de vigilancia autónomos, etc. En dicha ciudad, o absolutamente todos los elementos de ese entorno SmartCity están adecuadamente configurados, securizados y monitorizados, o los efectos pueden ser catastróficos en caso de que ese sistema caiga en manos de delincuentes: apagado de cámaras por donde va a circular los atracadores de un banco; cambios en la cloración de las aguas potables que lleguen a hacerlas no potables o tóxicas; problemas de tráfico por la reprograma- ción de semáforos; apagado de la iluminación viaria por la noche, etc. El catálogo de maldades posibles es directamente proporcional al número de servicios conectados, a las capacidades de éstos y a su criticidad.

- ¿Y qué hay de las amenazas a la privacidad o la salud? Relojes inteligentes que midan mal el ritmo cardíaco, marcapasos hackeables, SmartTV con webcam y micrófono integrados utilizadas para espiar a los propietarios, asisten- tes personales intervenidos que espían a los usuarios[4], tormentas de datos desde dispositivos que bloquean redes coropratívas o sistemas de monitorizción, o sistemas IoT que dependen de servicios cloud que se caen[5], etc.

¿Quiere decir ésto que no debemos apostar por este tipo de elementos? La respuesta es estándar: depende. Si se es consciente de los riesgos, éstos se evalúan y mitigan, y el riesgo residual es asumible, adelante. Si se configuran adecuadamente los dispositivos pensando en la seguri- dad y privacidad, adelante. Si se confía en el fabricante e instalador de los elementos IoT, adelante. Si se tiene sentido común y sólo se utilizan este tipo de elementos en aquellos entornos en los que el beneficio a obtener (del tipo que sea) por su uso merezca la pena frente a los riesgos, adelante. Pero como alguna de las condiciones que acabo de citar no se cumpla, más le vale pensarlo dos veces antes de desplegar cualquier elemento IoT, porque puede convertirse en una gota más en el tsunami de incidentes de ciberseguridad que se avecina por esa IoT defectuosamente desplegada.

Recuerden. La ciberseguridad es una tarea de todos, y para el beneficio de todos.

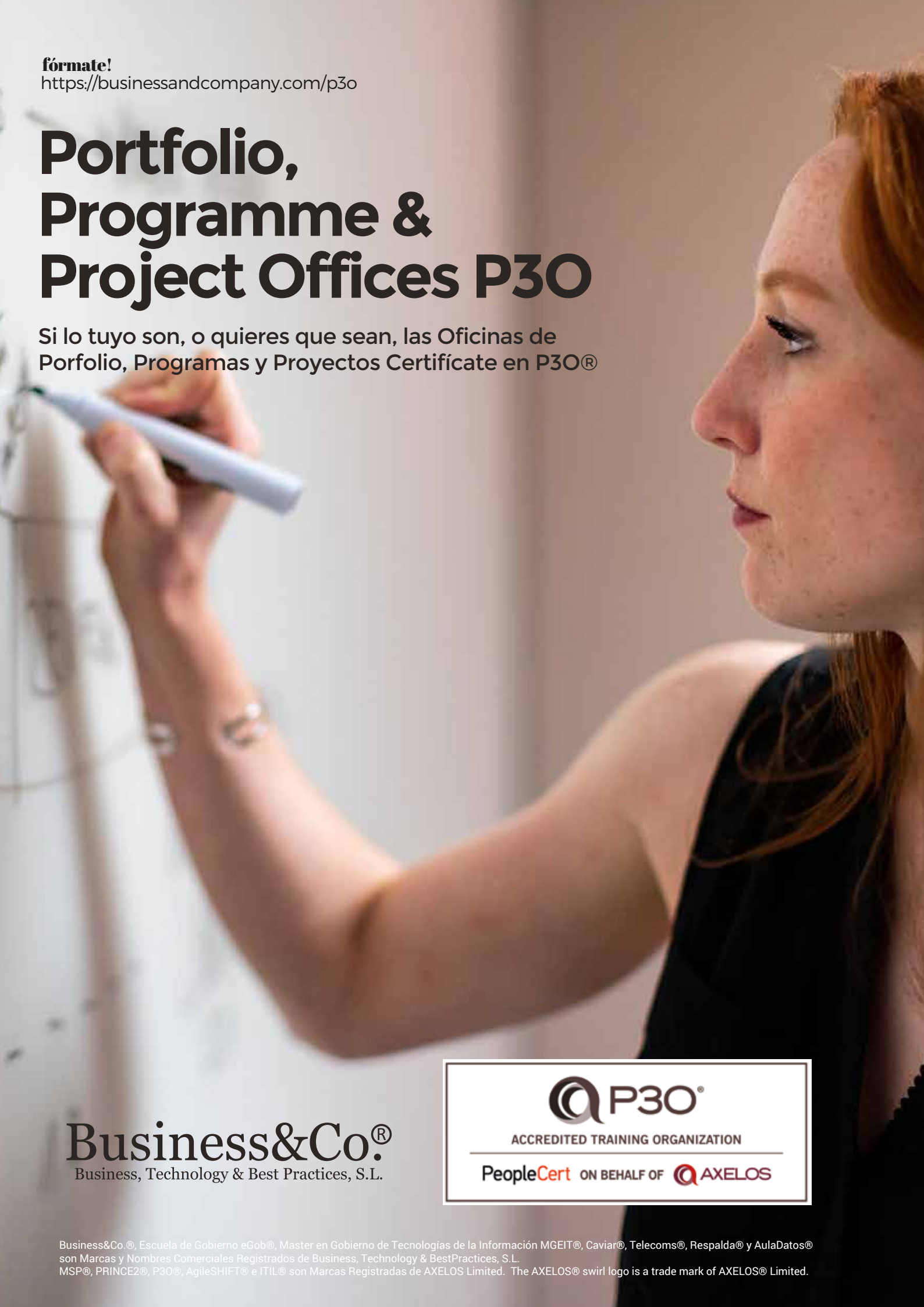
**REFERENCIAS**

[1] https://oasys-sw.com/diferencias-entre-it-y-ot/
[2] https://www.shodan.io/
[3] https://www.fundacionbankinter.org/en/ftf/tendencias/internet-de-las-cosas/ftfrefresh/impactoiot
[4] https://www.eleconomista.com.mx/tecnologia/Alexa-de-Amazon-te-ha-espiado-lo-sabes-20190511-0021.html
[5] https://www.xataka.com/seguridad/quedarse-encerrado-calefaccion-imprevisibles-consecuencias-apagon-google-casa-conectada

fórmate!
https://businessandcompany.com/p3o

# Portfolio, Programme & Project Offices P3O

Si lo tuyo son, o quieres que sean, las Oficinas de Porfolio, Programas y Proyectos Certifícate en P3O®



Business&Co.®
Business, Technology & Best Practices, S.L.

P3O®
ACCREDITED TRAINING ORGANIZATION
PeopleCert ON BEHALF OF AXELOS

# El Plan España Digital 2025

**Como parte del Plan Europeo de recuperación tras la pandemia provocada por el SARS-Cov-2, España presentó el conocido como Plan de recuperación, transformación y resiliencia. Una de las bases fundamentales de ese Plan es la digitalización de la economía española, para reducir su dependencia del turismo y el urbanismo. Y para ello, disponemos del Plan España Digital 2025, cuyas líneas fundamentales analizamos en el artículo de este mes.**

Desde hace unos años, se han aprobado varios planes para avanzar en la transformación digital de nuestro país, tales como el Plan Avanza, o el Plan InfoXXI, casi todos basados en cuatro pilares fundamentales: la capacitación digital de la ciudadanía, el despliegue de más y mejores redes de telecomunicaciones, el avance de la Administración electrónica, y la digitalización de los sectores productivos, y por ende, de la economía. Recientemente, el Gobierno de España ha aprobado el **Plan España Digital 2025**[1], que ha de ser una de las principales líneas de actuación del **Plan de recuperación, transformación y resiliencia** 2] que ha de favorecer que nuestro país salga lo mejor posible de la crisis económica que ha traído consigo la pandemia global del COVID-19, gracias al Fondo de Reconstrucción de la Unión Europea.

El Plan España Digital 2025 contiene medidas en torno a diez ejes fundamentales, y cito:

**1.** Garantizar una conectividad digital adecuada para el 100% de la población, promoviendo la desaparición de la brecha digital entre zonas rurales y urbanas (…).

**2.** Continuar liderando en Europa el despliegue de la tecnología 5G, incentivando su contribución al aumento de la productividad económica, al progreso social y a la vertebración territorial (…)

**3.** Reforzar las competencias digitales de los trabajadores y del conjunto de la ciudadanía (...).

**4.** Reforzar la capacidad española en ciberseguridad, consolidando su posición como uno de los polos europeos de capacidad empresarial (…)

**5.** Impulsar la digitalización de las Administraciones Públicas (...)

**6.** Acelerar la digitalización de las empresas, con especial atención a las microPYMEs y las start-ups (…)

**7.** Acelerar la digitalización del modelo productivo mediante proyectos tractores de transformación sectorial que generen efectos estructurales (…)

**8.** Mejorar el atractivo de España como plataforma europea de negocio, trabajo, e inversión en el ámbito audiovisual (…)

**9.** Favorecer el tránsito hacia una economía del dato, garantizando la seguridad y privacidad y aprovechando las oportunidades que ofrece la Inteligencia Artificial (…)

**10.** Garantizar los derechos de la ciudadanía en el nuevo entorno digital (…)"

Coincidirá conmigo el lector en que son acciones (casi todas) muy lógicas para el mundo en que vivimos. Medidas para las cuales, además, se supone que va a llegar un volumen importante de fondos europeos, por lo que es una oportunidad, que nuestro país no puede dejar escapar, para reducir nuestra dependencia del sector turístico y del 'ladrillo', aumentando el peso de la industria y de la parte de servicios no relacionados con el turismo, y con ello nuestra capacidad de soportar mejor futuras crisis.

CONTINÚA EN PRÓXIMA PÁGINA

Acordes a las 10 líneas de actuación o medidas antedichas son sus metas para 2025, y cito:

**Eje 1.**
Meta: 100% de la población con cobertura 100 Mbps.

**Eje 2.**
Meta: 100% del espectro radioeléctrico preparado para 5G.

**Eje 3.**
Meta: 80% de personas con competencias digitales básicas, de las que el 50% serán mujeres.

**Eje 4.**
Meta: 20.000 nuevos especialistas en ciberseguridad, IA y Datos.

**Eje 5.**
Meta: 50% de los servicios públicos disponibles en app móvil.

**Eje 6.**
Meta: 25% de contribución del comercio electrónico al volumen de negocio PYME.

**Eje 7.**
Meta: 10% reducción de emisiones $CO_2$ por efecto de la digitalización.

**Eje 8.**
Meta: 30% de aumento de la producción audiovisual en España.

**Eje 9.**
Meta: 25% de empresas usan IA y Big Data.

**Eje 10.**
Meta: Una carta nacional sobre derechos digitales.

El texto del Plan, a lo largo de sus 90 páginas, desgrana las 48 líneas de actuación que se van a implementar en cada uno de los ejes. Como es obvio que la mejor forma de conocerlas es leerse el propio documento del Plan, no voy a ser exhaustivo en citarlas, pero sí me gustaría resaltar en este texto algunas de ellas, por diferentes motivos.

El Plan de Conectividad Digital (medida 1), del Eje 1, porque pese a que la penetración de la banda ancha en nuestro país es muy alta respecto de otros países europeos, también es muy desigual geográficamente hablando, y ello es un freno para el desarrollo económico de esas zonas 'digitalmente aisladas'.

El Plan Nacional de Competencias Digitales (medida 11), del Eje 3, imprescindible en un país en el que es habitual jactarse de que se desconoce algo, y aún más si se trata de cuestiones tecnológicas. Será una reminiscencia cultural del 'que inventen otros'.

El Fortalecimiento de la ciberseguridad de ciudadanos, PYMEs y profesionales (medida 14) , del Eje 4, y que debe llevar aparejada necesariamente la creación de puestos de trabajo de expertos en ciberseguridad, además de la concienciación y formación de la ciudadanía en general.

El Puesto de Trabajo de Nueva Generación (medida 22), del Eje 5, para la Administración Pública, donde aún hay personajes recalcitrantes que incluso se oponen al teletrabajo, y que ha de cambiar de ser una Administración que presta servicios reactivos a prestar servicios de forma proactiva.

El Plan de Impulso a la Digitalización de PYME (medida 26), del Eje 6, muy necesario en un país como el nuestro con el volumen de PYMEs que tenemos y el empleo que generan.

La Estrategia nacional de Inteligencia Artificial (medida 41), del Eje 9, que ya fue presentada hace unos meses, y que pretende que nuestro país no se quede atrás en esta materia.

La Modernización del marco laboral aplicable al trabajo a distancia (medida 48), del Eje 10, para superar el modelo presencialista, típico de calentar la silla, y conseguir un marco que, facilitando la conciliación, pueda medir los objetivos cumplidos y no el tiempo de presencia en la oficina.

Una advertencia final a los responsables de llevar a cabo este Plan: recuerden Uds. que para 2025 quedan menos de 4 años. Y quien avisa no es traidor.

**REFERENCIAS**

[1] https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/230720-Espa%C3%B1aDigital_2025.pdf
[2] https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/plan_de_recuperacion.pdf

# Estrategias contra el ransomware

**La amenaza del ramsomware persiste y evoluciona, y es necesario conocerla y enfrentarla, cada cual según los medios de que disponga y los activos que deba proteger. Es importante, sin embargo, tener claras las diferentes estrategias o lineas de actuación frente a este fenómeno, para evitarlo o minimizar su impacto en las operaciones.**

En el número 2, de noviembre de 2020, de Tecnología y Sentido Común[1] ya tratamos la problemática que representaba el fenómeno del *ramsomware*.

Este mes de marzo, una entidad pública del tamaño del SEPE (Servicio Público de Empleo Estatal, el antiguo INEM) ha sufrido un ciberataque de este tipo que, según los medios, afectó a su página web, a las aplicaciones corporativas e, incluso, al sistema de atención telefónica, paralizando completamente su actividad[2]. Aparte de los perjuicios a los ciudadanos, se produce en estos casos un evidente daño reputacional a la entidad atacada. Y aunque se pueda recuperar el funcionamiento de la misma en un periodo razonable de tiempo y con una pérdida mínima de información, en estos casos siempre es mejor prevenir que curar.

En el citado artículo de noviembre, se indicaba que las medidas de protección frente a la amenaza del *ransomware* pasaban por afrontarlo a través de tres líneas de defensa: tecnológicas, organizativas, y legales. Sin embargo, todas ellas deben tener como hilo conductor la defensa en profundidad de los sistemas de información de la organización, desde el perímetro hasta el puesto de trabajo, desde la infraestructura del centro de proceso de datos hasta los servicios en la nube, desde la Alta Dirección hasta el último de los empleados. Con redes cuyos límites son cada vez más difusos, debido a la movilidad, al BYOD, al teletrabajo, etc, es crítico que todas las medidas a tomar estén coordinadas y sean coherentes entre sí, sean respaldadas por la Dirección de la organización, y se enfoquen en dos aspectos: la prevención, y la reducción del impacto en caso de infección.

Entre las medidas a tomar para evitar la infección de *ransomware*, una de las más importantes es la **concienciación y formación de los usuarios** de los sistemas de información. Ni que decir tiene que muchas medidas de seguridad implantadas pueden irse al traste si un usuario abre un fichero infectado sin más precauciones, pensando que es legítimo. De ahí la importancia de que nuestros usuarios de sistemas de información conozcan la existencia de este tipo de malware (y de otros tipos), aprendan a tomar precauciones antes de abrir archivos adjuntos o enlaces, e incluso sean capaces de detectar correos electrónicos sospechosos y los manejen con precaución hasta que se confirme o no su maliciosidad. Por esa razón, la capacitación y actualización de los usuarios de nuestros sistemas de información a este respecto debe ser continuada, siguiendo una adecuada planificación, y con los medios de concienciación apropiados.

Sin embargo, no sólo de concienciación y formación puede vivir la prevención. Disponer de un **antivirus actualizado** en los puestos de trabajo es ya un clásico, pero ya no es suficiente. Herramientas como microClaudia, del Centro Criptológico Nacional[3], aportan un enfoque diferente, más parecido al de una **vacuna**, frente a las amenazas de ransomware. Esta herramienta, disponible únicamente para entornos Windows, realiza determinados cambios en el sistema operativo que hacen que, en caso de infección de alguno de los malwares 'vacunados', éste crea que el sistema ya está infectado y no ejecuta su carga maliciosa. Si a esto le añadimos servicios de antivirus y antispam al servicio de correo electrónico, redondeamos la jugada.

También los **cortafuegos** o sistemas de detección de intrusiones, en el perímetro y en los puestos de trabajo, funcionando de forma coordinada, pueden tanto impedir la infección, como reducir a la mínima expresión los efectos de una posible infección. Por ejemplo, en el caso de que un usuario en un PC ejecute un fichero malicioso, y éste comience a realizar su actividad dañina, tal vez realice conexiones al exterior de la red de la entidad atacada. En ese momento, tanto el cortafuegos local como el de perímetro podrían bloquear esas conexiones, impidiendo al ransomware ejecutarse de forma normal, e incluso podrían bloquear al equipo infectado, derivándolo a una subred de cuarentena hasta que se pueda analizar la amenaza y llevar el equipo a un estado seguro antes de reincorporarlo a la red. Para ello, deberemos disponer en la red de los elementos adecuados, de los cuales hay una amplia variedad en el mercado, pero cuya característica fundamental ha de ser la de dotar de inteligencia y automatización a la red corporativa.

La vieja y humilde **copia de seguridad** también es una medida a tener muy en cuenta, pero en este caso, formará parte de las necesarias para la reducción del impacto de una infección, ya que permitirá devolver los sistemas de los que se hizo copia a un estado conocido, y supuestamente previo a la infección o a sus consecuencias. Para ello es esencial un adecuado esquema de copias de seguridad, adaptado a las necesidades de recuperación definidas por la organización (RTO y RPO[4]) que incluyan copias fuera de línea, para evitar que se pudieran ver afectadas por un ataque de ransomware.

**CONTINÚA EN PRÓXIMA PÁGINA**

Pero hay otra cuestión que va a reducir el impacto de uno de estos ataques y que suele olvidarse: la **planificación**. Si la organización cuenta con un Plan de Continuidad de Negocio (BCP), a buen seguro dispondrá de un Plan de Recuperación antes Desastres (DRP) que afronte desde todas las ópticas una amenaza como el *ransomware*. Disponer del Plan significa también necesariamente mantener entrenado al personal que ha de llevarlo a cabo en caso de ser necesario, por lo que los simulacros formarán parte de la actividad tanto preventiva como de reducción del impacto. Obviamente, el DRP puede ser erróneo, o su ejecución puede sufrir errores humanos o técnicos o inconvenientes de todo tipo. El DRP se depura con la práctica, y es mejor que esa práctica sea durante un simulacro que cuando se produce un ataque real.

Pero lo que no admite ninguna discusión es que es mucho mejor disponer de un mal Plan que no disponer de ninguno. La tensión a la que se está sometido en el momento en que se produce un incidente de este tipo es tal que es mejor no tener que ponerse a pensar cómo solventar la situación, y directamente aplicar un protocolo escrito y comprobado. Porque es más fácil tomar decisiones correctas con el tiempo y la información adecuados que cuando no se dispone ni del tiempo ni de la información correcta.

En conclusión, las estrategias para afrontar la amenaza del *ransomware* pasan por actividades de prevención y reducción de impacto, planificadas, coherentes, y por supuesto, adaptadas al entorno técnico, organizativo y económico de lo que se desea proteger.

**REFERENCIAS**


[1] https://tecnologiaysentidocomun.com/ipages/flipbook/revista-tysc02-noviembre-2020 págs. 10-12
[2] https://www.elmundo.es/economia/2021/03/09/6047578d-fc6c83411b8b4795.html
[3] https://www.ccn-cert.cni.es/soluciones-seguridad/microclaudia.html
[4] https://www.swgreenhouse.com/conceptos-de-continuidad-de-negocio/rto-rpo

fórmate!
https://businessandcompany.com/cobit

# Tu vida puede depender de la tecnología

## COBIT® 2019 Marco de Gobierno y Gestión de la Tecnología

La Implementación de un Marco de Gobierno y Gestión de Tecnologías de la Información permite conocer la salud global de los Sistemas de Información de los que depende los procesos habituales de una organización, sin un adecuado Marco de Gobierno y Gestión se podrá trabajar la seguridad, privacidad y otros aspectos de manera disociada tampoco se podrá garantizar que se estén teniendo en cuenta todos los factores necesarios para una adecuada operación. COBIT® aporta confianza.


Business&Co.®
Business, Technology & Best Practices, S.L.

# La pesadilla de la exfiltración de datos

**En el artículo del mes pasado tratamos las diferentes estrategias para afrontar el ransomware. En el artículo de nuestro compañero Alberto Rodríguez del mismo número de TYSC se hablaba de las técnicas OSINT. Este mes nos enfrentaremos a uno de los efectos más novedosos de los ataques de malware: las exfiltraciones de los datos obtenidos durante un ataque.**

¿Quién no ha oído a algún individuo aquello de '*a mi me da igual que me espíen, porque no tengo nada que ocultar*', refiriéndose no sólo a los ciberdelincuentes, sino también a las agencias de seguridad nacionales o a las grandes compañías tecnológicas? Dejando de lado el hecho de que cualquier elemento tecnológico comprometido por un extraño puede ser utilizado para todo tipo de actividades malignas, es un comentario del todo irresponsable que, sobretodo hoy en día, hay que tratar de desterrar. La privacidad, y la seguridad en la que ha de basarse, deben ser potenciadas en un mundo digital en el que tan fácil es, por ejemplo, suplantar la identidad de otra persona. Y al final, muchos de los elementos de nuestra identidad están hoy en día en soportes digitales.

Recientemente se han producido dos ataques de *ransomware* con cierta repercusión pública en España: el primero de ellos, al SEPE, como ya indicamos en nuestro artículo anterior[1]; y el segundo, al Ayuntamiento de Castellón de la Plana[2]. En este segundo caso, parece que los ciberdelincuentes, al no obtener el pago de su extorsión al cifrar los ficheros de esa Administración, han decidido publicar nada menos que 119 GB de datos robados en ese ataque[3]. Es una nueva modalidad del ransomware: no sólo cifran los ficheros y exigen un rescate por ellos, sino que amenazan con publicarlos si no reciben el pago en un corto periodo de tiempo.

Es obvio que las únicas estrategias, entre las mencionadas en mi artículo del mes pasado, que pueden funcionar contra este tipo de efecto de un ataque exitoso, son las estrategias preventivas, ya que aunque recuperemos la actividad en un tiempo razonable y no se pierda información, si el atacante **exfiltra** los datos que haya conseguido descargar desde el sistema atacado, no sólo la reputación de la organización puede estar en riesgo, sino que también se expone a potenciales sanciones de los organismos de control en materia de protección de datos, en el caso español, la Agencia Española de Protección de Datos. ¡Un verdadero infierno!

Este tipo de actividad, también denominada *leak,* no sólo se produce por un ataque de *ransomware*. El robo de información ha sido, históricamente, uno de los móviles para violentar sistemas de información, y también es uno de los métodos de venganza de empleados insatisfechos o necesitados de dinero, que vuelcan datos de la organización y, o bien los publican, o bien los venden a la competencia. Son muy conocidos los casos de los cables del Pentágono, publicados por Wikileaks, y obtenidos presuntamente a través de un empleado descontento, Bradley (o Chelsea) Manning[4]; los llamados 'papeles de Panamá', obtenidos al parecer del despacho de abogados panameño Mosack y Fonseca; o la filtración conocida como 'FootballLeaks', en la que se pusieron al descubierto documentos privados de transacciones entre clubes de fútbol, futbolistas y agentes.

En las organizaciones, es conveniente disponer de una política de prevención de las filtraciones o pérdida de datos (del inglés Data Loss/Leakage Prevention, DLP), basada tanto en medidas organizativas como en ciertas medidas técnicas y de seguridad física. Pero, ¿y el común de los mortales, el ciudadano de a pie, que tiene en sus dispositivos tecnológicos información personal, supuestamente poco valiosa para los ciberdelincuentes, qué hace? ¿Quién, de entre los lectores, no tiene una app en su dispositivo móvil con acceso a su banco? ¿Quién no tiene escaneado en su PC personal su documento de identidad? Por no hablar de la 'moda', por llamarla algo, del 'sexting', de enviar fotos íntimas a través de medios tecnológicos, y que hace que los dispositivos contengan material altamente privado, con el que se puede hacer mucho daño a la reputación de muchas personas si cae en malas manos.

CONTINÚA EN PRÓXIMA PÁGINA


cAnimal=setclass("Animal")
function
cAnimal.methods:init(action,
cutename)
self.superaction = action
self.supercutename = cutename
end
cTiger=setclass("Tiger",
cAnimal)
function
cTiger.methods:init(cutename)
self:init_super("HUNT
Tiger)", "Zoo Animal (Tiger)")
self.action = "ROAR FOR ME!!"
self.cutename = cutename
end
Tiger1 = cAnimal:new("HUNT",
"Zoo Animal")
Tiger2 = cTiger:new("Mr
Grumpy")
Tiger3 = cTiger:new("Mr
Hungry")
print("CLASSNAME FOR TIGER1
", Tiger1:classname())
print("CLASSNAME FOR TIGER2
", Tiger2:classname())
print("CLASSNAME FOR TIGER3
", Tiger3:classname())
print("==========")
print("SUPER
ACTION", Tiger1.superaction)
print("SUPER
CUTENAME", Tiger1.supercutename)
print("ACTION
", Tiger1.action)
print("CUTENAME", Tiger1.cutename
)
print("==========")
print("SUPER
ACTION", Tiger2.superaction)
print("SUPER
CUTENAME", Tiger2.supercutename)

Si, además, esas exfiltraciones se usan en combinación con otras técnicas de obtención de información, conocidas como OSINT, el daño puede resultar catastrófico. Imagine la situación: a través de una app maliciosa, nos roban una copia digital del DNI y acceso a nuestra cuenta bancaria. Con un poco más de esfuerzo, consiguen duplicar la SIM de nuestro teléfono móvil. Con estas tres cosas, cualquier puede hacerse pasar por nosotros en múltiples situaciones de la vida digital. Y si además consiguen hacerse con nuestra cuenta personal de email, el desastre será absoluto. Con esos datos y documentos importantes, más la información que puedan obtener a través de nuestra exposición, por ejemplo, en redes sociales, podríamos pasar de ser las víctimas de un delito, a ser legalmente responsables de lo que esos ciberdelincuentes pudiesen hacer con nuestra identidad robada: tarjetas de crédito sin control, compras en Internet que no habremos hecho nosotros, ventas fraudulentas a otros usuarios de Internet, etc. Pasamos de víctima a presunto delincuente, y va a ser complicado demostrar que el verdadero delincuente es quien nos ha robado nuestra identidad digital.

¿Cómo evitamos, pues, ser blanco de este tipo de problemáticas? En primer lugar, siendo muy precavidos. Los ataques de *phishing, vishing y smishing* se basan en parecer legítimos y en que nos fiaremos de según quien sea el que nos remita el correo malicioso. Mejor no clicar en enlaces recibidos a través del email, ni instalar apps en nuestro terminal móvil descargadas a través del mismo tipo de enlaces. **Mejor sospechar de todo** y verificar todo tipo de información y enlaces antes de clicar sobre ellos. Los fraudes al CEO también comienzan con técnicas de este tipo.

Tampoco es conveniente mantener determinada documentación en nuestros dispositivos sin **cifrar**. Si la ciframos, y el nombre de la carpeta o documento no es muy atractivo, aunque nos la roben, los 'malos' no perderán el tiempo en un ataque de fuerza bruta contra ficheros que pueden tener muy poco valor. Para los PC podemos usar, por ejemplo, herramientas como Veracrypt [5] para mantener cifradas carpetas o dispositivos. Y en nuestros terminales móviles deberíamos ser muy pulcros con la información que contengan, tanto por la posibilidad de que nos roben la información como el propio dispositivo. Pero sobretodo, lo que debemos tener es **consciencia** de en qué mundo digital nos movemos, y tener mucho **sentido común** en el uso de la tecnología.

Como se decía en una conocida serie policíaca de los años 80, '*Buena suerte, y tengan cuidado ahí afuera*', porque los 'malos' son muy buenos, y los 'buenos' hemos de dejar de ser tan malos en lo que a nuestra propia protección se trata. Nuestra ciberseguridad comienza por nosotros mismos.

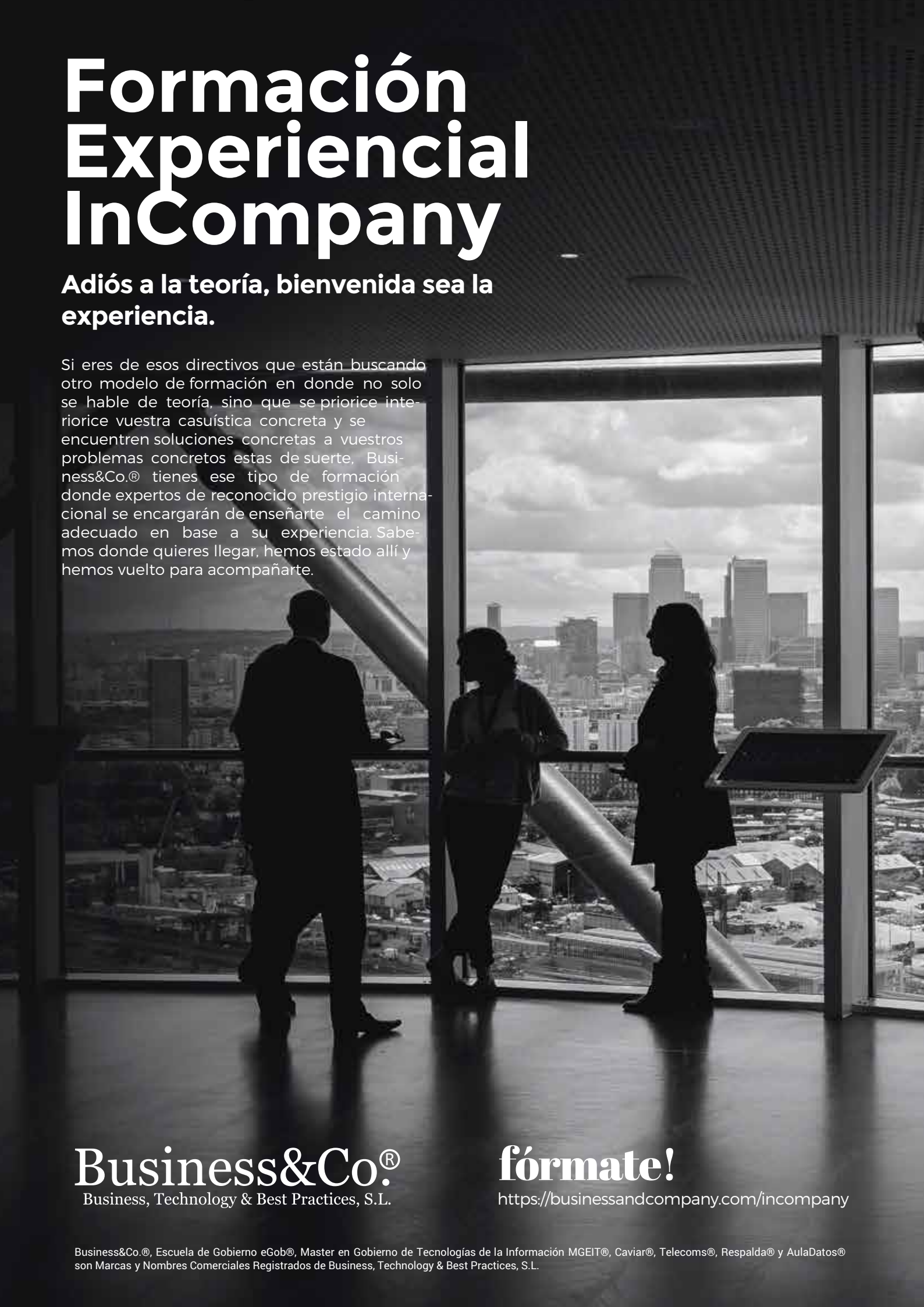
**REFERENCIAS**


**[1]** https://www.elmundo.es/economia/2021/03/09/6047578dfc6c83411b8b4795.html
**[2]** https://www.lasprovincias.es/castellon/ayuntamiento-castellon-sufre-20210401202943-nt.html
**[3]** https://twitter.com/Placi__/status/1381168568641978374
**[4]** https://es.wikipedia.org/wiki/Diarios_de_la_Guerra_de_Afganist%C3%A1n
**[5]** https://www.veracrypt.fr/en/Home.html

# Formación Experiencial InCompany

## Adiós a la teoría, bienvenida sea la experiencia.

Si eres de esos directivos que están buscando otro modelo de formación en donde no solo se hable de teoría, sino que se priorice interiorice vuestra casuística concreta y se encuentren soluciones concretas a vuestros problemas concretos estas de suerte, Business&Co.® tienes ese tipo de formación donde expertos de reconocido prestigio internacional se encargarán de enseñarte el camino adecuado en base a su experiencia. Sabemos donde quieres llegar, hemos estado allí y hemos vuelto para acompañarte.



Business&Co.®
Business, Technology & Best Practices, S.L.

fórmate!
https://businessandcompany.com/incompany

# Entendiendo Tor, el Anonimato y la Deep Web

**Tal vez el lector no sepa que menos de la mitad de los contenidos de Internet son 'visibles' usando las herramientas 'habituales', tales como un navegador web, un buscador como Google o una aplicación móvil. Sin embargo, existe toda una panoplia de servicios y contenidos que son invisibles a la inmensa mayoría de usuarios de Internet, en los que el anonimato y la ofuscación son conceptos clave. Conceptos que, por qué no decirlo, inducen a pensar en la comisión de actividades ilegales de todo tipo.**

Un cuchillo ¿es un arma o un utensilio de cocina? Un opiáceo ¿es perjudicial o beneficioso? El anonimato, ¿es bueno o malo? La respuesta a todas estas preguntas sólo puede ser una: "Depende (de para qué se use, en estos casos)". El anonimato permite actividades no sólo legítimas, sino incluso pertinentes y beneficiosas, como la lucha contra regímenes totalitarios, o la denuncia de actividades ilegales.

En Internet, el anonimato ha formado parte de la Red desde el inicio de su popularización, aunque con el advenimiento de los grandes oligopolios tecnológicos, la comercialización de todo tipo de datos de los usuarios de los diferentes servicios, y las redes sociales, el anonimato y la privacidad brillan por su ausencia. Aunque nuestra navegación pueda parecer anónima, es bastante simple para los agentes que operan las redes y servicios llegar a perfilar a sus usuarios, en incluso trazarlos perfectamente.

De ahí que a principios del siglo XXI, y como evolución de un proyecto de navegación segura de la Marina estadounidense, un grupo de investigadores crearon The Onion Router (TOR), que al poco tiempo fue patrocinado por la Electronic Frontier Foundation [1], una organización que lucha por los derechos digitales de los ciudadanos y contra la vigilancia electrónica masiva e indiscriminada. Gracias a este proyecto, se ha podido desplegar una red mundial de equipos que, conectados a Internet, permite el encaminamiento seguro y anónimo de información, de forma que no sea posible trazar a los usuarios de dicha red por parte de (en principio) gobiernos que no respeten los derechos humanos o la legalidad internacional.

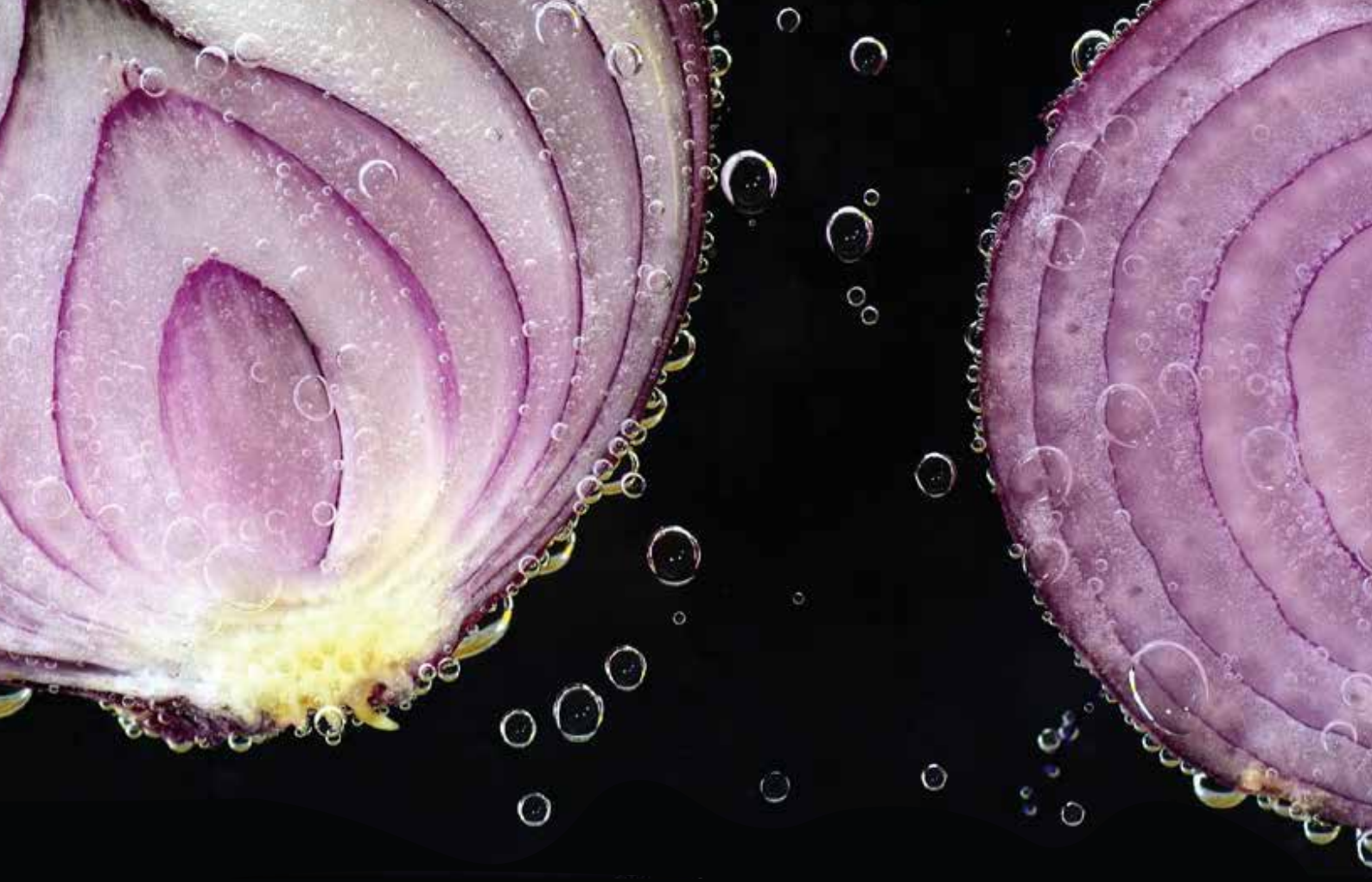
El funcionamiento de esta red es conceptualmente simple: cuando un usuario de la misma, utilizando el software TOR Browser [2], introduce una dirección de Internet, el software no encamina la solicitud directamente hacia el destino, sino que lo hace hacia uno de los routers de entrada de la red TOR, que tras tres o cuatro saltos por otros routers de la misma, acaba cursando la petición por el router de salida hacia el sistema de destino. Y esto ocurre con cada paquete que se envía, por lo que las peticiones de un mismo usuario pueden llegar al destino desde múltiples puntos de salida de la red TOR, impidiendo la trazabilidad del usuario original.

Igual que puede encaminar tráfico hacia destinos de Internet, el navegador TOR permite el acceso a direcciones cuyo dominio de nivel superior es ".onion", y que obviamente son internas de la propia red TOR. Al no existir un servicio en dicha red equivalente al DNS de Internet, los servicios de la red TOR permanecen ocultos, salvo que se conozca la URL que se quiere visitar. Hay, sin embargo, algunos lugares habituales a los que se recurre para localizar determinados servicios en el interior de la red TOR, el más conocido de los cuales es The Hidden Wiki, una especie de directorio de servicios que suele ser parada obligatoria de los usuarios noveles de esos servicios.

En el interior de la red TOR podemos encontrar accesos a Wikileaks, la web de la organización periodística que lideraba Julian Assange; proveedores de correo electrónico anónimo, como ProtonMail o RiseUp; diferentes web de denuncia de actividades de fraude y corrupción, tales como Globaleaks; o las de algunas organizaciones de lucha por los derechos digitales, como la francesa Le quadrature du Net.

Pero como no podía ser de otro modo, las características a priori positivas de esta red han sido aprovechadas por todo tipo de individuos y organizaciones para actividades ilegales, entre las que destacan la venta de drogas, de armas, de documentos o billetes falsificados, el intercambio de criptomonedas o bienes sujetos a propiedad intelectual, el acceso a pornografía infantil, la venta de datos exfiltrados mediante ataques a sistemas corporativos y personales, o, más recientemente, la venta de servicios de Ransomware-as-a-Service, fenómeno que merecería un artículo aparte.

**CONTINÚA EN PRÓXIMA PÁGINA**



A esta parte de la red TOR se la conoce como 'deep web' o 'dark web', y pronto captó la atención de las fuerzas del orden. En 2013, el FBI detuvo a Ross Ulbritch, creador del más conocido mercado negro de la Deep Web, conocido como Silk Road [3], y que finalmente fue condenado a cadena perpetua por tráfico de drogas, blanqueo de capitales y delitos informáticos. En sólo dos años, se calcula que amasó una fortuna de 1.200 millones de dólares en criptomonedas, que al igual que el tráfico de la red TOR, se suponen intrazables. Curiosamente, hasta el año 2020 había un monedero de bitcoin con más de 1.000 millones de dólares que no había registrado movimientos en varios años y que era blanco de todo tipo de intentos de desbloqueo para su vaciado, y que se presumía que era de Silk Road.

La existencia de este tipo de servicios en el interior de la red TOR y de otras redes anónimas, como Freenet e I2P ¿justifica eliminar el anonimato en la Red? La respuesta no puede ser otra que NO. Sin embargo, es necesario poder combatir ciertas actividades en estas redes, manteniendo aquellas que, como hemos dicho al inicio de este artículo, son perfectamente legítimas para la lucha contra gobiernos que no respetan del Derechos Humanos o contra redes políticas corruptas, permitiendo a los activistas su comunicación mientras se protege su identidad.

**REFERENCIAS:**

[1] https://www.eff.org/
[2] https://www.torproject.org/es/download/
[3]https://www.cbsnews.com/news/ross-ulbricht-dread-pirate-roberts-silk-road-fbi/

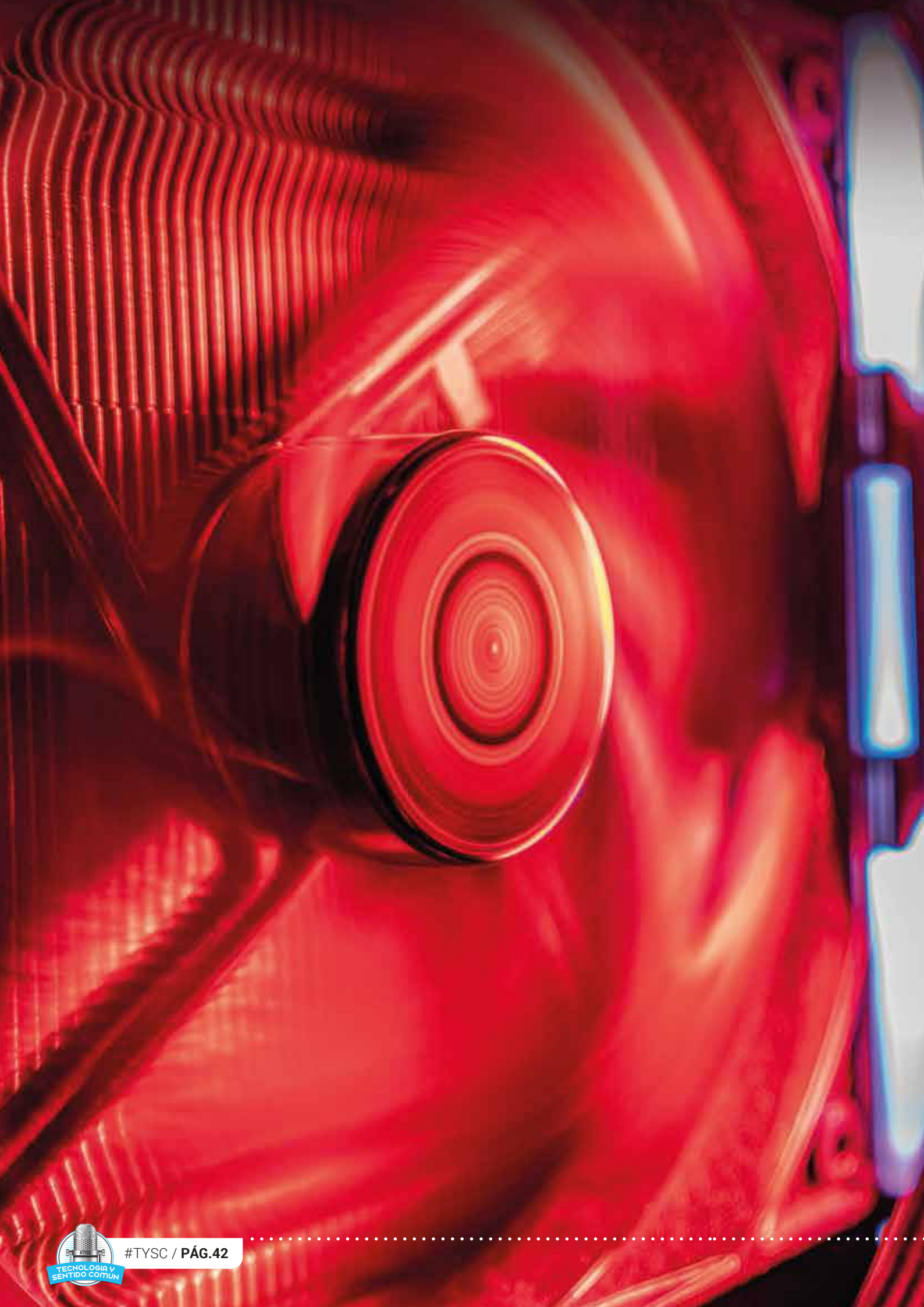
fórmate!
https://businessandcompany.com/itil

# El Sistema de Valor del Servicio de ITIL®4

## ...o todavía andas pensando en el ciclo de vida del Servicio.

Business&Co.®
Business, Technology & Best Practices, S.L.

ITIL®
ACCREDITED TRAINING ORGANIZATION
PeopleCert ON BEHALF OF AXELOS



# Retos del futuro ante la computación y comunicación cuántica

Desde hace unos pocos años, se libra un carrera silenciosa pero trascendental entre ciertos países para lograr la supremacía cuántica. Las grandes potencias políticas y económicas del globo están dedicando muchos esfuerzos a lograr computadores cuánticos cada vez más potentes y fáciles de construir y mantener. ¿A qué viene tanto interés en esta tecnología de computación? Es muy fácil de entender: porque es capaz de resolver en segundos problemas de cálculo que en un computador digital tardarían siglos en resolverse.

En octubre de 2019, la revista Nature publicaba un artículo sobre la supremacía cuántica[1], cuyos autores pertenecían al equipo Google AI Quantum Team. En dicho artículo, los investigadores explicaban cómo habían construido un procesador cuántico de 53 qubits (bits cuánticos, creados con partículas subatómicas) , capaz de realizar un determinado cálculo en 200 segundos, cálculo que en un supercomputador digital tardaría 100.000 años. Sin embargo, no se trataba de un procesador de propósito general, capaz de ejecutar cualquier algoritmo, sino que se había construido ad hoc para un algoritmo concreto. En todo caso, era una increíble mejora de velocidad. Actualmente, solo un par de años después, ya hay investigadores que han logrado construir computadores de 128 qubits.

La conocida como computación cuántica se basa en las características casi mágicas de la mecánica cuántica, y dio sus primeros pasos a principios de los 80 gracias a las propuestas del conocido físico Richard Feynman. Aunque se manejan complejos conceptos de la Física, hay determinados efectos de la mecánica cuántica que resultan interesantes [2]:

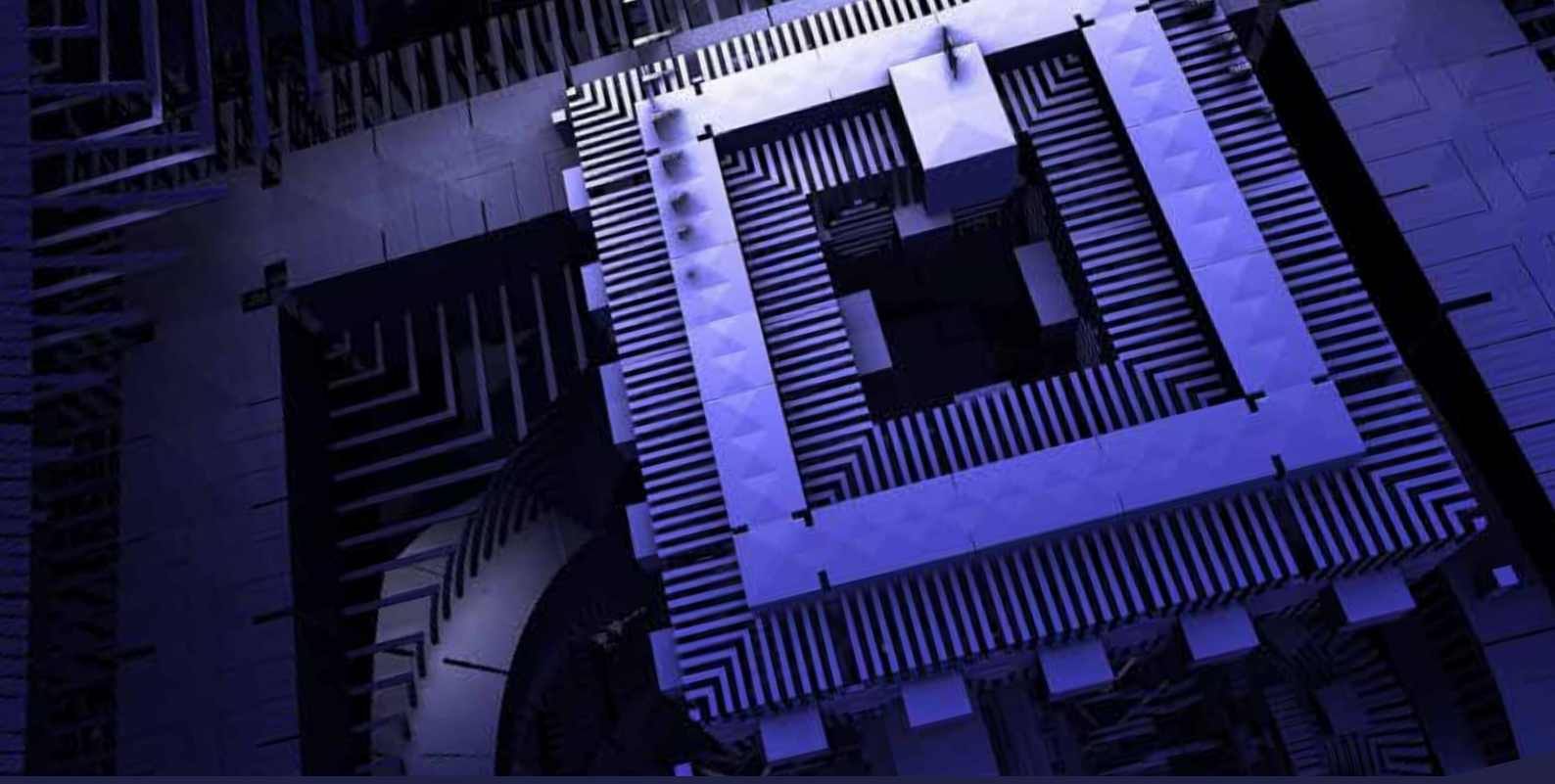
• **SUPERPOSICIÓN CUÁNTICA:** es la capacidad de los qubits de estar en varios estados al mismo tiempo, al contrario que los bits, que sólo pueden estar en estado uno o cero. ¿Le suena al lector la famosa cuestión del gato de Schrödinger? Es una de las formas más gráficas de explicar este fenómeno, y se basa en que hay un gato encerrado en una caja. La Física Clásica dice que estará vivo o muerto. Sin embargo, la Física Cuántica dice que está vivo y muerto a la vez, y que sólo al abrir la caja se situará en uno de los dos estados posibles.

• **ENTRELAZAMIENTO CUÁNTICO:** es posible generar pares de qubits que se encuentran entrelazados, de forma que aunque estén separados por una larga distancia, si cambia el estado de un qubit del par, el otro cambia al mismo estado. El porqué de este efecto es aún un misterio. Junto a la superposición, éste es el fenómeno que permite a los computadores cuánticos realizar más cálculos en menos tiempo, aumentando su potencia de cálculo exponencialmente. Además, merced a este efecto ya existen sistemas cuánticos de comunicaciones que no pueden ser intervenidos por un agente externo.

• **INCOHERENCIA CUÁNTICA:** cualquier pequeña modificación de las condiciones en las que se encuentra un qubit puede hacer que varíe su comportamiento cuántico, decayendo de su estado de superposición, por lo que los computadores cuánticos han de estar en un entorno muy controlado para que sus cálculos resulten fiables.

Estamos hablando de computadores aún en investigación, basados en conceptos parcialmente inexplicables, con unos costes de construcción y mantenimiento importantes, y con una importante dificultad en su programación. Son computadores que se han de mantener a temperaturas cercanas al cero absoluto, y que podrían ser utilizados para importantes avances científicos en campos como la genética, la meteorología o la investigación de medicamentos.

CONTINÚA EN PRÓXIMA PÁGINA



La tecnología cuántica puede suponer, a su vez un interesante campo de desarrollo económico, en el que empresas, universidades y centros de investigación puedan obtener interesantes resultados, para lo cual se han constituido asociaciones como la Quantum World Association[3], en cuya directiva hay varios destacados miembros españoles del ámbito de la computación cuántica, por cierto.

Pero no sólo de negocio se debe hablar cuando se trata de computación cuántica, sino también de los **usos éticos** de la misma, sobretodo, en conjunción con la inteligencia artificial. Y ello es debido a que el hecho de que esta tecnología esté disponible pone en el punto de mira a determinados elementos de la computación digital a la que estamos acostumbrado, sobretodo, a todas aquellas cuestiones que tengan que ver con el cifrado/descifrado de comunicaciones o de datos almacenados en soportes digitales.

Imagine el lector un documento cifrado con una contraseña. Cuanto más larga y compleja sea la contraseña, más tiempo tardará en poder ejecutarse con éxito un ataque de fuerza bruta, basado en probar todas las contraseñas posibles contra el sistema de verificación, hasta que se obtiene el descifrado del documento. Como se puede deducir, es sólo una cuestión de tiempo y de potencia de cálculo descubrir esa contraseña. Si con un supercomputador digital clásico hicieran falta, por ejemplo, 100 años para probar todas las contraseñas, es probable que con un computador cuántico la cosa se resolviese en segundos. Algo similar ocurre con los sistemas de cifrado asimétrico, en los que se basan ampliamente muchos mecanismos de seguridad de transacciones, como por ejemplo, las firmas digitales o el tráfico cifrado SSL de los servidores web. Sería sólo una cuestión de tiempo y potencia de cálculo violentar el cifrado de esos sistemas con un computador cuántico adecuadamente programado. De hecho, se estima que un ordenador de 20 millones de qubits sería capaz de descifrar un sistema RSA con una calve de 2.048 bits en sólo 8 horas.
Por tanto, son muchos los retos que afronta la seguridad de los sistemas de información ante la irrupción de los computadores cuánticos, sobretodo, cuando comiencen a ser asequibles, algo que ocurrirá seguramente en menos de una década. Y no es que ahora no lo sean para determinados *players* globales, como las grandes tecnológicas o los gobiernos de USA, China y otros, que están invirtiendo ingentes cantidades de dinero en su investigación, desarrollo y evolución. ¿Y si alguno de estos players está almacenando todo lo que ahora circula cifrado por Internet, para tratar de descifrarlo en cuanto sus sistemas cuánticos lo permitan?

De ahí que emerjan nuevas necesidades, como la de la **criptografía postcuántica** [4], tópico en el que desde 2016 está trabajando el NIST de USA con diferentes enfoques, aunque hasta la fecha no se han publicado conclusiones del mismo más allá de haber reducido las propuestas recibidas a 26. El impacto de esta cuestión es enorme, dado lo que se ha tardado en el pasado en sustituir un sistema de cifrado considerado vulnerable, como DES, por sistemas más adecuados a la realidad computacional del momento. El problema es que ahora mismo hay muchos más datos, computadores y sistemas de cifrado que en el pasado, por lo que el volumen del problema de volver a cifrar todo lo almacenado o de cambiar los protocolos seguros de comunicaciones digitales en miles de millones de dispositivos y servicios, es mucho mayor, y se convertirá en apremiante conforme la computación cuántica avance.

**REFERENCIAS**


[1] https://www.nature.com/articles/s41586-019-1666-5
[2] https://hardzone.es/reportajes/que-es/ordenador-cuantico/
[3] http://quantumwa.org/
[4] https://www.technologyreview.es/s/11310/que-es-la-criptografia-poscuantica-y-por-que-se-volvera-impresdincible

#BestPractices #BetterProfessionals

# Cursos oficiales de Certificación

## septiembre

GOBIERNO I&T

### COBIT® 2019 FUNDAMENTOS

**PRIMERA SESIÓN:**
Viernes 3 de Septiembre de 2021 de 16:00 a 21:00 horas

**SEGUNDA SESIÓN:**
Sábado 4 de Septiembre de 2021 de 09:00 a 14:00 horas

**TERCERA SESIÓN:**
Viernes 10 de Septiembre de 2021 de 16:00 a 21:00 horas

**CUARTA SESIÓN:**
Sábado 11 de Septiembre de 2021 de 09:00 a 14:00 horas

GESTIÓN DE SERVICIOS

### ITIL® 4 FUNDAMENTOS

**PRIMERA SESIÓN:**
Martes 7 de Septiembre de 2021 de 16:00 a 21:00 horas

**SEGUNDA SESIÓN:**
Jueves 9 de Septiembre de 2021 de 16:00 a 21:00 horas

**TERCERA SESIÓN:**
Martes 14 de Septiembre de 2021 de 16:00 a 21:00 horas

**CUARTA SESIÓN**
Jueves 16 de Septiembre de 2021 de 16:00 a 21:00 horas

GESTIÓN POR PROCESOS

### BPM PROFESIONAL ISO/IEC 19510

**PRIMERA SESIÓN:**
Viernes 17 de Septiembre de 2021 de 16:00 a 21:00 horas

**SEGUNDA SESIÓN:**
Sábado 18 de Septiembre de 2021 de 09:00 a 14:00 horas

**TERCERA SESIÓN:**
Viernes 24 de Septiembre de 2021 de 16:00 a 21:00 horas

**CUARTA SESIÓN**
Sábado 25 de Septiembre de 2021 de 09:00 a 14:00 horas

GESTIÓN DE SERVICIOS

### ITIL® 4 STRATEGIST: DIRECT, PLAN & IMPROVE

**PRIMERA SESIÓN:**
Martes 21 de Septiembre de 2021 de 16:00 a 21:00 horas

**SEGUNDA SESIÓN:**
Jueves 23 de Septiembre de 2021 de 16:00 a 21:00 horas

**TERCERA SESIÓN:**
Martes 28 de Septiembre de 2021 de 16:00 a 21:00 horas

**CUARTA SESIÓN**
Jueves 30 de Septiembre de 2021 de 16:00 a 21:00 horas

## octubre

GESTIÓN DE SERVICIOS

### ITIL® 4 FUNDAMENTOS

**PRIMERA SESIÓN:**
Viernes 1 de Octubre de 2021 de 16:00 a 21:00 horas

**SEGUNDA SESIÓN:**
Sábado 2 de Octubre de 2021 de 09:00 a 14:00 horas

**TERCERA SESIÓN:**
Viernes 8 de Octubre de 2021 de 16:00 a 21:00 horas

**CUARTA SESIÓN**
Sábado 9 de Octubre de 2021 de 09:00 a 14:00 horas

GOBIERNO I&T

### COBIT® 2019 FUNDAMENTOS + ISO 38500 PROFESIONAL

**PRIMERA SESIÓN:**
Martes 5 de Octubre de 2021 de 16:00 a 21:00 horas

**SEGUNDA SESIÓN:**
Jueves 7 de Octubre de 2021 de 16:00 a 21:00 horas

**TERCERA SESIÓN:**
Martes 12 de Octubre de 2021 de 16:00 a 21:00 horas

**CUARTA SESIÓN:**
ISO/IEC 38500 a elegir por el Alumno.

GESTIÓN DE PROYECTOS

### PRINCE2® FUNDAMENTOS

**PRIMERA SESIÓN:**
Viernes 15 de Octubre de 2021 de 16:00 a 21:00 horas

**SEGUNDA SESIÓN:**
Sábado 16 de Octubre de 2021 de 09:00 a 14:00 horas

**TERCERA SESIÓN:**
Viernes 22 de Octubre de 2021 de 16:00 a 21:00 horas

**CUARTA SESIÓN:**
Sábado 23 de Octubre de 2021 de 09:00 a 14:00 horas

GESTIÓN OFICINAS DE PROYECTOS

### P3O® FUNDAMENTOS

**PRIMERA SESIÓN:**
Martes 19 de Octubre de 2021 de 16:00 a 21:00 horas

**SEGUNDA SESIÓN:**
Jueves 21 de Octubre de 2021 de 16:00 a 21:00 horas

**TERCERA SESIÓN:**
Martes 26 de Octubre de 2021 de 16:00 a 21:00 horas

**CUARTA SESIÓN:**
Jueves 28 de Octubre de 2021 de 16:00 a 21:00 horas

Business&Co®
Business, Technology & Best Practices, S.L.

**Más información en**
https://javierperis.com/formacion-oficial/