

ESPECIAL “Futuro y Seguridad”

DE Tecnología & Sentido Común



ESPECIAL

AGOSTO
2025

Inteligencia Artificial
¿Responsable,
gestionada y
gobernada?

08

Resiliencia
organizacional
versus
40 kilobytes

12

La desprotección
de la cadena de
suministro:
un ejemplo
práctico

16

Análisis de riesgos,
resiliencia y toma
de decisiones

20

Qué esperar de
las ciberamenazas
para 2025

24

La ciberseguridad
de los vehículos
conectados (II)

28

Crisis de
ciberseguridad:
¿está su
organización
preparada?

32

Robos de
información:
¿evaluamos
bien su impacto?

36

Estamos
protegidos,
seguro

40

Vivir sin acceso
al Oráculo de
Delfos: medir
para proteger

44

Retos para
el uso
corporativo de
la Inteligencia
Artificial

48

“Futuro y Seguridad”

ESPECIAL

DE Tecnología & Sentido Común



EQUIPO TYSC

Javier Peris - El Gubernauta

Manuel Serrat - Futuro y Seguridad

Nacho Alamillo - Tecnoregulación en Prospectiva

Juan Carlos Muria - Diario de una Tortuga Ninja

Marlon Molina - Es Tendencia

Ricard Martínez - Ojo Al Dato

Marcos Navarro - Ai Futuro

Víctor Almonacid - La Nueva Administración

Alex Aliaga - Radio Security

Marta Martín - Mentes Divergentes

PUBLICIDAD Y CONTRATACIÓN

Carmen Usagre

carmen.usagre@businessandcompany.com

Teléfono: +34 96 109 44 44

GABINETE JURÍDICO

Jesús López Peláz

ATENCIÓN AL LECTOR

soluciones@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://tecnologiaysentidocomun.com>

soluciones@businessandcompany.com



MANUEL SERRAT OLMOS

Doctor en Informática por la Universitat Politècnica de València y Master en Dirección TIC de la UPM-INAP, dispone de varias certificaciones internacionales en Operación, Gestión y Gobierno de TI, tales como ITIL, FITSM, PRINCE2 y COBIT. Escritor técnico, ha sido profesor asociado en varias universidades y actualmente coordina el servicio de TI de una organización pública.

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

Twitter: <https://twitter.com/mdserratt>

(Business&Co.®) Business, Technology & Best Practices, S.L. en ningún caso y bajo ningún supuesto se hace responsable de las opiniones aquí expresadas por sus colaboradores o entrevistados.

Business&Co.®, Escuela de Gobierno eGob®, Master en Gobierno de Tecnologías de la Información MGEIT®, Caviar®, Telecoms®, Respalda® y AulaDatos® son Marcas y Nombres Comerciales Registrados de Business, Technology & Best Practices, S.L. "COBIT® es una Marca Registrada de ISACA.

ISSN 2951-8180

**La Escuela de Gobierno eGob®
Certifica su Sistema de Gestión
de Organizaciones Educativas
con la Norma ISO 21001**

Alcance: Formación Certificada y Programas Directivos para Alta Dirección,
Mandos Intermedios y Responsables de la Ejecución Estratégica
y el Cambio Organizacional en Organizaciones Públicas y Privadas



ESPECIAL
AGOSTO
2025



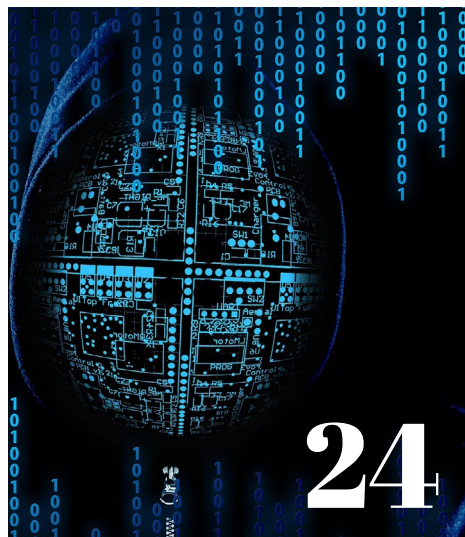
índice

DE CONTENIDOS

<https://tecnologiaysentidocomun.com>



**La desprotección de la
cadena de suministro:
un ejemplo práctico**



**Qué esperar
de las ciberamenazas
para 2025**



**Robos de información:
¿evaluamos bien
su impacto?**



**Vivir sin acceso al
Oráculo de Delfos:
medir para proteger**

Copyright

02

Índice de Contenidos

04

**Este mes te
recomiendo leer...**

por JAVIER PERIS

07

**Inteligencia
Artificial
¿Responsable,
gestionada y
gobernada?**

08

**Resiliencia
organizacional
versus 40 kilobytes**

12

**La desprotección
de la cadena de
suministro; un
ejemplo práctico**

16

**Análisis de riesgos,
resiliencia y toma
de decisiones**

20

**Qué esperar de
las ciberamenazas
para 2025**

24

**La ciberseguridad
de los vehículos
conectados (II)**

28

**Crisis de
ciberseguridad:
¿está su organización
preparada?**

32

**Robos de información:
¿evaluamos bien
su impacto?**

36

**Estamos
protegidos,
seguro**

40

**Vivir sin acceso al
Oráculo de Delfos:
medir para proteger**

44

**Retos para el uso
corporativo de la
Inteligencia Artificial**

48

**Cierre de
Temporada 2025
Revistas “Tecnología
y Sentido Común” y
“Stakeholders.news”**

52

**UNE presenta
su Estrategia 2030
para lograr un
mayor impacto
de las normas
en la sociedad**

68

Índice

#TYSC

Premios recibidos



Premio 2016 a la Difusión de los Valores de la Gestión y Gobierno TI



El Foro de Profesionales de la Gestión del Servicio en España itSMF otorga a «Tecnología y Sentido Común» el Galardón 2016 a la Difusión de los Valores de la Gestión y Gobierno de Tecnologías de la Información.

itSMF
ESPAÑA

Premio 2022 ESET al Periodismo y Divulgación en Seguridad Informática



VI Premios ESET Periodismo y Divulgación: Tecnología y Sentido Común Premiada en la Categoría Blogs por el Artículo de Ricard Martínez "Seguridad en el Smartphone".

Los Premios ESET apuestan por la educación y la concienciación de la sociedad en materia de ciberseguridad, y los medios de comunicación son esenciales en este cometido.

Los periodistas y divulgadores son fundamentales para difundir el conocimiento necesario que permita a los usuarios disfrutar de la tecnología de una manera más segura.

Estos VI Premios ESET pretenden fomentar la divulgación de la ciberseguridad.



Premio Medio de Comunicación 2018 de la Asociación Profesional Española de Privacidad



La Junta Directiva de la Asociación Profesional Española de Privacidad APEP celebrado en Madrid otorga el Premio Medio de Comunicación 2018 a Tecnología y Sentido Común #TYSC



Agradecimiento de la Asociación Valenciana de Informática Sanitaria AVISA



La Asociación Valenciana de Informática Sanitaria AVISA durante las XIV Jornadas Técnicas que bajo el título "20 Años Implantando TIC en Sanidad" se celebraron en Benidorm en febrero de 2024 hizo entrega de su agradecimiento a Tecnología y Sentido Común por su apoyo y visibilidad a la profesión.



Tecnología y Sentido Común "Premio Sapiens" Medio de Comunicación 2022



El Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana entregó el Premio Sapiens Medio de Comunicación 2022 a nuestra Revista "Tecnología y Sentido Común #TYC". El Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana COIICV alabó tanto la gran labor de difusión que viene realizando Tecnología y Sentido Común desde hace siete temporadas como su capacidad de adaptación y resiliencia adaptándose a nuevos formatos con los que continuar en su labor de evangelización en Buenas Prácticas al conjunto de los profesionales a pesar de la alerta sanitaria con nuevos formatos que partiendo de un programa de Radio y Podcast han permitido seguir llevando su mensajes a través de la Revista Mensual, o el informativo televisivo "El Semanal" de Tecnología y Sentido Común.



Gobierno del Tiempo y Gestión de la Productividad con Time Slot Governance TSG4®



Gobierno del Tiempo y Gestión de la Productividad con TSG4 White Belt

Javier Peris

Tras más de veinte años en las trincheras del gobierno TI y el Cambio organizacional, he visto a demasiados profesionales brillantes ahogarse. Vivimos encadenados a las notificaciones, luchando contra un torbellino de urgencias que devora nuestra capacidad para el trabajo profundo. Creemos que el *burnout* es el precio del éxito.

He escrito “**Gobierno del Tiempo y Gestión de la Productividad TSG4 White Belt**” porque estoy convencido de que estamos equivocados y quiero demostrártelo.

Te aseguro que no es otro método de productividad; es un manifiesto para una verdadera revolución personal.

Con este libro “**Gobierno del Tiempo y Gestión de la Productividad TSG4 White Belt**”, mi objetivo es darte la dosis fundamental de

conocimientos que no sabías que necesitabas. En él, disecciono la enfermedad de nuestra era: el “Lingchi Temporal”, esa muerte por mil cortes de interrupciones que aniquila nuestro foco.

Este primer libro es un llamado a las armas. Te obliga a abandonar el rol de “Gestor eficiente del caos” para asumir tu verdadero poder y responsabilidad como “Gobernador de tu tiempo”. No ofrezco herramientas, sino algo mucho más valioso: un cambio de paradigma.

Mi meta es que veas tu semana no como una agenda que se llena, sino como un territorio soberano que debes gobernar.



Inteligencia Artificial

¿Responsable, gestionada y gobernada?

Tenemos a la Inteligencia Artificial hasta en la sopa. IAs que escriben textos, que desarrollan programas, que generan imágenes más o menos realistas, y hasta que son capaces de generar video con una calidad sorprendente. Pero ¿qué hay de sus usos no tan 'productivos'? ¿Y cuáles son los límites que, si se superan, llevan a una IA a ser socialmente perjudicial. Para dar respuesta a estas cuestiones nace el concepto de *Responsible AI* o Inteligencia Artificial Responsable.

No cabe duda de que la Inteligencia Artificial (IA) ha transformado nuestra sociedad de maneras inimaginables hace solo unos pocos años. Recuerdo, cuando yo estudiaba la carrera de Informática, a principios de los años 90, que se hablaba de redes neuronales como algo supercomplejo y avanzado. Hoy en día se puede disfrutar de asistentes virtuales como Siri o Alexa, o de sistemas de diagnóstico médico avanzados, o de sistemas de IA generativa que construyen todo tipo de elementos digitales en base a lo que han aprendido. Incluso este artículo podría estar escrito por una IA. La IA es ya omnipresente. Sin embargo, con su crecimiento y adopción masiva, también ha surgido la necesidad de asegurarnos de que esta tecnología se utilice de manera ética y responsable, por no hablar de las consecuencias medioambientales del consumo eléctrico que los centros de proceso de datos donde se alojan estos sistemas. Y es en este punto donde entra en juego el concepto de **Inteligencia Artificial Responsable**.

Microsoft, propietaria de la empresa OpenAI, creadora de ChatGPT, ha elaborado un interesante documento sobre cómo entiende este concepto de IA Responsable. En dicho documento, se refiere a la IA Responsable como "la creación y uso de sistemas de inteligencia artificial que sean seguros, justos, transparentes y respetuosos con los derechos humanos y las normativas legales". Todo un reto, que obviamente afecta únicamente a las IA 'legales'. Y digo ésto porque no hace mucho tuve acceso a un sistema de IA. orientado a temas de ciberseguridad, en cuyo folleto de características se indicaba como gran ventaja que no estaba sujeta sesgos morales de ningún tipo. Con esa publicidad, queda claro cuál es el interés de sus desarrolladores y el posible nicho de mercado en el que se ubica el producto, alejado del concepto objeto de este artículo.



CONTINÚA EN
PRÓXIMA PÁGINA



Para entender mejor este concepto de Responsible AI, es útil desglosarlo en varios de sus principios clave:

•**Transparencia:** Uno de los principales desafíos de la IA es vencer esa barrera que representa la opacidad de su funcionamiento. Muchos algoritmos, especialmente los de aprendizaje profundo, son verdaderas cajas negras, difíciles de entender incluso para los expertos, y sujetos a férreas patentes de explotación. La transparencia implica que los desarrolladores y usuarios puedan entender cómo y por qué una IA toma determinadas decisiones para generar sus resultados. Y hemos de ir un paso más allá, permitiendo que estas decisiones se puedan explicar de forma que sea comprensible para los usuarios finales del sistema. Algo imprescindible en sectores como el de la salud, donde las decisiones basadas en IA pueden tener consecuencias directas y significativas para la vida de los pacientes.

•**Equidad y No Discriminación:** Los sistemas de IA deben ser diseñados y entrenados para evitar sesgos y discriminaciones. Fácil de decir, pero difícil de implementar y de comprobar, por la sencilla razón de que los propios seres humanos estamos sometidos a esos sesgos a menudo inconscientes. Si una IA se entrena con datos sesgados, los algoritmos que la mueven pueden perpetuar o incluso amplificar esas desigualdades de toda índole. Sin ir más lejos, en la selección de personal, un sistema de IA que se base en datos históricos puede favorecer a ciertos grupos demográficos sobre otros. En consecuencia, es esencial que los desarrolladores de sistemas de IA realicen auditorías independientes de sesgos y pruebas rigurosas para garantizar que sus sistemas sean justos y equitativos.

•**Privacidad y Seguridad:** De todos es conocido que la IA requiere grandes cantidades de datos para obtener resultados de calidad. Si estos datos se corresponden con categorías de datos personales, podemos tener un problema grave. La protección de esta información es crítica, por lo que las empresas que desarrollan sistemas de IA de este tipo han de implementar medidas de seguridad adecuadas para evitar filtraciones y asegurar que los datos de los usuarios se manejen de manera responsable. Además, deben ser transparentes sobre cómo se recopilan, almacenan y utilizan estos datos.

•**Responsabilidad y Gobernanza:** Las organizaciones que desarrollan y despliegan sistemas de IA deben ser responsables de sus creaciones, como no puede ser de otro modo. Esto incluye no solo la supervisión continua de la IA una vez implementada, sino también la predisposición a corregir y compensar cualquier daño causado por decisiones erróneas de la IA y su aplicación en el MundoRealTM. La gobernanza de la IA implica establecer políticas y procedimientos claros para su desarrollo y uso, asegurando que se sigan prácticas éticas en todas las etapas, y

preferentemente, se apliquen estándares de gestión y gobierno de la IA, tales como las ISO/IEC 38507 e ISO/IEC 42001.

•**Impacto Social y Sostenibilidad:** La IA tiene el potencial de causar cambios profundos en la sociedad, tanto positivos como negativos, como ya se está empezando a percibir. Es crucial que las empresas y gobiernos consideren el impacto a largo plazo de sus tecnologías de IA en el empleo, la economía y el medio ambiente. Aunque suene irreal o buenista, sólo se debería fomentar el uso de la IA para el bien común, lo que implica utilizarla para resolver problemas globales como el cambio climático, la pobreza y las enfermedades.

La legislación también debe dar respuesta a estos retos, aunque siempre vaya por detrás de la realidad del mercado o de la tecnología. La esperada aprobación del Reglamento Europeo de Inteligencia Artificial ha de traer un marco legal que obligue a empresas de fuera de la Unión Europea a ajustar sus productos de IA a esos requisitos normativos, aunque sus matrices estén fuera del espacio económico europeo, tal y como ocurrió en su día con el Reglamento Europeo de Protección de Datos. ¿Quiere Ud. vender en Europa? Ajústese a nuestras normas éticas y legales.

A este respecto, también merece la pena resaltar que en España se creó la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA), que con sede en La Coruña, deberá trabajar para garantizar un uso ético y legal de esta tecnología en territorio español, presuntamente garantizando el cumplimiento del Reglamento Europeo de IA.

En conclusión, la Inteligencia Artificial Responsable no es solo una opción, sino una necesidad en el mundo actual. A medida que la IA continúe evolucionando y penetrando en más aspectos de nuestra vida cotidiana, será más y más imperativo que la adoptemos con una mentalidad ética y consciente de los perjuicios y beneficios que aporte. Solo así podremos garantizar que los beneficios de la IA se distribuyan equitativamente y que los riesgos se minimicen, creando un futuro más justo y sostenible para todos.

Pero ¿qué pasa con aquellos sistemas de IA que no sólo no respetan la normativa, sino que abiertamente se usan para la comisión de delitos? ¿Cómo nos enfrentamos a ellos? Porque al final, la IA Responsable sólo liga a aquellos fabricantes de sistemas de IA que quieran mantenerse dentro de la legalidad y de la ética. ¿Veremos 'combates' entre sistemas de IA maliciosos y sistemas de IA que nos defiendan? ¿Veremos esas IA a bordo de sistemas robóticos? ¿Cómo de lejos estamos de la guerra de sistemas IA? El futuro dirá. De momento, ¡bienvenidos a la 10ª temporada de Tecnología y Sentido Común!

P4MGO![®] Essentials

Portfolio, Programme,
Project & Product
Management &
Governance



Resiliencia organizacional versus 40 kilobytes

¿Pueden 40 kilobytes poner en riesgo la continuidad de la sociedad digital? ¿Puede un incidente de seguridad afectar tanto como para que nuestras organizaciones tengan que volver al papel y al bolígrafo? ¿Realmente ese es el nivel de resiliencia digital que nuestra sociedad tiene? El incidente con CrowdStrike del 19 de julio de 2024 nos ha de hacer pensar en si realmente no estamos construyendo una sociedad digital con unos cimientos extremadamente débiles.

Llevamos bastantes años escuchando hablar de transformación digital, digitalización de las organizaciones y de la ciudadanía, de mercados digitales, de comercio electrónico, de criptomonedas, etc. En general, de aquello que bien podríamos llamar Sociedad Digital Global, cuyas bondades glosaban los voceros, donde ríos de leche y miel digital iban a inundarnos a todos.

En muchos de nuestros artículos hemos planteado que a esta Sociedad Digital Global la amenazan los cibercriminales de toda índole y nacionalidad, frente a los que las diferentes jurisdicciones tienen dificultades para actuar, por cuestiones de extraterritorialidad, por ejemplo, o por la dificultad en la atribución de los delitos, o porque se tratan de mafias organizadas, y en ocasiones, esponsorizadas por estados. Por todo ello, la necesidad de una adecuada ciberseguridad ha captado la atención por parte de las empresas, los poderes públicos y los ciudadanos, ignorantes de las amenazas a las que están expuestos, e indefensos en la mayoría de los casos, ante este tipo de actividades criminales, y deseosos de que nada destruya la confianza en los mercados digitales.

Una de las más recientes iniciativas europeas al respecto fue la aprobación, en 2022, de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, conocida popularmente como Directiva NIS2, y cuya transposición al derecho español debería hacerse antes de mediados de

octubre de 2024. El espíritu de esa norma es lograr algo que, en ocasiones, los expertos en ciberseguridad tendemos a obviar, y es el concepto de **ciberresiliencia**, que podríamos definir como *la capacidad de un sistema de información de resistir frente un determinado evento potencialmente catastrófico, aunque sea de forma degradada*. Por la coyuntura actual, se ha tendido a reducir la ciberresiliencia a poder enfrentar ataques de tipo ransomware, virus, intrusiones en los sistemas o ciberestafas, por citar algunos, olvidando otras situaciones que pueden suponer un riesgo para los sistemas de información.

Sin embargo, el pasado 19 de julio de 2024 se produjo un evento que demostró con nítida claridad los problemas de ciberresiliencia que aquejan a esa Sociedad Digital Global, afectando a todo tipo de organizaciones por todo el planeta y paralizando sus operaciones. Y ello, con un simple fichero de 40 kilobytes, puesto en el lugar inadecuado en el momento incorrecto.

Poco después de las 6 de la mañana, hora española, AENA informaba de un fallo en sus sistemas que le impedía operar con normalidad. Se presumió rápidamente un posible ciberataque, pero en un muy breve espacio de tiempo, se desechó la teoría del ciberataque y comenzaron las sospechas de que algún componente de una actualización de algún producto ampliamente utilizado estaba provocando que sistemas basados en Microsoft Windows se reiniciaran continuamente. El primer señalado fue el propio sistema operativo Windows, pero pronto se vio que no era ese el origen del incidente, sino una actualización del producto antivirus Falcon, de la compañía estadounidense CrowdStrike, y que provocaba el reinicio de aquellos sistemas donde las actualizaciones de ese producto estaban configuradas para aplicarse automáticamente.



**CONTINÚA EN
PRÓXIMA PÁGINA**



国际出发
International Departures
港澳/台出发
HK/Macao/Taiwan Departures

国内登机
Domestic Boarding

国际出发
International Departures
港澳/台出发
HK/Macao/Taiwan Departures

国内登机
Domestic Boarding



Los sistemas afectados fueron de todo tipo, y en organizaciones de muy variada naturaleza: compañías aéreas, bancos, hoteles, industrias, etc. Su 'cadena del dolor' quedó meridianamente clara poco antes de las 8 de la mañana, y entonces había que investigar cómo resolverlo con carácter urgente.

Los sistemas basados en otros sistemas operativos, o protegidos con otros antivirus, o simplemente, no teniendo activadas las actualizaciones automáticas de Falcon, no se vieron afectados, salvo quizá por el hecho de que dependiesen de sistemas que sí que hubieran resultado afectados por el incidente.

Aviones en tierra, vuelos cancelados, pasajeros teniendo que ser realojados, facturación aeroportuaria haciéndose con papel y bolígrafo, datáfonos desconectados, y un largo etcétera de efectos provocaron un caos internacional de proporciones desconocidas hasta la fecha. Y todo ello debido a un fichero de 40 kilobytes que no debería estar en la actualización. La situación puso de manifiesto la fragilidad de los sistemas sobre los que se basa la Sociedad Digital Global, y la escasa ciberresiliencia que presenta. No fue un ataque orquestado desde el Eje del Mal. Fue una simple actualización mal hecha sobre un producto masivamente usado en sistemas de alta criticidad.

Alrededor de las 10 horas, ya circulaban ciertas 'recetas' para resolver el problema, y durante el resto del día los administradores de los sistemas afectados se centraron en aplicarlas para devolver a la normalidad las operaciones de las organizaciones afectadas. Pero en el mundo real, las personas acababan de experimentar lo que podría haber sido un evento que marcara el fin de nuestra civilización, si se nos permite la exageración.

Resuelto el problema tecnológico y restaurados los servicios, quedaba sacar las oportunas conclusiones. La más obvia es que nuestra Sociedad Digital Global es un sistema complejísimo, por la interdependencia entre sistemas, y la complejidad intrínseca de muchos de ellos, que unido al hecho de las presiones competitivas, hace que se concentre en un puñado de soluciones la oferta en ciertos nichos de mercado, convirtiendo a esa Sociedad Digital Global en un gigante con los pies de barro, en el que una simple actualización mal hecha provoca cientos, si no miles de millones de dólares de impacto económico a nivel mundial. Coincidirán con nosotros en que lo que es confianza, no da precisamente.

Tras el evento, se produjeron tres situaciones que merece la pena resaltar:

1. Los ciberdelincuentes aprovecharon el evento para lanzar campañas maliciosas, con supuestas soluciones al problema de CrowdStrike, con el efecto final de amplificación del mismo. A río revuelto, ganancia de pescadores.
2. La compañía, tras pedir disculpas en redes sociales a través de su CEO, publicó un informe preliminar oficial sobre el incidente, y planteó compensar a los afectados con un vale de 10 dólares para pedidos en Uber Eats, cuestión que terminó de indignar a quienes directa o indirectamente, se han visto perjudicados por el incidente. Bastantes días después, publicaron un magnífico informe explicando el incidente con detalle.
3. Microsoft cargó la responsabilidad del incidente en las normas antimonopolio de la Unión Europea, que le obligaron a dar acceso al kernel de Windows a diferentes fabricantes de software.

A partir del momento en que se tranquilizó el sector, comenzó un debate que sí resulta realmente interesante, en torno a la pregunta de cómo podemos mejorar esa resiliencia. Una de las lecciones aprendidas del incidente de CrowdStrike es que nuestros servicios han de disponer de redundancia no sólo numérica o geográfica, como es habitual, sino, a ser posible, en cuanto a sus componentes. La otra lección aprendida es que en el sector de la ciberseguridad hemos desdeñado la ciberresiliencia para centrarnos exclusivamente en los ciberataques activos, lo que nos ha llevado a la especialización del personal en ese ámbito, y ha comportado que en algunas organizaciones se hayan priorizado las inversiones en esa faceta y no en otras relacionadas con la resiliencia. Con ello, perdemos de vista una cuestión fundamental: **las organizaciones actuales dependen totalmente de la tecnología, y por tanto, serán tan resilientes como lo sean sus sistemas tecnológicos.** Cabe, por tanto, optar por la ciberresiliencia, que incluye todos aquellos aspectos de la ciberseguridad 'chic', pero que también tiene en cuenta aspectos como la seguridad física, la redundancia de sistemas y la tolerancia a fallos. En caso contrario, éste incidente del 19 de julio de 2024 puede ser sólo el primero, y cada vez los impactos pueden ser mayores.

¿Demasiada Iniciativas?
¿Alineamiento Estratégico Cuestionable?
¿Dificultad para Priorizar?
¿Vision basada en Silos o Islas?
¿Falta de foco estratégico en el valor a largo plazo?



Alienamiento Estratégico de las iniciativas
Priorización Basada en el valor
Optimización de Recursos
Gestión de Riesgos Corporativos
Ejecución Estratégica Efectiva



soluciones@p4mgo.com
<https://p4mgo.com>

La desprotección de la cadena de suministro: un ejemplo práctico

El pasado septiembre el mundo entero se sorprendía por el hecho de que miles de buscapersonas y walkie-talkies del grupo libanés Hezbollah explotaban de forma coordinada, provocando varios muertos y cientos de heridos. Lejos de tratarse de un hecho fortuito, se atribuye a un presunto ataque de los servicios secretos israelíes al grupo yihadista, que ha puesto sobre la mesa la vulnerabilidad de nuestros procesos e infraestructuras a los ataques dirigidos contra la cadena de suministro. En este artículo analizaremos el caso y el por qué proteger dicha cadena está siendo cada vez más imprescindible.

En el número de mayo de 2024 de Tecnología y Sentido común se incluyó un artículo mío, “¿Vulnerabilidad o funcionalidad? Los fallos en el hardware”, en el que explicaba cómo determinados actores de la escena geopolítica mundial tenían capacidades para introducir vulnerabilidades no sólo en el software, sino también en el hardware de nuestros dispositivos electrónicos. Son intervenciones que pueden resultar en un ‘jaque mate’ al

funcionamiento de ciertos sectores de la sociedad o del gobierno, y que se producen en un punto de la cadena de suministros de esos elementos en los que es prácticamente imposible actuar para protegerse.

Precisamente la necesidad de proteger la cadena de suministro de nuestros elementos tecnológicos viene siendo cada vez más patente, y no sólo a nivel de equipos o programas, sino también de servicios. Ha habido casos muy mediáticos de grandes compañías que han sufrido robo de datos debido a que empresas subcontratistas cuyas disponían de acceso o de copias de subconjuntos de datos que han sido robados o utilizados para llevar a cabo accesos no autorizados. También de



CONTINÚA EN
PRÓXIMA PÁGINA



compañías de software de gestión de redes que han visto como en sus actualizaciones a clientes un actor malicioso había conseguido introducir malware, de manera que todos los clientes de la compañía que instalaron dichas actualizaciones vieron como se les instalaba inadvertidamente una puerta trasera en sus sistemas. Y por supuesto, está el caso Crowdstrike, del que versó nuestro artículo para TYSC del mes de octubre.

La teoría es simple, aunque compleja de llevar a cabo: si tengo mis sistemas bien protegidos, he de exigir a aquellos que me suministran software, hardware o servicios, que también los tenga bien protegidos, ya que éstos forman parte de mi cadena de valor, y si un eslabón se ve comprometido, toda la cadena peligra. Como digo, parece de sentido común, pero luego las situaciones son muy variadas, y sobre todo, suele escasear la conciencia sobre las repercusiones de no tomarse en serio esta cuestión de la seguridad. Porque no hablamos sólo de ciberseguridad, sino también de otros tipos de seguridad: en los procesos de negocio, en los accesos físicos, en la contratación de personal, etc.

Y si algo ha venido a demostrar que un adversario motivado y con capacidades de todo tipo puede hacernos morder el polvo ha sido la cadena de explosiones de ciertos dispositivos 'inusuales' que sucedieron a mediados de septiembre de 2024 en el Líbano. Unos tres mil dispositivos en total, entre buscapersonas y walkie-talkies en manos (supuestamente) de milicianos de Hezbollah estallaron de forma coordinada, produciendo cuantiosos daños personales, y sobre todo, morales a la organización yihadista, y por qué no decirlo, a civiles de todo tipo. Este ataque ha sido atribuido a la inteligencia israelí, pero no ha habido ningún tipo de confirmación oficial del acto, como era de esperar, por lo que podemos calificarlo de presunto. Lo curioso es que la organización libanesa parece que había desechado el uso de la telefonía móvil para evitar ser geolocalizados por los servicios de inteligencia israelíes, lo cual es también un indicativo de la ausencia absoluta de privacidad que 'disfrutamos' el común de los mortales por el hecho de usar estos dispositivos de comunicaciones.

La investigación del ataque llevó a la conclusión preliminar de que eran dispositivos falsificados, que no habían sido fabricados en las plantas del fabricante oficial de los productos, sino que habían sido adquiridos a una empresa de Hungría, donde presuntamente se realizó la manipulación de los dispositivos. Es decir, se atacó la cadena de suministro de Hezbollah haciéndoles creer que compraban equipos 'limpios' cuando en realidad eran dispositivos manipulados de una forma casi de película de James Bond. En un primer momento se pensó en una manipulación para

que la batería se calentase y estallase. Sin embargo, rápidamente se constató que se había introducido una pequeña cantidad explosivo en interior de los dispositivos en fábrica, y se había añadido la circuitería necesaria para que al recibir una señal de radiofrecuencia concreta, dicho explosivo estallase.

Es obvio que las capacidades necesarias para que todo este plan funcionase no están al alcance de cualquiera, como ya indiqué en mi artículo del mes de mayo. Y todos los dispositivos electrónicos en manos de cualquier persona con un mínimo de poder deberían ser sospechosos de poder actuar de la misma forma que los que adquirió Hezbollah, porque si (presuntamente) el gobierno de Israel es capaz de hacerlo, imaginen de lo que son capaces los gobiernos de las potencial globales en este ámbito. No creo que ahora mismo ningún servicio de inteligencia de ningún estado esté tranquilo y no esté chequeando los dispositivos de todos los altos cargos de sus respectivos países. No sólo de Pegasus viven los espías....

Hay otra cosa a destacar de este caso. El hecho de que Hezbollah renunciase a funcionalidades de las plataformas de teléfonos inteligentes también debería hacernos reflexionar sobre nuestra exposición y dependencia de los dispositivos de comunicaciones, tanto a nivel profesional como personal, y si estos casos no potencian las posiciones neo-luditas de rechazo a la tecnología, no por sus funcionalidades, sino por las 'esclavitudes' a las que nos someten los oligopolios tecnológicos.

El tercer aspecto a destacar es que, naturalmente, no sólo las infraestructuras de T.I. clásicas sufren ataques, sino que también otros tipos de elementos tecnológicos son susceptibles de ser violentados, como viene mostrando nuestro compañero de TYSC Alejandro Aliaga en sus artículos de cada mes, o como hemos podido ver en conferencias de seguridad por todo el planeta, con robots aspiradores usados como espías por control remoto, o vehículos interceptados y controlados a distancia por actores maliciosos.

A una mente calenturienta se le puede pasar por la cabeza hacer algo similar a lo ocurrido con los buscas con, por ejemplo, smartwatches, auriculares inalámbricos, bombas de insulina, o marcapasos. Cualquier cosa que pueda recibir una señal de radiofrecuencia y tenga espacio para una carga explosiva puede ser la siguiente arma de quien sea que haya llevado a cabo el ataque de septiembre. Pero ¿podemos protegernos de esto a nivel global? ¿Es segura nuestra cadena de suministro?

Piensenlo. ¿Les apetece vivir en un mundo así?

¿Objetivos ambiciosos?
¿Cambios transformadores fallidos?
¿Sinergias desaprovechadas?
¿Foco en entregables y no en beneficios?
¿Iniciativas sin visión de conjunto?



Maximización del Valor
Nuevas Capacidades Organizacionales
Gestión de interdependencias
Gobierno de la Transformación
Consolidación de beneficios



soluciones@p4mgo.com
<https://p4mgo.com>

Análisis de riesgos, resiliencia y toma de decisiones

En nuestro artículo del mes de octubre pasado, nos referíamos a la resiliencia de nuestra Sociedad Digital frente a determinados eventos de índole igualmente digital, en aquel caso, el suceso acaecido con el antivirus CrowdStrike. Sin embargo, con lo ocurrido en España con la DANA del 29 de octubre de 2024, se pone de manifiesto la necesidad de planificar adecuadamente la continuidad de diferentes servicios de nuestra sociedad en caso de catástrofe. Y no sólo desde el punto de vista tecnológico.

Hace unos ocho años tuve una conversación con un responsable TIC de un ayuntamiento acerca de sus medidas de continuidad de negocio, y la respuesta no pudo sino sorprenderme. Su Centro de Proceso de Datos (CPD) principal estaba situado en la planta baja del propio edificio del ayuntamiento, separado de un barranco encauzado por escasos cinco metros. Al preguntarle por si tenían CPD de respaldo y dónde estaba ubicado, me comentó que lo tenían a unos 500 metros de allí, en un edificio de titularidad municipal, situado también lindante al mismo barranco. A mi pregunta sobre si no consideraba eso arriesgado, o si no se había planteado sacarlo de allí, por el riesgo de inundación, la respuesta fue un lacónico “¿Para qué, si esto es un río seco?”. Imaginen que ese ayuntamiento fuese uno de los afectados por la DANA que arrasó la zona sur del área metropolitana de Valencia el pasado 29 de octubre de 2024.

Dicha respuesta denota una manera de gestionar, en este caso las Tecnologías de la Información y las Comunicaciones, basada en la intuición o la "idea feliz", que el Esquema Nacional de Seguridad pretende sustituir por una gestión de la seguridad basada en el análisis y la gestión de riesgos. Un análisis riguroso de los riesgos, y una gestión profesional de los mismos, hubiera aconsejado que el CPD de respaldo de ese ayuntamiento estuviese a una distancia mayor, o incluso, con la tecnología disponible, fuese desplegado en el Cloud. Y ello sería así porque la misma amenaza que hubiera dejado inutilizado el CPD principal, una riada destructiva de ese barranco, hubiera tenido las mismas consecuencias en el secundario.

Pero lamentablemente, seguimos asistiendo a decisiones que se toman, exclusivamente, basadas en creencias o criterios exclusivamente de ahorro a corto plazo, sin pensar en los impactos de que una amenaza se materializase sobre uno o varios activos del sistema de información. Hemos visto ejemplos de este tipo de análisis erróneos en películas como Parque Jurásico, donde un informático descontento deja el sistema en una situación que sin su participación directa no se puede mantener el sistema de seguridad del parque en funcionamiento tras un incidente, y de ahí el desarrollo posterior de los acontecimientos de la película.



**CONTINÚA EN
PRÓXIMA PÁGINA**



Si bien es verdad que el riesgo cero no existe, el trabajo de analizar los riesgos a los que nuestras organizaciones, o nuestros proyectos, están expuestos, y actuar en consecuencia, buscando la opción óptima para afrontarlos, debería ser una materia a tener en cuenta en cualquier programa de educación superior. Cabe recordar que, por ejemplo, en metodologías de gestión de proyectos como PRINCE2 se plantea analizar los riesgos con preguntas simples tales como “¿Qué pasa si no hacemos nada? ¿Y si hacemos sólo una parte? ¿Y si lo hacemos todo?”, que aunque no son un análisis de riesgos muy formal, si que permite que ciertas decisiones estén, al menos, basadas en algún tipo de análisis previo en base a argumentos y dato.

Y quizá de ahí vienen muchos de los problemas con la toma de decisiones, en muchos ámbitos, y es que no se toman en base a datos. Pero en cuestiones que pueden incluso poner en riesgo la continuidad de una organización, ¿no sería lógico que quienes han de tomarlas conozcan al menos la existencia de las diferentes metodologías de análisis y gestión de riesgos en los diferentes ámbitos, y dispongan de la posibilidad, a través de expertos en su caso, de poder obtener una idea clara de los riesgos que se asumen y cómo mitigarlos?

Sin embargo, se suele tildar a quienes advierten de dichos riesgos de exagerados, alarmistas, catastrofistas o, simplemente, de pesimistas. Pero cuando esas advertencias están basadas en métodos estadísticos, científicos o técnicos contrastados, fundamentadas en datos correctos, ignorarlas o dejarlas pasar es, en sí mismo, otro riesgo que habitualmente no se analiza.

Si la seguridad ha de ser un proceso, analizar los riesgos es una parte del mismo, y gestionarlos tomando las decisiones oportunas, también. Fomentar la cultura del análisis de riesgos previo a la toma de decisiones es no es plantear que las decisiones se demoren gratuitamente, ni que no se

puedan tomar decisiones rápidas. Armar un sistema que permita esa toma rápida de decisiones basadas en datos y en un análisis de los riesgos debería ser prioritario en las organizaciones, al menos, en las de determinado tamaño. En el s. XXI, lo contrario ya no es aceptable, y los costes de todo tipo asociados a ese tipo de decisiones tomadas ‘por intuición’ (por decirlo suavemente) pueden ser muy elevados.

Nos encontramos, por tanto, ante dos formas de tomar decisiones: una, basada en datos, tendencias, técnicas estadísticas y/o científicas y opiniones expertas; y otra, basada en creencias, intuiciones y otras cuestiones intangibles y no medibles. ¿Cuál es, o ha sido, la mayoritaria en las organizaciones de nuestro entorno? La segunda.

¿Disponemos de medios tecnológicos para que sea la primera opción la utilizada? Claramente, sí. ¿Por qué no se está haciendo más? ¿Por ignorancia? ¿Por miedo, en aquellos directivos que basan su autoridad en el ‘yo sé más que nadie cómo funciona esto’? ¿Por costes? ¿Porque siempre se ha hecho así, simplemente? Lo cierto es que lo desconocemos, pero sus efectos están a la vista todos los días a nuestro alrededor, con procesos ineficientes, decisiones incorrectas, y recursos desperdiciados.

Y en cuestiones como la seguridad de la información y la tecnología, donde los plazos son escasos, la dificultad de protegerse es elevada, y los posibles daños recibidos pueden ser grandes, es pertinente contar con unos esquemas de toma de decisiones basados no en creencias, sino en datos, en análisis y gestión de riesgos, y en experiencias previas contrastadas.

**En la Escuela de Gobierno eGob®
impartimos Cursos de Doble Certificación
y nos certificamos por partida doble
ISO 9001:2015 + ISO 21001:2018**

Alcance: Formación Certificada y Programas Directivos para Alta Dirección,
Mandos Intermedios y Responsables de la Ejecución Estratégica
y el Cambio Organizacional en Organizaciones Públicas y Privadas



ISO 9001:2015

ISO 21001:2018



Qué esperar de las ciberamenazas para 2025

En este primer artículo del año 2025, y en base a las opiniones de profesionales y empresas de ciberseguridad, daremos una ojeada a las que se supone que van a ser las “tendencias”, en lo que a ciberamenazas se refiere, en este nuevo año. No es que haya grandes novedades, ya que los ciberdelincuentes no son una marca de moda prêt-à-porter, pero sí merece la pena explicar ciertos cambios de tendencia o ciertas novedades en cuanto a su *modus operandi*.

En primer lugar, y pese a la temática de mis artículos, este modesto redactor les desea a todos los lectores de Tecnología y Sentido Común un provechoso y gozoso año 2025, en el que todos nuestros objetivos lleguen a buen término, y que nuestros programas y proyectos finalicen en el plazo, presupuesto, calidad y resultados pactados, y generen los beneficios esperados.

Dicho esto, debo empezar aclarando que este artículo es poco más o menos que un vaticinio o una apuesta por aquello que puede representar el año 2025 en lo que a las amenazas de ciberseguridad se refiere. A estas alturas de año, no podemos asegurar cómo se desarrollará el ejercicio en esta materia, pero sí podemos extrapolar las tendencias que en los últimos meses de 2024 se han visto desde las compañías punteras en la materia. Y de su experiencia se destila este texto, teniendo en cuenta que una de las características que se están confirmando en los últimos años es una cierta especialización geográfica de ciertos tipos de amenazas.

En opinión de empresas como Fortinet o ESET, en 2025 las organizaciones y los ciudadanos nos vamos a tener que enfrentar a amenazas no por ya conocidas, menos peligrosas, ya que la evolución se produce, sobre todo, en las técnicas, tácticas, procedimientos y objetivos de los ciberdelincuentes, más que en la aparición de nuevos tipos de amenazas. Lejos, tecnológicamente hablando, quedan eventos como la aparición del *ransomware*, o el *phishing* indiscriminado por correo electrónico.

Una amenaza que permanece, de ahí su nombre, es el de las APT (**Advanced Persistent Threat**) o Amenazas Persistentes Avanzadas, operadas en su mayoría por grupos de ciberdelincuentes asociados a determinados estados, y cuyas actividades se espera que aumenten en este 2025, ante la situación geopolítica internacional. De hecho, en diciembre se anularon las elecciones presidenciales en Rumanía por la supuesta manipulación que grupos de cibercriminales rusos habían hecho de las mismas, dando la



CONTINÚA EN
PRÓXIMA PÁGINA





victoria en la primera vuelta a un candidato pro-ruso. Al tratarse de grupos bien financiados y con muy buenos resultados en sus operaciones, se espera que en este 2025 mejoren aún más sus capacidades de ataques encubiertos cada vez más personalizados a la organización o sector atacados.

Ya hemos comentado en artículos pasados lo productivos que son ciertos ciberataques y lo especializado que está el mercado negro de productos y servicios de cibercriminalidad. Por esta razón, los grupos de ciberdelincentes pueden disponer de fondos para financiar sus actividades de investigación y desarrollo, orientadas a **mejorar sus técnicas, tácticas y procedimientos (TTPs)**, y que permitan que sus actividades tengan aún más éxito en este año que comienza.

Por supuesto que el avance de los productos de Inteligencia Artificial, y su uso en este ámbito de la ciberdelincuencia, van a suponer un gran reto para los equipos de seguridad. También hemos traído a Tecnología y Sentido Común algún artículo sobre esta cuestión, pero de acuerdo a los expertos podemos esperar en 2025 un incremento en el uso de estas tecnologías para plantear los ataques. En concreto, los ciberdelincentes de todo pelaje van a utilizar la IA para:

- Campañas de desinformación con IA Generativa, para diseminar campañas con información falsa en redes sociales y otros medios.
- *Vishing (voice phishing)*, generando artificialmente la voz de ciertos individuos para engañar a otros.
- Campañas de *phishing* automatizadas, aprovechando la información que se ha obtenido y vendido procedente de los robos de información a ciertas empresas y organismos públicos en los últimos tiempos.

- Mejoras en la creación de *malware*, ya que partiendo de la base de malware existente, se aprovecharán las capacidades de los sistemas de IA Generativa para mejorarlos, hacerlos menos detectables, o más destructivos.

- Creación de perfiles falsos en redes sociales, para apoyar estafas del Mundo Real™. Por ejemplo, el pasado noviembre hubo denuncias en la zona de Iberoamérica por unos perfiles que falseaban la identidad de la Princesa de Asturias, y que se utilizaron para estafar a personas necesitadas.

- Análisis de contraseñas potenciados con IA, a la búsqueda de patrones que permitan a los ciberdelincentes adivinar más fácilmente las contraseñas de diferentes servicios.

Todos estos elementos, además, se pueden lanzar aprovechando eventos de masas, sean positivos o negativos. Por ejemplo, también durante el mes de noviembre de 2024 se localizaron campañas de ciberdelincuencia asociadas a la ayuda a los afectados por las inundaciones provocadas por la DANA que afectó a la provincia de Valencia (España), y se espera que eventos como el Jubileo de Roma 2025 y otros similares se utilicen como 'gancho' en actividades maliciosas.

Si alguna tendencia resulta curiosa es ver como, desde mediados de 2024, la tendencia de los *malware* ha sido la de regresar al borrado de información y/o avería de ciertos componentes *hardware*, como ocurría con los virus de las primeras generaciones (años 90 del siglo XX), ante cierto 'decaimiento' de las técnicas de *ransomware*.

Otras tendencias que van a ver incrementado su porcentaje de utilización van a ser aquellas asociadas a los ataques a servicios en la Nube y, en general, a la **cadena de suministro**, como explicamos en el número de noviembre de esta revista. Por supuesto que el mercado de ciberdelincuencia en la Dark Web va a seguir en auge, y vamos a ver más **ataques de tipo híbrido**, donde las amenazas procedentes del ciberespacio se van a mezclar con ciertas operaciones de proximidad, en los casos donde los ciberdelincentes más beneficio esperen obtener, del tipo que sea.

Por sectores, las grandes 'estrellas' serán el **sector Salud**, donde se producen ataques, mayoritariamente de robo de información de pacientes y secretos industriales, por un lado, y de *ransomware*, por otro; el **sector Financiero**, donde por razones obvias el *ransomware* y las ciberestafas seguirán a la orden del día; el **sector de la Fabricación**, con ataques de *ransomware* a los sistemas tanto IT como OT, a la búsqueda de interrumpir los procesos productivos; y el **sector de las Utilities**, o proveedores de servicios básicos, especialmente del sector de la Energía, tratando también de infligir el mayor daño posible a las empresas o estados atacados, y de generar desconfianza en la ciudadanía.

Como se puede observar, 2025 seguirá la tendencia de ser un año con demasiado trabajo para los profesionales del sector, y en el que, de nuevo, se van a escuchar discursos acerca de la necesidad de la colaboración entre los diferentes actores de la ciberseguridad para evitar, mitigar o responder ante estos ciberataques. Desde aquí, les deseamos la mayor de las suertes, ya que en ello nos va el bienestar a todos.

Gobierno del Tiempo y Gestión de la Productividad con Time Slot Governance TSG4®



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



La ciberseguridad de los vehículos conectados (II)

En el artículo de junio de 2023 de Tecnología y Sentido Común, nos planteábamos una serie de cuestiones relacionadas con la ciber(in)seguridad de los vehículos conectados, con especial preocupación con lo que pudiera ocurrir con los vehículos autónomos cuando se generalizasen. Un año y medio después, es momento de revisitar la cuestión y analizar si se ha producido algún “avance” en la materia.

A estas alturas de partido, ya todos nuestros lectores estarán al cabo de la calle sobre la cuestión básica que transmitimos siempre que podemos: ningún sistema es seguro al 100% y es sólo cuestión de que a los ciberdelincuentes les merezca la pena la inversión en recursos y riesgo para que un sistema sea violentado. Partiendo de esa idea-fuerza, ya transmitimos en el artículo de esta revista de junio de 2023 una serie de preocupaciones acerca de a qué riesgos se podían enfrentar los vehículos conectados, y los autónomos en particular.

En este tiempo, hemos visto como la Inteligencia Artificial Generativa aparecía en nuestras vidas, manifestando de forma muy visible los avances en el campo de la IA para el común de los mortales, avances, que por otro lado, son sólo un tipo de uso de estas tecnologías. Ya hacía bastante tiempo que se estaban usando sistemas de IA en otros ámbitos, como el diagnóstico médico, el análisis y mejora de imágenes, o los sistemas de decisión en diferentes ámbitos, como los mercados bursátiles o la conducción autónoma de vehículos. En este último ámbito, los sistemas de IA para vehículos autónomos no sólo se enfrentaban a las necesidades de funcionamiento en tiempo real y a altas necesidades de computación, sino también al necesario estudio de sus algoritmos de decisión en un marco ético, ya que las vidas de personas estaban en juego en dichas decisiones. Por ejemplo, en el caso de que una persona se cruzase inesperadamente frente al vehículo autónomo, y el accidente fuese inevitable, el

coche deberá decidir en una fracción de segundo si da un volantazo, con el riesgo de que los viajeros del vehículo sufrieran daños o incluso la muerte, dependiendo de las circunstancias del impacto, o si debía reducir todo lo posible la velocidad antes de impactar con la persona que cruza la vía, como mal menor, resultado del análisis de todas las opciones posibles. Y ese mal menor, ¿dependerá de la edad o el sexo del peatón? ¿Será mejor opción el volantazo si quien cruza sin precaución es una mujer embarazada o con un carrito de bebé? ¿Y si es un anciano o un niño?

Observará el lector que existe un evidente riesgo de sesgo en ese algoritmo, por ejemplo, si un desarrollador racista decide (e implementa) que el vehículo tenga en cuenta la raza del peatón para tomar la decisión. O si un fabricante sin escrúpulos dirige el algoritmo hacia decisiones que provoquen daños al vehículo que le reporten más beneficios en su reparación. De ahí la necesidad de que los algoritmos de la IA deban ser analizados desde un punto de vista ético por entidades externas y, a ser posible, públicas, y que la IA tenga una regulación importante para evitar abusos y desmanes varios.

Además de los riesgos que la IA aporta al vehículo autónomo, como sistema de computación y comunicaciones, el vehículo inteligente, sea autónomo o no, está sujeto a los mismos tipos de amenazas que los sistemas IT (Information Technology) y OT (Operational Technology), y especialmente en este último ámbito, hay riesgos específicos en ataques de Denegación de Servicio o de interceptación/manipulación de las órdenes de navegación.



CONTINÚA EN
PRÓXIMA PÁGINA





En este tiempo, se han identificado ataques a los sistemas de GPS de buques mercantes, con el supuesto objetivo de desviarlos de las rutas habituales y facilitar su asalto por piratas en el Océano Índico, por ejemplo. A nadie le apetecerá subirse a su coche autónomo si un malhechor es capaz, de forma remota, de controlar el destino del mismo y llevar a sus ocupantes a una zona en la que dicho malhechor pueda tenerlos a su merced.

Dicho todo esto, como resumen o actualización de los ya advertido en nuestro artículo de junio de 2023, merece la pena destacar que las autoridades competentes están tratando de poner coto a estas amenazas, y no puede ser de otro modo que mediante la oportuna legislación para los fabricantes de coches inteligentes. Y en este ámbito el Instituto Nacional de Ciberseguridad de España (INCIBE) publicó una interesante guía el pasado mes de junio, titulada “Nuevas normativas de 2024 de ciberseguridad para vehículos”, y en la que se repasan las iniciativas a este respecto, y cómo afectan a la fabricación de las nuevas generaciones de vehículos.

En el primer párrafo del documento queda meridianamente claro su objetivo: *“El objetivo de esta guía es proporcionar información que ayude a entender la nueva regulación emitida por el Foro mundial para la armonización de la reglamentación sobre vehículos (WP.29), un cuerpo de la Comisión Económica de las Naciones Unidas para Europa (UNECE), referida a la ciberseguridad en vehículos, así como la presentación de consejos que ayuden a su cumplimiento”*.

No es un documento normativo, si no informativo, que ayude a facilitar a los fabricantes el entendimiento sobre el proceso de homologación requerido para la fabricación y comercialización de vehículos en Europa. En concreto, respecto de los reglamentos UN R155, que *“conciernen a los requisitos para la gestión de la ciberseguridad”* en los vehículos, y UN R156, que *“estipula los requisitos para la gestión de actualizaciones de software”*. Ambos reglamentos entraron en vigor en julio de 2024, y por tanto, en la actualidad deberían estar siendo aplicados por los fabricantes de vehículos que se tengan que comercializar en Europa.

Para las personas que estamos habituadas al manejo de la nomenclatura del ámbito de la ciberseguridad, es muy curioso y satisfactorio ver muchos de esos conceptos en una normativa dirigida a fabricantes de vehículos. Por ejemplo, respecto de UN R155, la guía de INCIBE indica que *“El objetivo principal de la regulación R155 es definir los requisitos a cumplir por el vehículo y el fabricante para considerar que presenta un nivel de ciberseguridad adecuado frente a las amenazas de ciberseguridad recogidas en el anexo 5 de la homologación”*, y un poco más adelante, que *“Estos requisitos se centran en el sistema de gestión de la ciberseguridad del vehículo (SGSI), es decir, cómo se organiza y ejecuta la ciberseguridad, no sólo a nivel del vehículo y sus sistemas, también incluye en su alcance la ciberseguridad en los servidores del fabricante, su proceso de diseño y fabricación, sus capacidades para mantenimiento, monitorización y vigilancia, la gestión de vulnerabilidades y la gestión de la cadena de suministros”*.

Es decir, se trata el vehículo como un sistema tecnológico de tipo industrial, y como a éstos, se le han de aplicar medidas de seguridad apropiadas a su función. Realmente, merece la pena la lectura de la guía de INCIBE, donde se resumen las 24 medidas a tener en cuenta en el SGSI del fabricante para lograr la homologación, y donde se hace mucho hincapié en la necesaria protección de todos los componentes de la cadena de suministro, aspecto en el que hemos incidido en varias ocasiones en esta revista.

Por lo que respecta a la UN R156, la guía también resume los requisitos que ha de evidenciar el fabricante para mantener actualizado correctamente el software de los vehículos, de forma que éste no se convierta en una fuente de vulnerabilidad del sistema, dado que de él puede depender la vida de los ocupantes del vehículo o de las personas que están alrededor del mismo.

En fin, estamos ante un ámbito en el que los profesionales de la ciberseguridad tienen mucho trabajo por hacer, y con unas peculiaridades que lo convierten en un campo muy interesante. ¿Cuánto tardaremos en conocer algún caso de incidente real con estos vehículos? ¿Estaremos razonablemente seguros en su interior? Veremos....

Gobierno del Tiempo y Gestión de la Productividad con Time Slot Governance TSG4®



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



Crisis de ciberseguridad: ¿está su organización preparada?

En el artículo de este mes, tratamos un tema poco habitual: las crisis de ciberseguridad y la (por lo general) nula preparación que nuestras organizaciones tienen ante este tipo de situaciones que exceden en magnitud a un "simple ciberincidente". Nos conviene plantearnos preguntas que comiencen por un "¿Y qué pasa si...?", evaluar el riesgo, y actuar en consecuencia.

En números anteriores de esta revista ya se publicó una serie de artículos sobre la Gestión de Ciberincidentes, en base a metodologías y conceptos ampliamente aceptados. Claramente, parece una cuestión puramente técnica, y de contar con los recursos apropiados, asumible en condiciones normales. Pero, ¿qué ocurre si el ciberincidente escala a un alcance o magnitud que el equipo asignado para su resolución es incapaz de contener? ¿O si se alarga en el tiempo de forma excesiva y afecta gravemente al funcionamiento de la organización, poniendo incluso en riesgo su existencia? Pues nos encontramos ante una crisis en materia de ciberseguridad que hay que afrontar, y como tal, la preparación previa será fundamental.

La "Guía de gestión de crisis de ciberseguridad en empresas", publicada recientemente por el Instituto Nacional de Ciberseguridad de España (INCIBE) define este tipo de crisis aludiendo a que *"Un incidente de ciberseguridad se convierte en una crisis cuando los daños ocasionados superan la capacidad de respuesta de la empresa afectada. Esto ocurre cuando los recursos y procedimientos habituales de la entidad no son suficientes para dar respuesta al incidente, provocando una escalada en la gravedad y el alcance del problema"*.

La norma "ISO 22361 Gestión de crisis", más general y no tan enfocada en la ciberseguridad como la guía del INCIBE, establece un enfoque sistemático para la gestión de crisis, que consta de cinco etapas clave:



CONTINÚA EN
PRÓXIMA PÁGINA





- La identificación de riesgos y amenazas.
- La planificación y preparación.
- La comunicación y coordinación.
- La capacitación y ejercicios o simulacros.
- Y la evaluación y mejora continua.

¿Cuántas de sus organizaciones han pensado siquiera en ello? Pues las más maduras y con espíritu de resiliencia, donde la continuidad de la actividad de la organización es un objetivo en sí mismo, y que como otros, ha de planificarse cómo lograrlo. A este respecto, conviene indicar que la continuidad de negocio/servicio/organizacional no es únicamente ver cómo mantenemos las Tecnologías de la Información y las Comunicaciones disponibles, sino que es un concepto más amplio, que incluye personal, instalaciones y otros recursos.

Por ello, cuando se trata de gestionar crisis de ciberseguridad podemos atender a lo planteado por el estándar ISO 22361, circunscrito a los riesgos de ciberseguridad, pero sin perder de vista la altísima dependencia que de las TIC tienen nuestras organizaciones. Al final, lo que se pretende es implementar estrategias de respuesta adecuadas, optimizar la gestión de recursos y minimizar el impacto de la crisis en nuestra organización, y ello pasa por elaborar los planes apropiados, que éstos se conozcan, que los roles estén claros, y que el personal esté entrenado y motivado. Todos hemos estado en simulacros de incendios en el colegio o en el trabajo, tras alguna sesión de formación o concienciación. Pues algo parecido hay que lograr que ocurra con la ciberseguridad, ya que si bien es más dudoso que afecten a la salud y la vida de los afectados (aunque en algunos entornos, como el sanitario, claramente puede ocurrir), sí que puede llegar a provocar el cese de actividad de la organización.

La Guía del INCIBE cita, como beneficios de contar con un plan de gestión de crisis de ciberseguridad, que dicho plan permitirá:

- Identificar y mitigar riesgos.
- Prevenir una posible crisis.
- Disminuir el impacto que puede causar un ciberataque.
- Proteger la reputación de la organización.
- Y cumplir con normativas y regulaciones.

Pero si algo queda claro que que el citado plan permite **prepararse** ante esa eventualidad, diagnosticando y valorando riesgos. También permite que la organización reparta por anticipado responsabilidades (en forma de roles) entre las personas de la misma y organizaciones externas de soporte, para acometer las diferentes tareas que habrá que asumir para afrontar la crisis de ciberseguridad. En medio de la tormenta no podemos ponernos a pensar quién ha de llevar el timón, quien debe manejar el velamen, o quien debe fijar el rumbo. Esos roles han de estar meridianamente claros antes de comenzar la travesía, y las personas que los desempeñen han de estar capacitadas para ello.

De ahí que el plan ha de contar en la fase de preparación con elementos de capacitación de los implicados en la gestión de la crisis, y a ser posible, de actividades que permitan simular la situación crítica para analizar la adecuación del plan y de las respuestas previstas para cada rol. Es habitual que en este tipo de actividades se detecten problemas como, por ejemplo, que la lista de contraseñas de los sistemas de información están en documentos que, en caso de un ataque de ransomware, podrían quedar cifrados, dejando a la organización a merced de los ciberdelincuentes. Por tanto, el plan ha de definir cuándo, cómo y en qué formato se debe disponer de esa información, quizá en otro lugar y quizá en formato no digital, lo que supone que ese cambio de formatos debe realizarlo alguien o algo.

En cualquier caso, en la organización se deberá constituir un comité de gestión de crisis, que dirigirá la resolución de ésta a partir del momento en que se declare. Y por tanto, debe quedar definido quién declara la crisis y convoca al comité, y en qué situaciones ha de hacerlo. Por ejemplo, el documento de buenas prácticas "CCN-CERT BP/29 Gestión de crisis para ciberincidentes en entidades locales" recomienda que exista un comité de crisis donde estén presentes el/la Alcalde/sa, la persona responsable TIC, el/la Secretario/a, el/la Interventor/a, el/la Delegado/a de Protección de Datos, un responsable de Comunicación, y algún otro miembro de la Junta de Gobierno municipal. Con todos estos roles presentes, las decisiones que el comité de crisis impulse para afrontar la crisis estarán respaldadas por las máximas autoridades municipales, contarán con el respaldo legal y económico de los funcionarios con habilitación nacional, y se comunicarán adecuadamente a las partes interesadas del municipio.

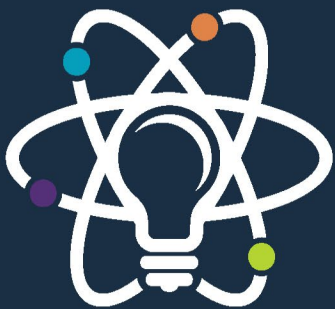
Como conclusión: gestionar cualquier tipo de crisis no es fácil, y requiere preparación previa para mitigar el impacto de la misma. Como dijo Confucio "hombre prevenido vale por dos". Y en este caso, más aún.

Gov Book

Governance

Body of Knowledge

P4MGO!®



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE



Robos de información: ¿evaluamos bien su impacto?

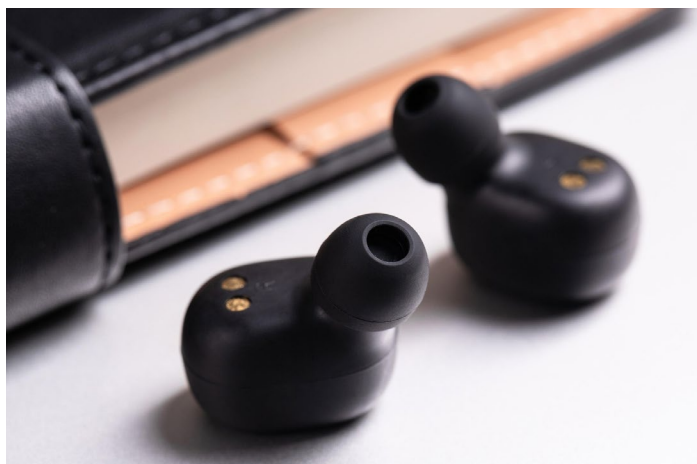
Que en un ataque a una organización o a una persona se produzca un robo de información es casi un clásico en la actualidad. Hasta los ataques de ransomware han evolucionado hacia esa consecuencia. Pero, ¿evaluamos correctamente las organizaciones, o las personas, el riesgo al que nos enfrentamos en caso de sufrir un robo de información?

Una de las preguntas típicas que hago en la primera clase a mis alumnos en materia de ciberseguridad es qué pretendemos proteger cuando establecemos medidas de seguridad en un sistema. Un elevado porcentaje del alumnado se decanta por la respuesta correcta, la información que se trata en dicho sistema, aunque es significativo la porción del alumnado que se decanta por citar la red, o la organización en general, como respuestas.

Cuando les confirmo que, efectivamente, es la información el activo más valioso de las organizaciones, planteo dos preguntas relacionadas. La primera es si creen que la protección de su información, la que llevan en su móvil o la que publican en sus redes sociales merece también ser protegida de forma análoga a la información de las organizaciones, y muchos responden que la importancia de esa información es menor. La segunda pregunta que les hago, especialmente a quienes han contestado así la primera pregunta, es si me pueden apuntar en un papel su nombre y su número de tarjeta de crédito, con su fecha de caducidad, el PIN y el CVV. Aquí automáticamente todos responden que no, que con esa información podría hacer compras en Internet.



**CONTINÚA EN
PRÓXIMA PÁGINA**



Este pequeño experimento social con personas jóvenes, nativos digitales, demuestra a mi entender dos cosas: no hay una sensación de que se está desprotegiendo la información personal al publicar en redes sociales, pero sin embargo, en cuanto se toca el tema económico, la actitud cambia. Y ello se debe a que el dinero sí se percibe por este grupo social (y por casi todos los grupos sociales) como un activo valioso, pero la privacidad no.

En las organizaciones, sobre todo en ciertos tipos de ellas, la conciencia de que toda la información que se maneja ha de ser protegida es mucho mayor, aunque los niveles de protección sean dispares y las actitudes reales antes los costes que esa protección requiere también lo sean. Sin embargo, todas las normas de seguridad de la información ponen el acento, precisamente, en la necesidad de que todos seamos conscientes de que esa información es el activo más valioso de nuestros sistemas, y que probablemente sea el único irremplazable (o con un costo enorme de reemplazo).

Es obvio que es así, ya que los sistemas de cómputo se crearon para tratar información, por lo que, por caros que éstos sean, es la información que tratan lo que requiere ser protegido.

En este contexto, merece la pena analizar cada nueva tipología o variante de los ataques que afectan, sobre todo, a los *leaks*, o exfiltración de información. Los ciberdelincuentes saben muy bien el valor de la información en el mercado negro. De hecho, hay incluso estudios que ponen precio a diferentes piezas de información personal o corporativa, aunque en este último caso, al tratarse de ataques dirigidos específicamente a determinadas empresas o organismos públicos, no suelen ser objeto de comercialización aquellos datos confidenciales que se exfiltran. Curiosamente, algunos de los datos más cotizados en ese mercado son los datos de salud de las personas, ya que ello puede permitir campañas de publicidad (legítimas o maliciosas) dirigidas a quienes sufren una determinada enfermedad, tratando de venderles medicamentos o tratamientos específicos (reales o no). Por no hablar de los problemas que pueden generar las suplantaciones de personalidad en transacciones electrónicas en muchos países.

En estos últimos meses se ha conocido un nuevo tipo de ataque de esta clase, al que se ha llamado **bluesnarfing**. Se trata de un ataque cuyo objetivo primordial es la exfiltración de información personal de terminales móviles, gracias al aprovechamiento de ciertas vulnerabilidades del protocolo Bluetooth y al descuido de los usuarios de *smartphones*, por lo que merece la pena darlo a conocer a nuestros lectores con cierto detalle, y sobre todo,

aconsejar cómo pueden protegerse del mismo.

El ataque se produce, sobre todo, en zonas concurridas, donde la probabilidad de que el software que han creado los ciberdelincuentes pueda localizar teléfonos vulnerables es mayor. Dicho software analiza cada dispositivo que tenga el interfaz Bluetooth activado, y trata de explotar las vulnerabilidades conocidas. Dependiendo del software concreto del teléfono atacado, los ciberdelincuentes pueden acceder al almacenamiento del mismo, ya que es uno de las funcionalidades que Bluetooth permite. Una vez accedido el almacenamiento, pueden exfiltrar información, o subir posibles scripts o aplicaciones maliciosas, aunque es cierto que el alcance de esta última amenaza es muy reducido.

Piense el lector sobre toda la información personal que hoy en día acumulamos en nuestros teléfonos: contactos, calendarios, chats, imágenes, documentos, historial de navegación, tarjetas de crédito, etc. Si los ciberdelincuentes son capaces de dejar un dispositivo malicioso en un lugar concurrido haciendo estas tareas de robo de información de forma automatizada, pueden recopilar una ingente cantidad de información de muchas personas, que adecuadamente clasificada y analizada, puede acabar siendo valiosa. Y no será porque no existan mecanismos para hacerlo hoy en día, incluidos los servicios de Inteligencia Artificial al alcance de cualquiera.

Cualquier lector mínimamente avisado ya podrá intuir cómo podemos protegernos de este tipo de ataques, y no, no es evitando ir a lugares concurridos:

1. Como el ataque se produce sobre conexiones Bluetooth activas, basta con llevar el interfaz Bluetooth del teléfono desactivado para que no seamos víctimas propiciatorias de los ciberdelincuentes que usan esta técnicas. Sin embargo, hoy en día, con los relojes inteligentes, los auriculares inalámbricos, o los teléfonos integrados en nuestros vehículos, mucha gente lleva el Bluetooth siempre activado para evitar tener que encenderlo y apagarlo cada vez que lo quieran usar. Nuestra recomendación es llevarlo apagado, salvo cuando sea estrictamente necesario.

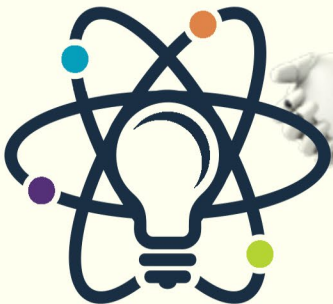
2. Como el ataque explota determinadas vulnerabilidades conocidas del protocolo Bluetooth y determinadas versiones de su implementación, la medida adecuada es mantener actualizado dicho software, para eliminar esas vulnerabilidades.

3. Es probable que ese ataque, en ciertas versiones de software Bluetooth, solicite permiso para establecer la conexión. Por tanto, debemos rechazar siempre intentos de conexión Bluetooth que no hayamos iniciado nosotros mismos en ese mismo momento. No importa lo atareados que estemos, mejor denegar una conexión legítima por error, que aceptar una conexión maliciosa por prisa.

Como concluirá el lector, para protegernos del *bluesnarfing*, y de otras muchas amenazas, lo principal es el sentido común y la conciencia de qué estamos haciendo cuando hacemos uso de cualquier dispositivo o aplicación informática: tratar información personal o corporativa, que debe ser protegida por ser lo más valioso que se tiene entre manos en ese momento.

CoE Book

Centres of Excellence Body of Knowledge P4MGO!®



P4MGO!

**PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE**



Estamos protegidos, seguro

Casi tan peligroso que no ser consciente de los riesgos en materia de seguridad de la información es pensar que se está a salvo de cualquier incidente en la materia. La falta de método en la definición de las medidas de seguridad, quizá impulsada por el mercado y a golpe de sobresalto, suele ser habitual en las organizaciones de nuestro entorno. De ahí que se desconozca en muchas ocasiones el nivel de riesgo que se está aceptando de forma inconsciente.

La expresión *“Tranquilo, que nosotros estamos seguros”* (aplicada a los sistemas de información) es una de las frases que muchos responsables de organizaciones escuchan (o han escuchado en el pasado) de ciertos personajes. Si quien la pronuncia es un mando no técnico, probablemente no sea consciente de la realidad de la situación. Pero si quien la pronuncia es un responsable técnico de los sistemas, sólo hay dos opciones: o ha hecho muy bien su trabajo y ha simplificado la frase para que se entienda la situación, o no ha hecho bien su trabajo y desconoce no ya la situación de sus sistemas, sino cómo está el entorno.

En muchas organizaciones, las inversiones tecnológicas se han venido realizando en base a argumentos, digamos, poco objetivos. Hacía falta computación, comprábamos servidores, por ejemplo. Y con la ciberseguridad ha ocurrido algo parecido. Como hace falta tenerla, mucha gente se puso en su día a comprar cortafuegos, antivirus, sistemas de backup, etc., simplemente porque parecía que había una “receta para estar ciberseguro”. Sin embargo, la tozuda realidad en esta materia, por mucho que haya quien no quiera verla o interpretarla correctamente, no es tan fácil de resolver simplemente comprando equipos o contratando personal o servicios de terceros.



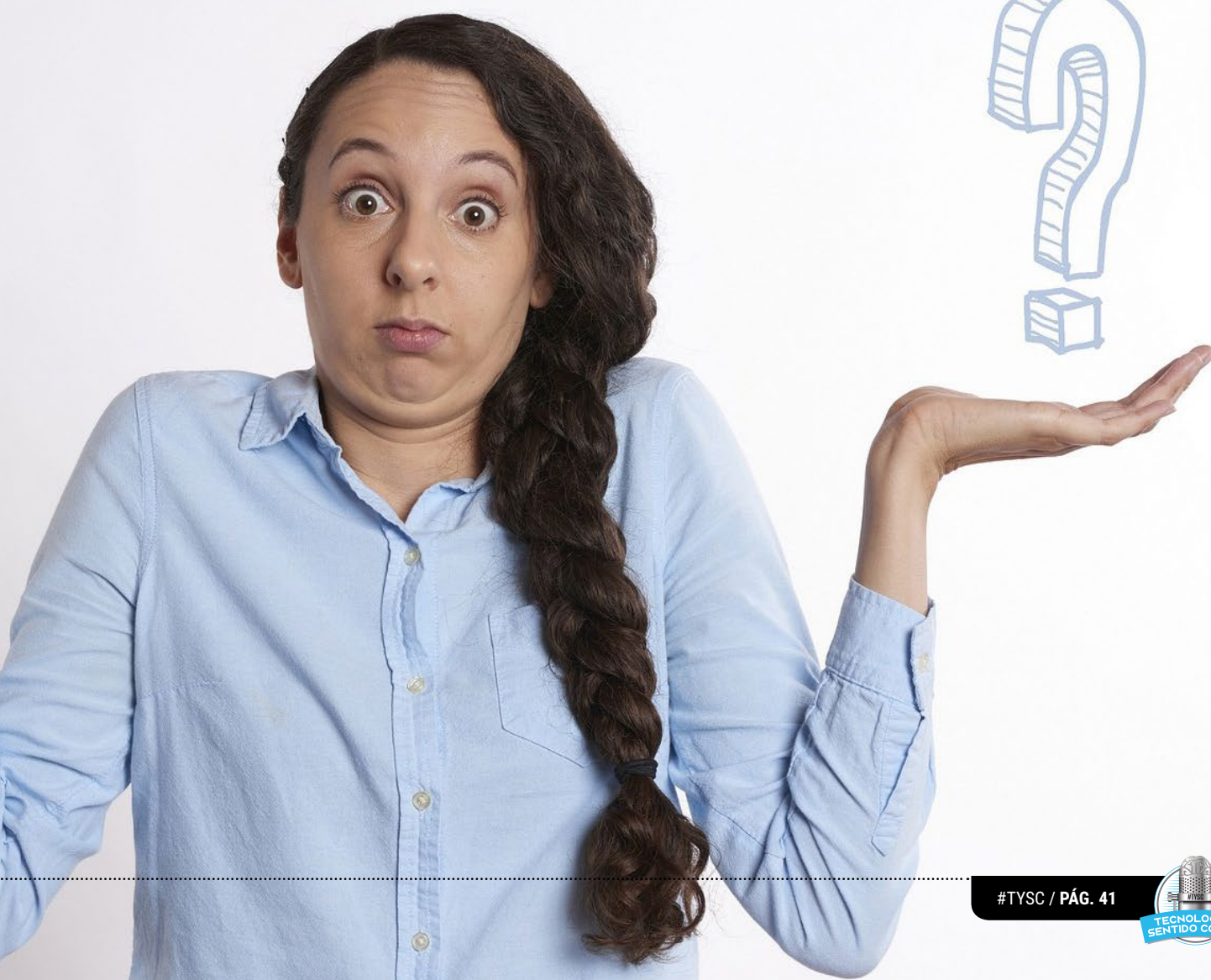
Lo primero que la Dirección de una organización debe exigir a sus servicios de Tecnologías de la Información es que conozcan las amenazas a las que sus sistemas de información están sometidos, cuál es el posible impacto de dichas amenazas en la organización, y cuál es el nivel de riesgo al que se está expuesto. A continuación, se debe exigir que, a ser posible de forma sistemática y usando algún método contrastado, se proceda a realizar un análisis de las posibles medidas de seguridad que permitan reducir el riesgo hasta niveles aceptables. Y finalmente, aquellos riesgos que no se puedan reducir más, aceptarlos, transferirlos o evitarlos.

Con un **enfoque metódico**, como el propuesto por la norma UNE 71504 "Metodología de análisis y gestión de riesgos para los sistemas de información", o el que se puede encontrar en la metodología MAGERIT 3.0, utilizada en las Administraciones Públicas españolas, la organización que desea obtener un adecuado rendimiento de sus inversiones en ciberseguridad dispondrá de una forma adecuada para planificar e implementar las medidas de seguridad apropiadas, evitando sobrecostes o asumiendo riesgos inasumibles.

Sea cual sea la metodología, es muy probable que la organización deba realizar una serie de actividades para lograr un marco de ciberseguridad adecuado a su situación contextual concreta, y que le permita revisarlo con una periodicidad apropiada. Es la aplicación del **ciclo PDCA de Deming a la ciberseguridad** lo que dotará a la organización de un nivel de riesgo lo suficientemente bajo como para que se puedan decir en voz alta expresiones del tipo "*Estamos razonablemente seguros*", aplicada a los sistemas de información. Porque si algo debe tener claro cualquier responsable de una organización es que el **riesgo cero no existe**. Lo que existe es un nivel de riesgo aceptable.

Las actividades que, en general, se deberán acometer en cualquier organización para adecuar su nivel de riesgo son las siguientes:

1. Realizar un inventario de los **activos** relacionados con las tecnologías de la información, no sólo tecnológicos, sino también información, instalaciones, personal, proveedores, etc.





2. Valorar qué supondría para la organización la pérdida (en sentido amplio) de ese activo. Ténganse en cuenta aspectos reputacionales, posibles impactos por pérdidas de confidencialidad en cuestiones de propiedad intelectual, etc. Está claro que valorar los dispositivos tecnológicos es muy fácil. Lo complicado es valorar el resto de componentes. La valoración puede hacerse cuantitativamente (en euros) o cualitativamente (en una escala de Muy valioso a Despreciable).

3. Analizar a qué amenazas está sujeto cada uno de los activos, y cuál es la probabilidad de su ocurrencia. Esta valoración de la probabilidad también puede hacerse de forma cualitativa (en porcentaje en un periodo de tiempo) o cualitativa (en una escala desde Muy alta a Despreciable). Se puede empezar por tres o cuatro amenazas principales, y dejar para ciclos futuros de mejora ir agregando otras. Hay que tener en cuenta que habrá amenazas que no dañen al 100% un activo, por lo que ese factor de daño también hay que tenerlo en cuenta.

4. Conocidos los activos y las amenazas que les circundan, y siendo homogéneos en las escalas de valoración (o cualitativas o cuantitativas ambas) se puede calcular cuál es el daño que cada amenaza haría en caso de materializarse, y a ese valor se le llama **Riesgo**. Se suele escalar en valores de 0 a 10 ó a 100.

5. A continuación, se evalúan las medidas de seguridad existentes en los diferentes activos, y cómo reducen el impacto de la amenaza en el activo, es decir, como reducen el riesgo de esa amenaza y activo. Tras esta evaluación, tenemos un riesgo residual, que es el que debemos tratar (quizá con más medidas de seguridad), transferir (con un seguro, por ejemplo), evitar (retirando activos del uso) o aceptar.

6. Al final, siempre acabaremos teniendo que aceptar algún nivel de riesgo, por lo que es responsabilidad de la Dirección de la organización establecer cuál es **el nivel de riesgo que se acepta (NRA)** en cada ciclo de mejora de la ciberseguridad.

7. Para todos los riesgos que se encuentran por encima del NRA, el personal especializado debe plantear un **Plan de Tratamiento del Riesgo (PTR)**, que, de forma justificada, plantee qué medidas de seguridad pueden ponerse en marcha para reducir esos riesgos por debajo del valor del NRA. Estas medidas pueden ser inversiones, contratar nuevos servicios, o simplemente, cambios organizativos, lo que incluye también políticas, normas y procedimientos a poner en marcha para lograr nuestro objetivo.

8. Idealmente, tras la finalización del PTR sería conveniente realizar algún tipo de auditoría para verificar la efectividad de las medidas ejecutadas y que realmente el riesgo de los sistemas de información está por debajo del NRA.

9. Pasado un determinado plazo (uno o dos años), o cuando los sistemas de información sufran cambios de calado, se deberá reiniciar el ciclo de mejora de la ciberseguridad, de forma que la Dirección pueda bajar el NRA en cada ciclo, acercándolo cada vez más al cero. Y tampoco estaría de más hacer análisis de riesgos de los nuevos servicios durante la fase de concepción de los mismos.

Como puede ver el lector, esta es una aproximación sistemática, que permite justificar todos los costes que se asumen en la seguridad de los sistemas de información, y que no se ve afectada por “ideas felices” o “presión comercial”.

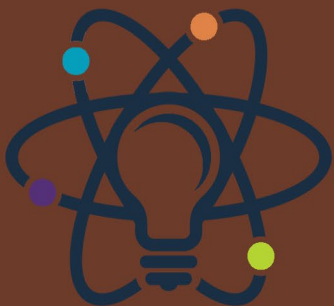
Y en su organización ¿se analizan los riesgos tecnológicos así, o se gestionan las TIC con el **método ASM (A Salto de Mata)**?

PMO Book

Management Offices

Body of Knowledge

P4MGO!®



P4MGO!

**PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE**



Vivir sin acceso al Oráculo de Delfos: medir para proteger

En el artículo del mes pasado de Tecnologías y Sentido Común tratamos el tema de cómo valorar si las iniciativas de seguridad de la información estaban correctamente orientadas y podían ser eficientes en la consecución del objetivo de proteger los activos de la organización. El siguiente problema es cómo medir la eficacia de las medidas implantadas a consecuencia del Plan de Tratamiento del Riesgo. Este mes, planteamos una aproximación a cómo hacerlo.

En el contexto actual, donde las amenazas cibernéticas son cada vez más sofisticadas y frecuentes, como venimos poniendo de manifiesto en esta sección mensual de Tecnología y Sentido Común, es esencial que las organizaciones puedan conocer cuál está siendo la evolución de la eficacia de las medidas de seguridad de la información que implanten. No basta con pensar o decir que tal o cual medida nos protege de tal o cual amenaza, sino que hay que demostrarlo con datos.

Por ello, es necesario que se implementen **métricas e indicadores de ciberseguridad** que permitan a la organización evaluar (y mejorar) su postura de seguridad. Estas métricas permiten a las organizaciones medir la efectividad de sus controles de seguridad, identificar áreas de mejora y comunicar el estado de la seguridad a las partes interesadas, especialmente, a la Dirección General de la misma.



La importancia de establecer métricas e indicadores de ciberseguridad radica en la capacidad de una organización para anticipar, detectar y responder a incidentes de seguridad de manera eficaz. Según las Guías CCN-STIC del Centro Criptológico Nacional de España, la implementación de métricas de ciberseguridad es fundamental para mantener un nivel adecuado de protección y resiliencia frente a las amenazas cibernéticas. Estas guías proporcionan normas, instrucciones y recomendaciones que ayudan a las organizaciones a mejorar su grado de ciberseguridad mediante la adopción de buenas prácticas y la utilización de herramientas adecuadas, y aunque en principio se orientan a las Administraciones Públicas, pueden utilizarse por cualquier organización.

Las **métricas de ciberseguridad** son valores cuantificables que reflejan el rendimiento de los controles de seguridad de una organización. Por otro lado, los **indicadores de ciberseguridad** son medidas específicas que se utilizan para evaluar el estado de la seguridad en áreas concretas de interés para la organización. Para definir métricas e indicadores efectivos, es importante seguir estos pasos:

1. Identificación de Objetivos de Seguridad: Determinar los objetivos de seguridad de la organización, tales como la protección de datos sensibles o confidenciales, la prevención de intrusiones o la respuesta rápida a incidentes.

2. Selección de Métricas Relevantes: Elegir métricas que sean relevantes para los objetivos de seguridad establecidos. Estas métricas deben ser específicas, medibles, alcanzables, relevantes y temporales (SMART: *Specific, Measurable, Achievable, Relevant, y Time-bound*).

3. Establecimiento de Indicadores: Definir indicadores claros que permitan evaluar si las métricas seleccionadas muestran una situación adecuada o no de la organización respecto del objetivo a alcanzar. Los indicadores deben ser precisos y proporcionar información útil para la toma de decisiones.

4. Recopilación de Datos: Implementar procesos para recopilar los datos necesarios para calcular las métricas e indicadores. Esto puede incluir el uso de herramientas de monitorización, logs de eventos y tests o auditorías específicas de seguridad de la información.

5. Análisis y Reporte: Analizar los datos recopilados para evaluar el rendimiento de los controles de seguridad y generar informes que comuniquen los resultados a las partes interesadas.

Tal vez todo esto parezca etéreo o complejo, pero en otros ámbitos de la gestión y el gobierno de las organizaciones la definición de métricas e indicadores es una actividad consolidada y básica, y la ciberseguridad no debe ser una excepción. También es usual que las organizaciones presenten sus indicadores en forma de cuadro de mandos, una herramienta gráfica que muestra la información de forma visual y cómoda, y que suele permitir 'navegar' por los diferentes gráficos del mismo para indagar en la información que presenta.

Sin entrar en excesivo detalle, a continuación se presentan tres ejemplos de métricas de ciberseguridad, junto con sus indicadores asociados, el valor que aportan a la organización y el proceso para recopilar los datos necesarios.



CONTINÚA EN
PRÓXIMA PÁGINA





1. Tiempo Medio de Detección (MTTD)

- Indicador Asociado: Tiempo transcurrido desde la ocurrencia de un incidente de seguridad hasta su detección.
- Valor para la Organización: El MTTD es crucial para evaluar la capacidad de la organización para identificar rápidamente las amenazas. Un MTTD bajo indica una alta eficiencia en la detección de incidentes, lo que permite una respuesta más rápida y reduce el impacto potencial. Este indicador debe asociarse siempre a otro que defina el nivel de falsos positivos de la herramienta de detección, ya que un MTTD bajo asociado a una alta tasa de falsos positivos puede significar una excesiva carga de trabajo para el personal de ciberseguridad y una necesidad de ajuste en dicha herramienta de detección.
- Proceso de Recopilación de Datos: Lo habitual es utilizar herramientas de monitorización de seguridad que registren los eventos de seguridad, tal como un SIEM (*Security Information Event Management*) y sus tiempos de detección. Este tipo de herramientas analizan los registros de los equipos monitorizados a la búsqueda de patrones que indiquen la ocurrencia de los incidentes. Después, se puede calcular el tiempo medio de detección.

2. Tasa de Éxito de los Ataques de Phishing

- Indicador Asociado: Porcentaje de intentos de phishing que resultan en compromisos exitosos.
- Valor para la Organización: Esta métrica ayuda a evaluar la efectividad de las campañas de concienciación y formación en seguridad. Una tasa de éxito baja indica que el personal está bien preparado para identificar y evitar ataques de *phishing*.
- Proceso de Recopilación de Datos: Realizar pruebas de *phishing* simuladas y registrar los resultados, para poder analizar los datos y determinar el porcentaje de personal que cayó en los intentos de *phishing*.

3. Tiempo Medio de Resolución (MTTR)

- Indicador Asociado: Tiempo transcurrido desde la detección de un incidente de seguridad hasta su resolución completa.
 - Valor para la Organización: El MTTR es fundamental para evaluar la capacidad de la organización para responder y mitigar incidentes de seguridad. Un MTTR bajo indica una alta eficiencia en la gestión de incidentes, lo que minimiza el impacto y la duración de los mismos.
 - Proceso de Recopilación de Datos: Utilizar herramientas de gestión de incidentes que registren los tiempos de resolución y posteriormente, analizar los registros de incidentes para calcular el tiempo medio de resolución.
- En conclusión, definir y establecer métricas e indicadores de ciberseguridad es esencial para cualquier organización que desee mejorar su postura de seguridad y proteger sus activos digitales. Al seguir un enfoque estructurado tanto para analizar y mitigar los riesgos, como para la selección de métricas, la definición de indicadores y la recopilación de datos, las organizaciones pueden obtener una visión clara de su rendimiento en ciberseguridad y tomar decisiones informadas para fortalecer sus defensas.

En su organización, ¿siguen este proceso o están suscritos al Oráculo de Delfos?

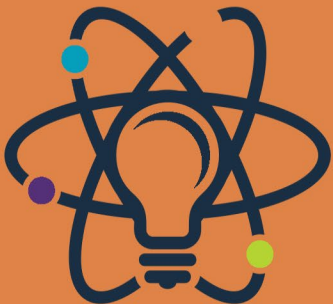
PgM Book

Programme

Management

Body of Knowledge

P4MGO!®



P4MGO!

**PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE**



Retos para el uso corporativo de la Inteligencia Artificial

Hoy en día tenemos Inteligencia Artificial hasta en la sopa. Los servicios de IA se multiplican como los hongos en un ambiente cálido y húmedo. Y los usuarios corporativos, ávidos de mejorar su productividad (o pensando en trabajar menos), están utilizándolos de forma masiva. Pero en estos entornos hay condicionantes que no se dan en el uso doméstico o particular de estos servicios, como tantas veces ha ocurrido con la tecnología y sus avances. Éstos son los retos a los que prestar atención en el entorno empresarial o en el sector público.

Cuando comenzó la 10ª temporada de Tecnología y Sentido Común en septiembre de 2024, publiqué un artículo acerca de la necesidad de que la Inteligencia Artificial (IA) discurriera por un camino de responsabilidad y uso ético. Diez meses después, hablaremos de los retos a los que se enfrentan aquellos que tratan de que esto ocurra en un entorno empresarial o del sector público.

Como ha ocurrido en el pasado con otros productos o servicios tecnológicos, la consumerización de los servicios de Inteligencia Artificial, básicamente desde la popularización de la IA Generativa (IAGen) hace un par de años, ha hecho que muchos empleados de las organizaciones se animen a tratar de usarla para su trabajo.

Cualquier directivo de una empresa europea mínimamente consciente de los riesgos que se asumen debe haber sentido una creciente inquietud por la acelerada adopción de herramientas de Inteligencia Artificial Generativa por parte de sus equipos. Lo que comenzó

como una curiosidad puntual, una simple experimentación con plataformas gratuitas como ChatGPT, Bard o Copilot, se ha convertido en una práctica habitual entre analistas, redactores, programadores e incluso personal de atención al cliente. Este fenómeno plantea oportunidades innegables, pero también retos significativos, especialmente en lo relativo al cumplimiento normativo, la protección de datos y la seguridad de la información corporativa.

La Inteligencia Artificial Generativa, en sus diferentes formas, ha demostrado ser una herramienta poderosa para aumentar la productividad, automatizar tareas rutinarias, generar contenido original y asistir en procesos de generación de ideas o redacción de textos. No obstante, la facilidad de acceso a estas tecnologías, especialmente a través de servicios gratuitos y generalistas, ha provocado que muchos empleados empiecen a utilizarlas sin una comprensión adecuada de los riesgos implicados.

Uno de los principales problemas, si no el mayor, es la falta de control sobre la información que se introduce en estos sistemas. Muchos empleados copian y pegan datos sensibles, borradores de contratos, estrategias comerciales o incluso código fuente en interfaces web sin



**CONTINÚA EN
PRÓXIMA PÁGINA**





considerar que, en muchos casos, los términos de uso de estas plataformas permiten el almacenamiento, análisis e incluso reentrenamiento de los modelos de IAGen con dicha información. En el contexto europeo, donde el Reglamento General de Protección de Datos (RGPD) impone obligaciones estrictas sobre el tratamiento y almacenamiento de datos personales, este tipo de uso representa un riesgo legal serio.

Nos encontramos, por tanto, ante una tensión constante entre la innovación tecnológica y el cumplimiento normativo. Por un lado, deseamos fomentar la eficiencia, creatividad y agilidad que estas herramientas pueden aportar. Por otro, estamos obligados a garantizar que nuestros procesos respetan los marcos regulatorios europeos, especialmente en lo relativo a la confidencialidad de la información y la responsabilidad en la toma de decisiones automatizadas. También a la protección de la propiedad intelectual e industrial de la compañía, que puede verse amenazada si cierta información se vuelca en uno de estos servicios sin control.

Un aspecto particularmente complejo es la diferenciación entre el uso de servicios gratuitos y generalistas, y el uso de servicios de pago o soluciones empresariales que garanticen un mayor nivel de privacidad y cumplimiento. Muchos empleados, motivados por la inmediatez y gratuidad de herramientas como ChatGPT (en su versión pública) o similares, optan por estas sin consultar con el departamento de TI o legal. Sin embargo, estas plataformas, al no estar diseñadas para un uso empresarial ni ofrecer garantías contractuales sobre la no compartición de datos, pueden comprometer seriamente la información estratégica de la compañía.

En contraste, existen soluciones empresariales de IAGen que, si bien suponen un coste adicional, están diseñadas para garantizar que la información introducida por los usuarios no se comparte ni se utiliza para entrenar modelos que puedan beneficiar a terceros. Estos servicios ofrecen acuerdos de tratamiento de datos, almacenamiento en la Unión Europea, autenticación robusta de usuarios y capacidades de auditoría. Su adopción puede suponer una barrera inicial en términos de costes o de integración con los sistemas existentes, pero representan una inversión necesaria para proteger la competitividad y la integridad legal de la organización.

Otro reto significativo es la falta de formación específica entre los empleados sobre los riesgos y buenas prácticas en el uso de IAGen. En muchos casos, se da por hecho que estas

herramientas son seguras por defecto, o que su uso no tiene implicaciones legales si se limita a tareas “menores” como redactar correos o hacer resúmenes. Esta percepción errónea puede llevar a errores graves, especialmente cuando se manejan datos de clientes, información financiera o propiedad intelectual. De hecho, el Reglamento Europeo de IA establece la obligatoriedad de la alfabetización en IA de los empleados de nuestras organizaciones.

Desde la perspectiva de la dirección, es esencial adoptar un enfoque proactivo. Esto implica desarrollar una política corporativa clara sobre el uso de la IAGen, incluyendo directrices sobre qué herramientas están aprobadas, qué tipo de información puede compartirse, y cuáles son las obligaciones de cada empleado respecto al cumplimiento normativo. Asimismo, es fundamental integrar la formación sobre estas herramientas en los programas de *onboarding*, reciclaje y capacitación continua.

Del mismo modo, se hace necesario un trabajo coordinado entre los departamentos de tecnología, legal, recursos humanos y cumplimiento. Solo a través de una estrategia transversal podremos garantizar que la adopción de estas tecnologías en la organización no se produzca de forma caótica o descontrolada. Es vital, además, establecer mecanismos de monitorización y auditoría que permitan detectar usos indebidos, evaluar riesgos emergentes y ajustar las políticas según evolucione el marco legal y tecnológico.

Por otro lado, no podemos obviar el aspecto reputacional. El uso indebido de estas herramientas puede dar lugar a filtraciones de datos, errores en decisiones automatizadas o contenido generado que infrinja derechos de autor. Estos riesgos no solo suponen posibles sanciones económicas, sino también una pérdida de confianza por parte de clientes, inversores y socios. En un entorno competitivo y altamente digitalizado, la reputación corporativa es un activo tan valioso como la tecnología o el capital humano.

Ante esta situación, es fundamental que la alta dirección lidere con claridad y coherencia. No basta con advertencias o restricciones técnicas. Es necesario promover una cultura de uso responsable de la IAGen, en la que los beneficios vayan acompañados de una conciencia plena sobre los riesgos y responsabilidades. La transparencia, la formación y la coherencia en la aplicación de políticas deben ser los pilares de esa estrategia.

También debemos reconocer que la solución no pasa por prohibir estas herramientas, sino por canalizar su uso dentro de marcos seguros. Negar su utilidad o intentar bloquear su acceso solo fomentará prácticas encubiertas y la aparición de una “IAGen en la sombra” dentro de la organización. En cambio, si ofrecemos alternativas corporativas seguras, formación adecuada y apoyo técnico, podremos convertir la IAGen en un aliado estratégico en lugar de una amenaza latente.

Aprovecho este último artículo de la 10ª temporada de nuestra revista para desear a todos nuestros lectores un feliz verano y que disfruten del bien merecido descanso. ¡Volvemos en septiembre!

¿Entregas Caóticas?
¿Insatisfacción con los resultados?
¿Descoordinación de esfuerzos?
¿Ausencia de progreso o incumplimiento de plazos?
¿Falta de visión de la actividad transformadora?



Regularidad, progreso y cumplimiento
Entregas predecibles y satisfactorias
Credibilidad en la actividad transformadora
Claridad de responsabilidades
Ganancia rápidas y logros que motivan



soluciones@p4mgo.com
<https://p4mgo.com>

Cierre de Temporada 2025 Revistas “Tecnología y Sentido Común” y “Stakeholders.news”

El Evento de Cierre de Temporada 2025 de las Revistas “Tecnología y Sentido Común” y “Stakeholders.news” celebrado el viernes 11 de julio quedará grabada en la memoria de todos los asistentes como una fecha especial, no solo por marcar el cierre de la décima temporada de dos revistas de referencia, sino por condensar, en un solo acto, el espíritu de una década entera de trabajo, aprendizaje y crecimiento compartido. La sede de UNE, la Asociación Española de Normalización, se impregnó desde bien temprano de un ambiente animado, mezcla de solemnidad y calidez. Al abrirse las puertas, la sensación era la de asistir a una gran reunión de familia profesional, un reencuentro anual que cada vez gana en prestigio, asistencia y profundidad de lazos personales.

La bienvenida, realizada por Javier Peris en su doble faceta de director de ambas revistas, así como por Fernando Machicado en representación de la entidad que acoge el evento, marcó el tono de la mañana. Ambos recordaron a los presentes que, más allá del recuento de logros o de un simple cierre de curso, el encuentro de final de temporada persigue renovar el compromiso de todos los que integran las comunidades de Tecnología y Sentido Común y Stakeholders.news, ya sea desde la primera línea como expertos, columnistas y responsables de áreas, o desde la imprescindible labor de los lectores y socios estratégicos. Subyacía en sus palabras la presencia constante de la tradición, compañera inseparable de toda evolución significativa, así como la importancia de la normalización y la excelencia, valores irrenunciables para el futuro inmediato del sector.



CONTINÚA EN
PRÓXIMA PÁGINA

Suscríbete gratis

REVISTA MENSUAL DE DIRECCIÓN Y GESTIÓN DE PROYECTOS, PROGRAMAS Y PROYECTOS

Stakeholders .news

PORTFOLIO, PROGRAMAS Y PROYECTOS MANAGEMENT

NÚMERO 11 DICIEMBRE 2022

PROTAGONISTA DEL MES

MARC
HUGHMANS

FONDOS, ESTOS LÓBOS

PRENDIDAS

REGULARES

VER EN CUENTA

NO

V DIGITAL

CIÓN

ESCA PARA

SO \$1.000

Even
CIER
Revista
y "Stak

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Stakeholders

En este contexto, la primera intervención de la jornada adquiere todo su sentido. Elena Ordozgoiti, responsable de negocio del sector servicios de UNE, supo captar la atención de la sala no solo con datos y argumentos, sino con una visión estratégica que puso de relieve el papel esencial que juega la normalización en el desarrollo de las industrias, las administraciones y, en definitiva, en la vida cotidiana de la población.

Ordozgoiti explicó la compleja red de colaboraciones y sinergias entre los organismos nacionales, europeos y globales de normalización, y cómo la participación española en el Subcomité CTN 309/SC 01 ha permitido situar a nuestro país en la vanguardia de la excelencia. Destacó también el profundo impacto de la normalización en la generación de confianza, interoperabilidad y competitividad, recordando que el establecimiento de estándares no es solo una labor técnica, sino también ética y social. Su exposición abierta y comprometida no solo resultó didáctica, sino que afianzó la convicción de la audiencia sobre la necesidad de participar activamente en la construcción de estándares de calidad para el conjunto de la sociedad.

Así, la meta de facilitar marcos de referencia sólidos se presenta como una oportunidad estratégica de futuro, y una responsabilidad compartida por todos los presentes, desde los autores de artículos hasta quienes ocupan responsabilidades de dirección y toma de decisiones.



CONTINÚA EN
PRÓXIMA PÁGINA

CIÓN DE PORFOLIOS, PROGRAMAS Y PROYECTOS

holders

.news

AGEMENT

CONISTA DEL MES

MARC
BERGHMANS

NDOS, ESTOS LODOS

APRENDIDAS

INGULARES
ega

NER EN CUENTA

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

años, de 1470 a 1484

El tono inspirador de la mañana se mantuvo durante la intervención de Marcelino Lominchar, cuyo discurso supuso un viaje inesperado, enriquecedor y muy humano por la historia de España. A partir de los relatos recogidos en su obra "Historias de la Historia de España", Lominchar desenmascaró mitos, ofreció detalles sorprendentes y recuperó figuras cuyo legado ha sido frecuentemente eclipsado por prejuicios y narrativas ajenas.

Lejos de limitarse a una crónica tradicional, su charla estuvo plagada de guiños al presente, extrayendo lecciones de gestión, resiliencia y liderazgo de episodios históricos. Sorprendió a los presentes mostrando monedas icónicas como el real de a ocho o el maravedí, verdaderos símbolos de la pujanza hispánica que influyeron decisivamente en la economía global. Detalló cómo personajes como Colón o Magallanes debieron desplegar una impresionante cantidad de habilidades de persuasión para sacar adelante sus proyectos, anticipándose así a lo que actualmente conocemos como gestión del cambio, emprendimiento y defensa de la innovación.

Pero uno de los momentos más celebrados de su exposición fue la reivindicación de Gonzalo Fernández de Córdoba, el Gran Capitán, a quien Lominchar atribuyó – con sólidos argumentos – la invención de una suerte de "agilismo" aplicado al arte de la guerra y, por extensión, a la administración y gestión de proyectos en épocas de incertidumbre.



CONTINÚA EN
PRÓXIMA PÁGINA



STA

logía & Común



REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Estas reflexiones sirvieron de nexo para el siguiente bloque de la jornada, la mesa redonda en la que participaron siete colaboradores de las revistas, una suerte de gabinete de expertos en el que confluyeron voces de disciplinas tan variadas como la inteligencia artificial, el derecho, la gestión pública y la creatividad.

El diálogo, hábilmente moderado por Javier Peris, permitió repasar aquellas tendencias, inquietudes y expectativas que han marcado el último año editorial. Los ponentes compartieron reflexiones sobre cómo escogen sus temas, cómo detectan tendencias y qué importancia conceden al rigor y a la originalidad a la hora de abordar asuntos de actualidad, desde la expansión de la inteligencia artificial hasta los desafíos regulatorios o el potencial transformador de la creatividad en los procesos de cambio. Hubo consenso respecto a la urgente necesidad de que la sociedad

saque partido a las mentes divergentes, esas voces innovadoras, a menudo incómodas pero imprescindibles para que cualquier organización y ecosistema profesional pueda reinventarse y crecer.

Muy lejos de un debate corporativo y riguroso, en varios momentos la conversación adoptó un tono cercano y humorístico, rebajando la solemnidad y recordando la importancia del factor humano para el éxito de cualquier iniciativa. Se insistió en la importancia de mantener la independencia intelectual de los colaboradores, de seguir apostando por la pedagogía aplicada y de construir puentes de entendimiento entre generaciones y perfiles profesionales muy distintos.



CONTINÚA EN
PRÓXIMA PÁGINA



TECNOLOGÍA Y SENTIDO COMÚN

12:15 a 13:00

					
RICARD MARTÍNEZ	ALEJANDRO ALIAGA	MARLON MOLINA	MARCOS NAVARRO	VICTOR ALMONACID	MARTA MARTÍN
Sección: Ojo al dato	Sección: Radio Security	Sección: Es Tendencia	Sección: AI Futuro	Sección: La Nueva Administración	Sección: Mentes Divergentes

Suscríbete gratis

REVISTA

Tecnología & Sentido Común

2022

PREMIOS SAPIENS



REVISTA

Tecnología & Sentido Común

<https://tecnologiaysentidocomun.com>

La mañana prosiguió con la segunda de las mesas redondas, en este caso consagrada a la comunidad internacional de Stakeholders.news.

La mesa reunió tanto a colaboradores presentes como a los corresponsales internacionales, que aportaron sus reflexiones en formato de mensaje grabado, conectando así Madrid con América Latina y el Caribe.

Entre los aspectos más destacados del debate figuraron las diferencias regionales en la percepción y aplicación de la innovación social y empresarial, el impacto de la regulación en los procesos de sostenibilidad y la creciente importancia

de la ética, la transparencia y las alianzas multinacionales.

Cada colaborador expuso aquello que considera el mayor aporte de su sección durante el año, detallando no solo las temáticas, sino también las reacciones suscitadas entre los lectores y el valor añadido de contar con una red plural y cosmopolita. La interacción entre moderador y ponentes sirvió para poner de manifiesto la transversalidad de los retos contemporáneos y la urgencia de compartir aprendizaje y experiencias más allá de fronteras y disciplinas.



CONTINÚA EN
PRÓXIMA PÁGINA



MESA REDONDA
moderada por Javier Per



LUIS
MORÁN

Sección:
Personas Y
Procesos



#TYSC / PÁG. 60

Sharing

13:00 a 13:30

DA "STAKEHOLDERS.NEWS"

					
JOSE ANTONIO PUENTES	JOSE LUIS PORTELA	RICARDO SASTRE	LUIS GUARDADO	NESTY DELGADO	DANIEL SOROKINS
Sección: Tendencias Puentes	Sección: Empleo y Futuro	Sección: Super PMO	Embajador: El Salvador	Embajador: Puerto Rico	Embajador: Uruguay



Suscríbete gratis

REVISTA

Tecnología & Sentido Común

#10

2022 PREMIOS SAPIENS

Llanos Cuenca

Alejandro Blasco

Talento y Liderazgo

Es tend

Por Procesos

Consejo de amigo

REVISTA

REVISTA

Tecnología & Sentido Común

<https://tecnologiaysentidocomun.com>



Este espíritu de apertura y renovación se evidenció de nuevo durante la presentación en sociedad de los nuevos colaboradores y secciones que integrarán la próxima temporada.

El público recibió con interés las propuestas de Domingo Gaitero, dispuesto a arrojar luz sobre la cara más amenazante y menos conocida de la ciberseguridad; la de Angie López Gea, quien acercará la cultura hacker a lectores de todas las edades; y la de Ismael Novo, que analizará el impacto y las aplicaciones prácticas de la inteligencia artificial en los negocios. A ellas hay que sumar la presencia internacional de Estuardo Castañeda, que aportará un enfoque desde Centroamérica mediante contenidos audiovisuales.

Estas nuevas incorporaciones dan fe de la apuesta continua de ambas revistas por la renovación, la pluralidad y el abordaje de tendencias emergentes con relevantes implicaciones sociales y culturales.



CONTINÚA EN
PRÓXIMA PÁGINA

Suscríbete gratis

DIRECCIÓN Y GESTIÓN DE PORFOLIOS, PROGRAMAS Y PROYECTOS

Stakeholders .news

PROGRAMME & PROJECT MANAGEMENT

NOVIEMBRE #011 - NOVIEMBRE 2022

» STAKEHOLDERS NEWS

PROTAGONISTA DEL MES

MARC BERGHMANS

DE AQUELLOS FONDOS, ESTOS LOGROS
en EDITORIAL
con Javier Paris

LECCIONES NO APRENDIDAS
DE LA PANDEMIA
en PROYECTOS SINGULARES
con Carlos Pampliega

DIMENSIONES A TENER EN CUENTA
EN UN PROCESO (SERIO)
DE TRANSFORMACIÓN DIGITAL
en TECNOTRANSFORMACIÓN
con Juan Jesús Urbizu

ESTÁNDARES DE REFERENCIA PARA
LA GESTIÓN DE RIESGOS ISO 21.000
en STEERING COMMITTEE
con Pedro Balas

¿CÓMO MEDIMOS LA RESILIENCIA
DE LAS ORGANIZACIONES?
en ORGANIZACIONES RESILIENTES
con Juan Manuel Domínguez

LAS PMOS EN EL METAVERSO
en SUPER PMOS
con Ricardo Sastre

CONTRATOS ÁGILES
en TRANSFORMACIÓN ÁGIL
con Ángela Plaza

¿CÓMO GENERAR AUTORIDAD
COMO INTERIM MANAGER?
en EMPLEO Y FUTURO
con José Luis Portela

MANEJANDO LAS EXPECTATIVAS
DE UN PROYECTO
en EL LADO HUMANO
con Chayo Fresneda

ENTOCARSE EN EL BIEN SER DE LA
PERSONAS, UNA DIMENSIÓN MÁS
HUMANA DENTRO DE LA DIRECCIÓN
de PROYECTOS
en CENTROAMÉRICA
con Estuardo



51 8



#TYSC / PÁG. 62

TECNOLOGÍA Y
SENTIDO COMÚN

13:30 a 13:45

NUEVOS COLABORADORES



**DOMINGO
GAITERO**
El lado oscuro
(TVSC)



**ESTUARDO
CASTANEDA**
Guatemala
(Stakeholders.news)



**ANGIE
LOPEZ GEA**
Hack & News
(Stakeholders.news)



**ISMAEL
NOVO**
Power AI
(Stakeholders.news)





Uno de los momentos más esperados de la mañana fue, como cada año, la entrega de los premios anuales con los que ambas publicaciones reconocen la labor de personas y entidades fundamentales para el progreso del sector. El Premio Tecnología y Sentido Común 2025 recayó sobre la Subdirección de Sistemas de Información del Hospital Universitari i Politècnic La Fe, una distinción más que merecida por su firme compromiso con la modernización digital, la eficiencia clínica y, sobre todo, la calidad asistencial a través de soluciones tecnológicas innovadoras.

Cayetano M. Hernández Marín recogió el premio en nombre de todo su equipo, acompañando el agradecimiento con un breve y emotivo discurso de gratitud, memoria y optimismo, recordando que todo avance tecnológico es, en última instancia, una apuesta por el bienestar del paciente y la dignidad del profesional sanitario.

En el ámbito de la responsabilidad social, Stakeholders.news reconoció a la Fundación The Pink Force por su extraordinaria iniciativa de acompañamiento emocional a niñas en tratamiento oncológico, haciéndolo en colaboración con el entrañable droide rosa R2-KT, inspirado en la historia real de Katie Johnson. El momento en que Andoni Serrano y el propio R2-KT se acercaron al estrado fue, sin duda, uno de los capítulos más conmovedores del evento. La ovación que recibieron, sincera y prolongada, recordó a todos que la tecnología, por avanzada que sea, solo tiene sentido cuando se pone al servicio de las personas más vulnerables.



**CONTINÚA EN
PRÓXIMA PÁGINA**

Suscríbete gratis

REVISTA MENSUAL DE DIRECCIÓN Y GESTIÓN DE PORTFOLIOS
Stakeholders

PORTFOLIO, PROGRAMME & PROJECT

NÚMERO #011 - NOVIEMBRE

PROYECTOS · GESTIÓN · EXCELENCIA · CALIDAD · PROFESIONALES



ENTREGA DE PREMIOS

PREMIO REVISTA

**Tecnología &
Sentido Común**
20



REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Llegados a este punto de la jornada, la sucesión de testimonios espontáneos, agradecimientos y recuerdos personales dibujó un ambiente único de comunidad y pertenencia. Los asistentes revivieron anécdotas de pasadas ediciones, mencionaron logros y desafíos superados, e incluso hubo espacio para la emoción y la lágrima compartida, fruto del profundo compromiso y afecto construido entre los colaboradores. Se homenajeó también la memoria de quienes, por motivos personales o profesionales, no pudieron estar presentes, dejando constancia del legado intergeneracional que caracteriza a las revistas.

La mañana se cerró, como manda la tradición, con un exclusivo catering que sirvió para prolongar la conversación y multiplicar las oportunidades de networking. Con mesas repletas de propuestas gastronómicas, la comunidad disfrutó de un momento de distensión en el que las fronteras jerárquicas desaparecen, permitiendo una interacción franca y productiva entre autores, lectores, directores, expertos y nuevos colaboradores. Este ambiente informal y dinámico, lejos de ser un simple complemento social, se ha revelado como uno de los espacios más fructíferos para el surgimiento de ideas, proyectos y futuras colaboraciones.

Culminado el acto, lo que queda es mucho más que el recuerdo de una celebración o el repaso a una década de publicaciones: es precisamente la constatación de que detrás de cada artículo, cada premio, cada panel y cada colaboración hay una apuesta decidida por el humanismo tecnológico, la ética profesional y la convicción de que el conocimiento debe ser compartido, discutido y puesto en acción colectiva. La décima edición del evento de cierre de temporada de Tecnología y Sentido Común y Stakeholders.news se reafirma, así, como un espacio de encuentro, inspiración y referencia para el ecosistema innovador en habla hispana.

El horizonte que se adivina tras esta cita es aún más prometedor. Los desafíos de la próxima década serán, si cabe, todavía más complejos y apasionantes. Nuevos colaboradores y lectores se sumarán a la conversación, las disciplinas seguirán expandiéndose y las alianzas, tanto nacionales como internacionales, pondrán a prueba la capacidad de adaptación, resiliencia y sentido común de toda la comunidad. Pero, como quedó patente a lo largo de toda la jornada, si algo distingue a los protagonistas de esta historia es su voluntad de cielo abierto y mirada larga. Porque, en definitiva, la tecnología y el compromiso social solo son motores de cambio si encuentran a mujeres y hombres dispuestos a caminar juntos, sumar talento y soñar, cada día, una sociedad mejor.



**Curso de
Certificación en:**

Gobierno Corporativo

**ISO 37000
Corporate
Governance
Leader**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695€
- Tasas Examen: Incluidas
- Acceso a la Norma: On Line
- A tu ritmo con toda comodidad

MidMgmt[®]

MPPM[®]

MGEIT[®]

eGob[®]

Tutorías en Directo

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>

UNE presenta su Estrategia 2030 para lograr un mayor impacto de las normas en la sociedad

Se basa en tres objetivos estratégicos: poner el conocimiento recogido en las normas al servicio del progreso compartido de España; impulsar la comunicación sobre los beneficios de las normas y su aplicación; y aportar estabilidad a UNE adaptando su modelo de financiación a la evolución del contexto.

La Estrategia 2030 de la Asociación Española de Normalización, UNE, aprobada en Asamblea General por sus miembros, se basa en tres objetivos y 14 prioridades, con los que la Entidad cumplirá su propósito: contribuir al progreso compartido de la sociedad.

Para lograr la Estrategia, UNE ampliará el alcance de su actividad y generará soluciones para facilitar su aplicación, poniendo el foco en visibilizar los beneficios de los estándares: la normalización aporta un 14,7 % al crecimiento medio anual del PIB en España.

La Asociación Española de Normalización, UNE, ha puesto en marcha su Estrategia 2030, que tiene como objetivo lograr un mayor impacto de las normas en la economía y en la sociedad.

Este ambicioso plan, aprobado por los miembros de UNE en Asamblea General, se basa en tres objetivos estratégicos: poner el conocimiento recogido en las normas al servicio del progreso compartido de España; impulsar la comunicación y el apoyo a la aplicación de las normas; y aportar estabilidad a UNE adaptando su modelo de financiación a la evolución del contexto.

Con ellos, el Organismo español busca ampliar el alcance de la actividad de normalización y dar respuesta eficaz a los grandes desafíos de las organizaciones españolas, potenciando la generación de soluciones que faciliten su implementación; para ello, adaptará el contenido de las normas a sus necesidades con las nuevas herramientas que ofrece la digitalización y, en especial, la inteligencia artificial (IA).

El vicepresidente de UNE, Luis Rodulfo, ha señalado: “La Estrategia UNE 2030 es una hoja de ruta que marca con claridad y suficiente nivel de detalle hacia dónde debemos dirigir todos nuestros esfuerzos y capacidades los próximos años para lograr nuestro propósito: contribuir al progreso compartido de la sociedad y a la creación de un mundo más seguro, sostenible y competitivo a través del desarrollo de estándares”.

En la definición de la Estrategia UNE 2026-2030 se han contemplado los elementos que definen el contexto geopolítico, económico, digital, social, legal y medioambiental, en los que las actividades de normalización y cooperación deben contribuir a lograrla. Además, se ha contemplado la contribución de UNE y de las normas técnicas a la consecución de los 17 Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030 de Naciones Unidas.



CONTINÚA EN
PRÓXIMA PÁGINA

Estos objetivos estratégicos aterrizan la ambición de UNE de seguir aportando un valor único a la sociedad y a la economía española, consolidando su impacto positivo. De hecho, la normalización aporta un 14,7 % al crecimiento medio anual del PIB en España, lo que se traduce en una contribución de más de 140.000 millones de euros en las últimas cuatro décadas, según el reciente Estudio “Impacto económico de la normalización en España”, realizado por el Centro de Estrategia y Prospectiva Industrial (CEPI), entidad impulsada por el Ministerio de Industria y Turismo y la Fundación EOI.

Los tres objetivos estratégicos son:

1.Poner el conocimiento recogido en las normas técnicas al servicio del progreso compartido de España

Para lograrlo, UNE se ha marcado cinco prioridades: reforzar la Norma como un servicio para las entidades públicas y privadas; dar respuesta a los retos a los que se enfrenta la empresa española con un catálogo de normas actualizado y alineado con sus necesidades; impulsar el liderazgo internacional y europeo de la normalización española; desarrollar un ecosistema equilibrado de alianzas de colaboración entre el ámbito público, privado y la sociedad civil; y ser ejemplar en materia de buen gobierno corporativo.

UNE es depositaria del mejor conocimiento generado por los 12.500 expertos de organizaciones españolas que participan en el desarrollo de estándares en los 200 Comités UNE.

2.Impulsar la comunicación sobre los beneficios de las normas y su aplicación

UNE reforzará la comunicación sobre los beneficios de las normas y generará soluciones para facilitar su aplicación a través de cinco prioridades: incrementar la aplicación de las normas en apoyo a las Administraciones públicas para simplificar la legislación y el despliegue de políticas públicas; garantizar la adecuación del contenido de las normas a las necesidades de aplicación del mercado; impulsar la difusión y aplicación de las normas mediante la actividad de cooperación a nivel nacional, internacional y multilateral, fijando una senda de crecimiento reputacional y económico; promover la cultura de cumplimiento de las normas apoyando la vigilancia de mercado y la evaluación de la conformidad en el marco de la infraestructura de la calidad; y fortalecer la comunicación de UNE.

3.Aportar estabilidad a UNE adaptando su modelo de financiación a la evolución del contexto

Mediante la contribución de todos los actores de su cadena de valor. El tercer objetivo se basa en cuatro prioridades: lograr una mayor contribución económica de las Administraciones públicas a la sostenibilidad de UNE; garantizar la aportación de la explotación del contenido de las normas a la sostenibilidad de UNE en el entorno cambiante de las necesidades de los usuarios; aumentar la contribución de los proyectos de cooperación fijando objetivos de rentabilidad económica y reputacional; y analizar otras líneas potenciales de crecimiento orgánico derivadas del valor generado por UNE



**Hace mucho
tiempo que
hablas.**

**¿Pero hace
cuánto no
dialogas?**



Somos una organización global de beneficio para la comunidad cuya misión es crear normas para contribuir a la construcción de un mundo más seguro, sostenible y competitivo.

Creamos espacios de colaboración neutrales e inspiradores en los que compartir conocimiento para desarrollar, a través del diálogo y el consenso, normas que sirvan a los intereses de toda la sociedad y que movilicen a los que apuestan decididamente por la excelencia empresarial y la conciencia social.

NUEVOS MASTERS

MasterPPM®
Gobierno, Dirección, Gestión y Ejecución de
Portfolios, Programas y Proyectos

MPPM® eGob®



Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
<https://escueladegobierno.es>