

ESPECIAL “Futuro y Seguridad”

DE Tecnología & Sentido Común



ESPECIAL

AGOSTO
2026

No al tocomochó:
estrategias de
prevención de
estafas on line

08

La seguridad de la
información empieza
por nosotros: hábitos,
cultura y conciencia (I)

12

La seguridad de la
información empieza por
nosotros: hábitos,
cultura y conciencia (II)

16

La seguridad de la
información empieza por
nosotros: hábitos, cultura y
conciencia (y III)

20

Aplicaciones móviles:
cuando la falta de
seguridad pone en riesgo
nuestros datos (I)

24

Aplicaciones móviles:
cuando la falta de
seguridad pone en riesgo
nuestros datos (II)

28

Aplicaciones móviles:
cuando la falta de
seguridad pone en
riesgo nuestros
datos (y III)

32

Domando al caballo
desbocado: gobierno
y gestión de la IA y
sus riesgos (I)

36

Domando al caballo
desbocado:
gobierno y
gestión de la IA y
sus riesgos (II)

40

Domando al caballo
desbocado: gobierno
y gestión de la IA y
sus riesgos (y III)

44

Evaluando el factor
humano: Human Risk
Management

48

“Futuro y Seguridad” DE Tecnología & Sentido Común



EQUIPO TYSC

Javier Peris - El Governauta
Manuel Serrat - Futuro y Seguridad
Nacho Alamillo - Tecnoregulación en Prospectiva
Domingo Gaitero - El Lado Oscuro
Marlon Molina - Es Tendencia
Ricard Martínez - Ojo Al Dato
Marcos Navarro - Ai Ai Ai
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

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

Curso de Certificación en:
Gobierno Corporativo
ISO 37000
Corporate Governance Leader

Dirección Académica:
 Javier París

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Basado en la Norma ISO 37000
- A tu ritmo con toda comodidad

Tutorías en Directo

Solicita tu admisión en:
 +34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
 EDUCATION ORGANIZATIONS
 MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Desarrollo de Indicadores de Gobierno Eficaz
ISO 37005
Effective Governance Indicators Designer

Dirección Académica:
 Javier París

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Basado en la Norma ISO 37005
- A tu ritmo con toda comodidad

Tutorías en Directo

Solicita tu admisión en:
 +34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
 EDUCATION ORGANIZATIONS
 MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Gobierno de la Inteligencia Artificial
ISO 38507
AI Governance Leader

Dirección Académica:
 Javier París

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

Tutorías en Directo

Solicita tu admisión en:
 +34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
 EDUCATION ORGANIZATIONS
 MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Gestión de la Inteligencia Artificial
ISO 42001
AI Management Leader

Dirección Académica:
 Javier París

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

Tutorías en Directo

Solicita tu admisión en:
 +34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
 EDUCATION ORGANIZATIONS
 MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Gobierno del Dato
UNE 0077
Data Governance Leader

Dirección Académica:
 Javier París

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Basado en la Norma UNE 0077
- A tu ritmo con toda comodidad

Tutorías en Directo

Solicita tu admisión en:
 +34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
 EDUCATION ORGANIZATIONS
 MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Gestión del Dato
UNE 0078
Data Management Leader

Dirección Académica:
 Javier París

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Basado en la Norma UNE 0078
- A tu ritmo con toda comodidad

Tutorías en Directo

Solicita tu admisión en:
 +34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
 EDUCATION ORGANIZATIONS
 MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Excelencia en el Servicio
ISO 23592
Service Excellence Leader

Dirección Académica:
 Javier París

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Basado en la Norma ISO 23592
- A tu ritmo con toda comodidad

Tutorías en Directo

Solicita tu admisión en:
 +34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
 EDUCATION ORGANIZATIONS
 MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Diseño de Servicios Excelentes
ISO 24082
Service Excellence Designer

Dirección Académica:
 Javier París

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Basado en la Norma ISO 24082
- A tu ritmo con toda comodidad

Tutorías en Directo

Solicita tu admisión en:
 +34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
 EDUCATION ORGANIZATIONS
 MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Inteligencia Estratégica
ISO 56006
Strategic Intelligence Management Leader

Dirección Académica:
 Javier París

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 18 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Acceso a la Norma: On Line
- A tu ritmo con toda comodidad

Tutorías en Directo

Solicita tu admisión en:
 +34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
 EDUCATION ORGANIZATIONS
 MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Gestión de la Innovación
ISO 56002
Innovation Management Leader

Dirección Académica:
 Javier París

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 18 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Acceso a la Norma: On Line
- A tu ritmo con toda comodidad

Tutorías en Directo

Solicita tu admisión en:
 +34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
 EDUCATION ORGANIZATIONS
 MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Gestión del Conocimiento
ISO 30401
Knowledge Management Leader

Dirección Académica:
 Javier París

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 18 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Acceso a la Norma: On Line
- A tu ritmo con toda comodidad

Tutorías en Directo

Solicita tu admisión en:
 +34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
 EDUCATION ORGANIZATIONS
 MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Gestión Documental
ISO 30301
Document Management Leader

Dirección Académica:
 Javier París

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 18 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Acceso a la Norma: On Line
- A tu ritmo con toda comodidad

Tutorías en Directo

Solicita tu admisión en:
 +34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
 EDUCATION ORGANIZATIONS
 MANAGEMENT SYSTEMS

ESPECIAL
AGOSTO
2026



índice

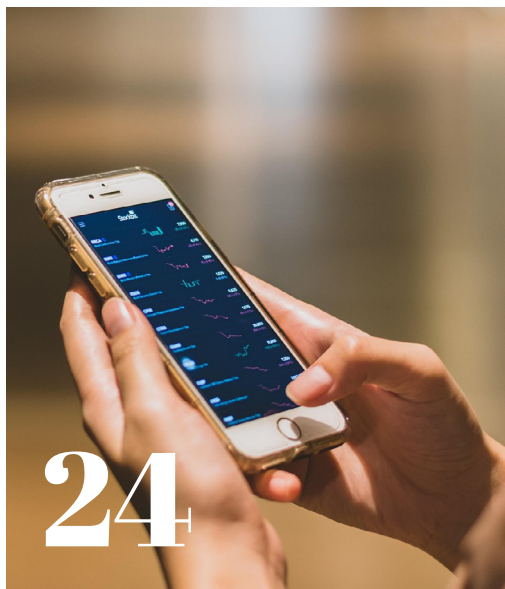
DE CONTENIDOS

<https://tecnologiaysentidocomun.com>



16

**La seguridad de la información
empieza por nosotros: hábitos,
cultura y conciencia (II)**



24

**Aplicaciones móviles:
cuando la falta de
seguridad pone en
riesgo nuestros datos (I)**



36

**Domando al caballo
desbocado: gobierno
y gestión de la IA y
sus riesgos (I)**



44

**Domando al caballo
desbocado: gobierno
y gestión de la IA y
sus riesgos (y III)**

Copyright

02

Índice de Contenidos

04

Este mes te recomiendo leer...

por JAVIER PERIS

07

No al tocomochó: estrategias de prevención de estafas on line

08

La seguridad de la información empieza por nosotros: hábitos, cultura y conciencia (I)

12

La seguridad de la información empieza por nosotros: hábitos, cultura y conciencia (II)

16

La seguridad de la información empieza por nosotros: hábitos, cultura y conciencia (y III)

20

Aplicaciones móviles: cuando la falta de seguridad pone en riesgo nuestros datos (I)

24

Aplicaciones móviles: cuando la falta de seguridad pone en riesgo nuestros datos (II)

28

Aplicaciones móviles: cuando la falta de seguridad pone en riesgo nuestros datos (y III)

32

Domando al caballo desbocado: gobierno y gestión de la IA y sus riesgos (I)

36

Domando al caballo desbocado: gobierno y gestión de la IA y sus riesgos (II)

40

Domando al caballo desbocado: gobierno y gestión de la IA y sus riesgos (y III)

44

Evaluando el factor humano: Human Risk Management

48

El Liderazgo de la Mujer en la Normalización

NORMALIZACIÓN

52

Cierre de Temporada 2026 Revistas “Tecnología & Sentido Común” y “Stakeholders.news”

EVENTOS

56

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 Medio de Comunicación 2018 de la Asociación Profesional Española de Privacidad



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

a pep | Asociación Profesional Española de Privacidad

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.

 COLEGIO OFICIAL DE INGENIERÍA INFORMÁTICA DE LA COMUNITAT VALENCIANA

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.

eset

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.

AVIS@
ASOCIACIÓN VALENCIANA DE INFORMÁTICA SANITARIA

ESTE MES TE RECOMIENDO LEER...

por Javier Peris

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

Prólogo de:
**Luis
Morán**



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



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.

available at
amazon

No al tocomucho: estrategias de prevención de estafas on line

En anteriores artículos hemos venido lanzando advertencias sobre la proliferación de estafas on line, o que se inician on line, y la ayuda que la Inteligencia Artificial Generativa presta a los delincuentes para facilitar sus crímenes. En este artículo, el primero de la 11ª temporada de nuestra revista, intentaremos dar algunas pistas para evitar caer en este tipo de situaciones.

En la actualidad, el aumento de las interacciones *online* ha traído consigo una preocupante proliferación de estafas a través de medios digitales. En TYSC hemos venido advirtiendo de los riesgos, y de los efectos que determinadas situaciones tienen a nivel económico y psicológico en los afectados. Tanto a nivel personal como profesional, las amenazas cibernéticas se han diversificado y sofisticado, lo que exige una respuesta igualmente compleja y estratégica. Prevenir caer en estafas *online* no es solo una cuestión de tecnología, sino más bien de concienciación, formación y cultura de seguridad, como no se cansan en repetir en España las Fuerzas y Cuerpos de Seguridad del Estado, el CCN o el INCIBE. Tampoco hay que olvidar que, si bien todos estamos expuestos a este tipo de comportamientos delictivos, los más mayores y los más jóvenes de nuestra sociedad son objetivos claros de los ciberdelincuentes. Es vital, por tanto, promover campañas de educación digital, ofrecer soporte familiar y establecer controles parentales o comunitarios que protejan a estas poblaciones.

Pero antes de poder prevenir, es esencial entender las amenazas. Ya hemos hablado aquí de que las estafas *online* pueden adoptar diversas formas: *phishing*, *smishing* (phishing por SMS), *vishing* (por voz), *qrishing* (usando códigos QR), fraudes en redes sociales, estafas de soporte técnico, fraudes de inversión, y

manipulaciones emocionales como las estafas amorosas. En el ámbito laboral, se suman a éstos ataques como el *Business Email Compromise (BEC)*, el *ransomware* dirigido y el fraude del CEO. A nivel personal, requerimos una educación continua sobre ciberseguridad. Mantenerse informado sobre las técnicas actuales de los estafadores es fundamental. Seguir a fuentes confiables como agencias gubernamentales de ciberseguridad o medios especializados ayuda a estar al tanto de las amenazas emergentes. Pero seamos realistas: ¿nuestra tía Enriqueta va a seguir en redes sociales a los gurús de este tema? Hace falta que estas cuestiones se traten más en los medios de comunicación de masas, como la radio o la TV.

También es básica la verificación de la autenticidad de los mensajes que recibimos. Nunca se debe hacer clic en enlaces de correos o mensajes sospechosos. Y no sólo porque lo sea el emisor, sino también por su contenido. ¿Qué amigo suyo le va a pedir dinero por Whatsapp, por ejemplo? No hace mucho recomendábamos verificar la dirección del remitente, buscar errores ortográficos o de formato, y contactar directamente con la entidad que supuestamente envía el mensaje. Pero hoy en día, y debido al uso de IA Generativa, los mensajes fraudulentos son perfectos, y es muy complicado diferenciar los maliciosos de los legítimos sin conocimientos técnicos.



CONTINÚA EN
PRÓXIMA PÁGINA





También solemos recomendar usar contraseñas únicas y complejas para cada servicio, junto con un gestor de contraseñas, y habilitar la autenticación multifactor cuando sea posible, porque dificulta el acceso a cuentas incluso si una contraseña se ve comprometida. Igualmente, conviene evitar redes Wi-Fi públicas (hoteles, aeropuertos, cafeterías, etc.) sin utilizar una red privada virtual (VPN) para cifrar el tráfico de datos, porque eso nos protege frente a la interceptación de información.

También comentamos en una serie de artículos en TYSC sobre la ingeniería social la importancia de desconfiar ante lo urgente o emocional. Los estafadores suelen apelar a la urgencia o las emociones de sus potenciales víctimas. Mensajes que piden actuar rápido, que generan miedo o que apelan a la compasión deben ser tratados con escepticismo.

Con el uso de las redes sociales, nosotros mismos nos ponemos la soga al cuello. Limitar la información que se comparte en redes sociales puede prevenir que estafadores usen esos datos para realizar ataques dirigidos contra nosotros o contra nuestros conocidos o familiares. Téngase en cuenta que hoy en día puede clonarse fácilmente la voz de cualquiera, y que se pueda falsear cualquier mensaje. Y con un poco de tiempo disponible, también la imagen en video puede ser generada artificialmente. Es el potencial adiós a las pruebas judiciales basadas en audio o video. A este respecto, una recomendación que puede sonar a antigua es el establecimiento de una contraseña, o un santo y seña, con nuestros allegados, de manera que si detectamos algún comportamiento extraño en nuestra interacción digital con ellos, podamos recurrir a esa palabra o frase compartida para asegurarnos de que realmente es esa persona con quien interactuamos, y no un ciberdelincuente.

Si se sospecha de que se está siendo víctima de una intento de estafa, o ésta ya se ha consumado, es importante reportarla a las autoridades pertinentes, como la Policía Nacional, la Guardia Civil, o el INCIBE, en España, o instituciones equivalentes en otros países.

En el entorno laboral, es crítico impulsar la cultura de seguridad. Para ello, la concienciación de los empleados es la primera línea de defensa. Programas de formación periódicos, simulacros de

phishing y sesiones informativas ayudan a desarrollar una cultura de seguridad. También es muy importante disponer de políticas claras de ciberseguridad, y comunicarlas: sobre el uso de dispositivos, sobre los intercambios de información, sobre la gestión de contraseñas y sobre las autorizaciones que se requieren en cada servicio. Esto debería minimizar la posibilidad de errores humanos.

Una de las formas en que en los entornos empresariales se materializan las estafas es mediante el engaño a quienes efectúan pagos o tienen la capacidad de ordenar transferencias bancarias. Por ello, es importante disponer de procedimientos claros, y adherirse a ellos siempre, para este tipo de operaciones, incluidas las de establecimiento de las formas de pago de facturas. Hay que tener en cuenta que no se puede cambiar la cuenta en la que pagamos a un determinado proveedor simplemente porque se recibe un supuesto correo de su departamento administrativo. Es necesario corroborar esa información por otros medios, y nunca respondiendo a ese correo electrónico.

Igualmente, hay que evitar el uso de servicios no autorizados para compartir archivos o información sensible, y fomentar el uso de plataformas corporativas seguras para la transmisión de esa información.

Por supuesto, las empresas harían bien en auditar a sus proveedores tecnológicos y exigirles niveles adecuados de seguridad. Muchas brechas ocurren a través de terceros, como también hemos resaltado en artículos anteriores en esta sección.

Tanto en el hogar como en la empresa, existen herramientas que, bien utilizados y configurados, pueden servir como escudos frente a estafas:

- Filtros *antispam* y *antiphishing*.
- Gestores de contraseñas.
- Redes privadas virtuales (VPN).
- Aplicaciones de control parental.
- Aplicaciones de autenticación de doble factor.

Comprender cómo operan los estafadores, qué tácticas utilizan y por qué muchas personas caen en sus trampas es inexcusable. Suelen explotar la confianza, el miedo, la codicia o el amor. Del lado del usuario, la sobrecarga de información y la falta de atención pueden hacer que se bajen las defensas. Por eso, es fundamental fomentar una actitud de pensamiento crítico, pausa y validación. También analizar incidentes reales de estafa *online* ayuda a comprender cómo ocurren y qué se puede mejorar. Casos como el ataque a Twitter en 2020 mediante ingeniería social, o las estafas masivas por SMS en bancos europeos, son lecciones valiosas.

En conclusión, la prevención de estafas online es un reto complejo que requiere acción coordinada entre tecnología, formación, represión policial, legislación y cultura digital. Tanto a nivel personal como laboral, la clave está en anticiparse, educarse y actuar con criterio y sentido común. La tecnología nos conecta y potencia, pero también nos expone. Nuestra responsabilidad es protegernos y proteger a quienes nos rodean, construyendo un entorno digital más seguro, consciente y resiliente.

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



**Curso de
Certificación en:**

**Gobierno del
Tiempo y
Gestión de la
Productividad**

**Time Slot
Governance
Yellow Belt**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tasas Examen: Incluidas
- Basado en el TSG4® Yellow Book
- 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>



21001:2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**

La seguridad de la información empieza por nosotros: hábitos, cultura y conciencia (I)

¿Por qué escribimos estos artículos sobre las problemáticas de seguridad de la información en el entorno digital? Pues sencillamente porque el componente humano es uno de los factores de mayor riesgo en las organizaciones en este ámbito. En esta serie de artículos analizaremos la cuestión y los enfoques que pueden ayudarnos a reducir ese riesgo.

PRIMERA PARTE: EL FACTOR HUMANO EN LA SEGURIDAD DIGITAL

Cuando escuchamos hablar de ciberseguridad, muchos piensan en algoritmos complejos, en ciberdelincuentes expertos capaces de penetrar sistemas con una sudadera con capucha, un teclado y una pantalla llena de extraños códigos, o en grandes compañías que invierten fortunas en blindar sus sistemas. El cine y la cultura urbana han hecho mucho para que esa sea la imagen percibida del sector. Sin embargo, la realidad muestra una cara mucho más sencilla y preocupante de los problemas que la seguridad de la información afronta en este entorno digital: la inmensa mayoría de incidentes no se deben a fallos técnicos imposibles de prever, sino a un "despiste" humano, provocado o no por malhechores con técnicas sobre las que ya hemos escrito en Tecnología y Sentido Común con anterioridad.

Según diversos informes internacionales, entre el 90 % y el 95 % de los incidentes de seguridad tienen su origen en errores cometidos por las personas. Ojo, errores en muchas ocasiones promovidos o provocados por todo es mundillo al que solemos referirnos como ciberdelincuentes.

Pero este dato nos recuerda algo esencial: el verdadero talón de Aquiles de la seguridad digital casi nunca es la tecnología, sino **el comportamiento humano**. Porque aunque el problema sea tecnológico, como es el caso de las vulnerabilidades de software, éstas se han creado por errores humanos de programación, por no tener seguridad desde el diseño de los productos, porque los administradores de los sistemas no parchean con la suficiente celeridad, etc.

Un simple clic impulsivo puede desencadenar una cadena de problemas. Pensemos en situaciones como estas:

- Contraseñas débiles o repetidas:** la comodidad de usar "123456" o la misma clave en todas las cuentas facilita el acceso a los atacantes. Una vez vulnerada la contraseña común, los ciberdelicuentes tratan de probar el mismo par usuario+contraseña en otros servicios. De ahí uno de los riesgos de las filtraciones de datos masivas, de las que también hemos escrito aquí.

•**Correos fraudulentos:** abrir un archivo adjunto enviado por un supuesto compañero de trabajo o conocido puede introducir un virus en toda la red corporativa. Esta amenaza se ve materializada a diario, con miles de infecciones por ransomware, que están provocando miles de millones de euros en pérdidas a las empresas y administraciones públicas de todo el planeta.

•**Exceso de confianza en redes sociales:** compartir información aparentemente inocente, como “estoy de viaje en Kuala Lumpur”, puede dar pistas a delincuentes sobre vulnerabilidades físicas.



CONTINÚA EN
PRÓXIMA PÁGINA





O puede dar la oportunidad para que, sin estar nosotros presentes, alguien trate de hacerse pasar por nosotros para realizar alguna actividad maliciosa en nuestro entorno.

Por no hablar de que si se relaciona nuestra red social con alguna filtración de datos donde aparezca nuestra dirección física real, un delincuente “de los de toda la vida” podría vaciarnos la casa aprovechando nuestra ausencia.

•**Malas prácticas físicas:** es muy clásico quejarnos de que hay quien apunta claves en notas adhesivas o libretitas que deja al lado del ordenador; o dejar ordenadores sin bloquear en espacios públicos, o con contraseñas recordadas en el navegador; o tirar documentos en formato papel sensibles a la basura sin destruirlos. Todo ello son acciones con un riesgo inherente y que debemos extirpar de raíz de nuestras organizaciones, porque, además, pueden suponer incluso sanciones económicas por incumplir ciertas normativas generales o sectoriales.

Lo curioso es que muchas de estas conductas **no nacen de la ignorancia, sino de la costumbre**. Sabemos que deberíamos ser más cuidadosos, pero el día a día, las prisas o la sensación de “a mí no me va a pasar” nos empujan a atajos inseguros. Los delincuentes digitales conocen bien cómo funciona nuestra mente y aprovechan sus debilidades. Entre los factores más comunes destacan:

•**El sesgo de urgencia:** los mensajes que exigen actuar “ahora mismo” activan nuestra respuesta automática y reducen nuestra capacidad crítica.

•**La autoridad:** si el correo parece venir de un jefe, una entidad bancaria o una institución oficial, tendemos a obedecer sin cuestionar.

•**La aversión a la pérdida:** tememos más perder algo que ya tenemos que no ganar algo nuevo. Por eso funcionan mensajes como “su cuenta será suspendida si no...”.

•**El exceso de confianza:** creemos que reconocemos los engaños y que a nosotros no nos van a estafar, lo que nos hace bajar la guardia.

En todos estos casos, ejemplos paradigmáticos de ataques de ingeniería social, lo conveniente es pararse, analizar, reflexionar, comprobar, contar hasta cien, y luego actuar. No reaccione de manera inmediata ni irreflexiva. En ediciones anteriores de la revista también hemos analizado estas debilidades psicológicas y cómo afrontarlas en un entorno corporativo y personal. Estos sesgos cognitivos, estudiados por la psicología, son los mismos que determinan muchos de nuestros hábitos de consumo o de comportamiento social. En el ámbito de la seguridad, sin embargo, pueden tener consecuencias devastadoras, como ya sabemos.

Sin embargo, no se trata de señalar con el dedo a los usuarios. Culpar a las personas de sus errores solo genera miedo o rechazo, pero no cambia conductas. La solución está en crear **una cultura de la seguridad compartida**, un entorno donde las buenas prácticas se conviertan en algo natural, sencillo y repetido. Del mismo modo que aprendemos desde pequeños a lavarnos las manos para prevenir enfermedades, podemos incorporar **rutinas digitales saludables** que nos protejan sin necesidad de conocimientos técnicos avanzados.

En los próximos artículos de esta serie analizaremos cómo lograr precisamente incorporar esas rutinas y, sobre todo, como intentar que esa cultura de la seguridad sea global.

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



**Curso de
Certificación en:**
**Ejecución
Estratégica y
Cambio
Organizacional
P4MGO!®
Essentials**

Docente:
Javier Peris

- Formato: Grabado
- Disponibilidad: Inmediata
- Carga Lectiva: 20 Horas
- Importe del Curso: 395€
- Tasas Examen: Inclúas
- A tu ritmo
- En tu horario
- Desde donde te encuentres
- Con toda comodidad

MidMgmt®

MPPM®

MGEIT®

eGob®

Disponibilidad Inmediata

Solicita tu admisión en:



+ 34 96 109 44 44

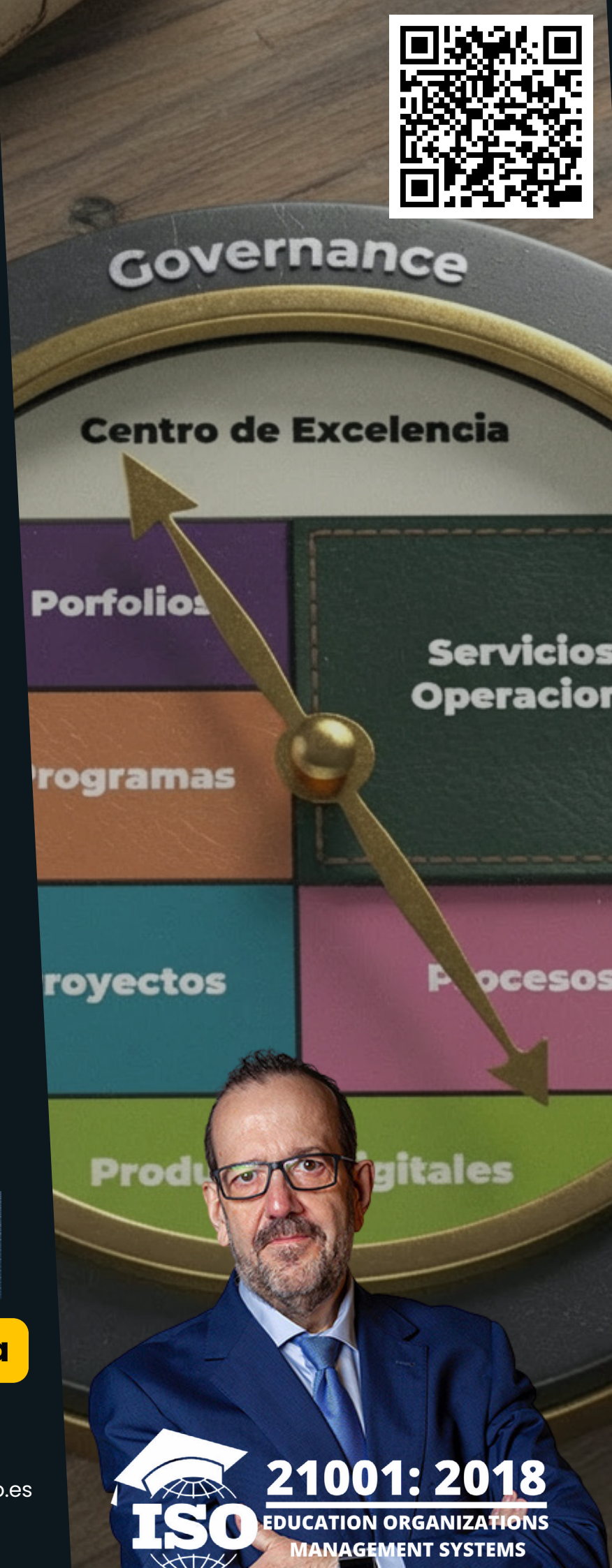
admisiones@escueladegobierno.es

<https://escueladegobierno.es>



21001:2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**



La seguridad de la información empieza por nosotros: hábitos, cultura y conciencia (II)

En el artículo del mes pasado analizamos someramente los riesgos asociados al factor humano en la seguridad de la información. En el artículo de este mes plantearemos cómo lograr que las rutinas de higiene digital sean una realidad en nuestros entornos.

SEGUNDA PARTE: ESTRATEGIAS PARA FOMENTAR BUENOS HÁBITOS

Como vimos en el artículo del mes pasado, las personas tenemos una serie de debilidades psicológicas que los ciberdelincuentes saben aprovechar para convencernos de que llevemos a cabo ciertas acciones que, en realidad, son perjudiciales para nosotros. Son las mismas vulnerabilidades o características que aprovechan las campañas de marketing o los *influencers* de todo pelaje y motivación. De ahí la necesidad de reconocer esas debilidades y de convertir en hábitos ciertas rutinas de higiene digital.

La pregunta clave es: ¿cómo conseguimos que las personas adopten hábitos seguros en su vida digital? La respuesta no puede sino combinar educación, diseño inteligente de sistemas y comprensión de cómo funciona la mente humana. En formación, se aduce que las personas, ante un nuevo conocimiento o habilidad, pasamos por cuatro estados diferentes:

- **Incompetencia Inconsciente:** no sabemos nada sobre la cuestión, porque ni siquiera sabemos que existe.
- **Incompetencia Consciente:** sabemos que no sabemos nada sobre la cuestión, y estamos quizá en las primeras etapas de la formación al respecto.

•Competencia Consciente: ya nos hemos formado sobre el tema en cuestión, pero para aplicarlo hemos de estar continuamente alerta y concentrados en ello.

•Competencia Inconsciente: conocemos el tema en cuestión y podemos llevarlo a cabo casi sin pensar en ello.

El ejemplo paradigmático de este último estado es cuando llevamos muchos años conduciendo. No nos paramos a pensar en que hay que pisar el embrague antes de cambiar de marcha, o que a partir de unas ciertas revoluciones hemos de pasar a una marcha más larga. Nuestro conocimiento y nuestra experiencia ha convertido conducir en un **hábito**, y nuestro cerebro lo lleva a cabo con una carga mental mínima.

El psicólogo Charles Duhigg popularizó la idea de que los hábitos se sostienen en un “bucle” (*Habit Loop*) compuesto por tres elementos: **señal, rutina y recompensa**.

•Señal: algo que activa el comportamiento. Por ejemplo, un correo con un enlace puede activar la rutina de clicar en él.

•Rutina: la acción que seguimos automáticamente. Siguiendo con el ejemplo, tras la señal, clicamos en el enlace sin fijarnos ni a dónde apunta realmente, ni si de verdad necesitamos acceder a esa información.



CONTINÚA EN
PRÓXIMA PÁGINA





•Recompensa: la satisfacción inmediata tras la rutina. En nuestro ejemplo, nuestra curiosidad sobre la información que pueda haber en el enlace queda saciada.

En seguridad de la información, este bucle juega en nuestra contra, porque los hábitos de todas las personas que interactúan en el mundo digital se han venido creando desde bien jóvenes, en muchos casos.

Para cambiar ese bucle, necesitamos **rediseñar las señales** y por supuesto, **ofrecer recompensas positivas** a las conductas seguras. Por ejemplo, al recibir un correo sospechoso (Señal), nos detenemos a verificar el remitente, el asunto y los enlaces (nueva Rutina), y con ello obtenemos la tranquilidad de evitar un posible fraude y el reconocimiento, incluso social, de haber actuado de forma responsable (nueva Recompensa).

Este enfoque muestra que la seguridad no es cuestión de memorizar normas, sino de **entrenar rutinas** hasta que se vuelven automáticas. Los **nudges** son pequeños estímulos que orientan hacia conductas seguras sin imponerlas. Son ejemplos habituales los navegadores que bloquean páginas web sospechosas y muestran un aviso en rojo; las plataformas que recomiendan contraseñas largas y generan combinaciones seguras; o los mensajes emergentes que preguntan “¿Está seguro de compartir esta información en público?”. Lo importante es que actúan en el momento exacto en que se necesita la decisión correcta, reduciendo la carga mental del usuario.

En muchas organizaciones hace tiempo que se plantean iniciativas de concienciación a sus miembros o empleados. Sin embargo, los programas de concienciación tradicionales suelen ser monótonos y poco eficaces. Por ello, cada vez más organizaciones apuestan por la **gamificación**: simulaciones de ataques de phishing para que los empleados practiquen en reconocerlos, concursos con premios simbólicos por detectar fraudes, o incluso juegos de *escape room* digitales donde la seguridad de la información es el reto principal.

Estas dinámicas convierten la seguridad en algo cercano, divertido y memorable, y sobre todo, apoyan la creación de nuevos hábitos siguiendo el “ciclo de los hábitos” de Duhigg.

Para finalizar el artículo de este mes, citaremos algunos ejemplos prácticos de hábitos que cualquier persona puede incorporar en su vida digital, igual que en su vida física física han incorporado el hábito de lavarse los dientes o cerrar la puerta de su casa al salir:

- Usar gestores de contraseñas: para no repetir claves y poder usar combinaciones robustas sin tener que recordarlas.

- Autenticación multifactor: si el servicio la soporta, y aunque a veces resulte molesta, es una de las barreras más efectivas frente a ataques de fuerza bruta o robo de contraseñas.

- Actualizar dispositivos y aplicaciones con regularidad: muchas brechas de datos se producen porque no instalamos parches de seguridad estando disponibles.

- Desconfiar de lo demasiado bueno para ser cierto: sorteos, premios o herencias sorpresa siguen siendo anzuelos frecuentes y, por lo que dicen los datos, muy efectivos.

Cuando estos comportamientos se repiten y se refuerzan con señales y recompensas, se integran en el bucle de los hábitos y dejan de ser un esfuerzo consciente, que es lo que buscamos: incorporar la seguridad de la información a nuestra vida de la forma que menos esfuerzo posible requiera.

En el próximo, y último, artículo de esta serie analizaremos cómo transitar hacia una cultura de la seguridad global.

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



**Curso de
Certificación en:**

**Gestión de
Proyectos**

**P4MGO! PjM
Project
Management**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tasas Examen: Incluidas
- Basado en el P4MGO! PjM BoK
- 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>



21001:2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**

La seguridad de la información empieza por nosotros: hábitos, cultura y conciencia (y III)

En los dos artículos anteriores de esta serie analizamos someramente los riesgos asociados al factor humano en la seguridad de la información, y cómo lograr que las rutinas de higiene digital sean una realidad en nuestros entornos a través de la creación de hábitos seguros. En este último artículo concluiremos la serie reflexionando sobre cómo lograr crear una cultura de seguridad compartida.

TERCERA PARTE: HACIA UNA CULTURA DE SEGURIDAD CENTRADA EN LAS PERSONAS

La evolución de las amenazas digitales parece no tener fin: *deepfakes* que imitan voces, fraudes mediante códigos QR, ataques a dispositivos domésticos conectados a internet, robos de identidad con inteligencia artificial, etc. En este escenario, es evidente que la tecnología sola no basta. La verdadera fortaleza reside en nuestra capacidad para crear una **comunidad consciente y entrenada**.

Cuando hablamos de ciberseguridad, es común pensar que la carga recae en gobiernos, empresas tecnológicas o especialistas en informática. Sin embargo, la experiencia demuestra que ningún sistema puede garantizar una protección total si los usuarios no adoptan comportamientos seguros. La seguridad digital, en este sentido, se parece mucho a la salud pública: el esfuerzo colectivo es tan importante como las medidas individuales.

Un ejemplo ilustrativo es el de las contraseñas filtradas en servicios populares. Aunque una plataforma pueda tener medidas de cifrado avanzadas, si un usuario reutiliza la misma contraseña en múltiples sitios, abre la puerta a que un solo ataque exponga toda su vida digital. Algo parecido ocurre con los correos de phishing: basta con que una persona dentro de una organización caiga en la trampa para comprometer toda la red.

La idea de **responsabilidad compartida** implica que cada acción, por insignificante que parezca, tiene un impacto real en la seguridad global. Bloquear el ordenador antes de levantarnos de la mesa en el trabajo no es solo una medida personal, también protege la información de toda la empresa. Avisar a un amigo de que un enlace que circula en WhatsApp es sospechoso ayuda a cortar la cadena de ataque antes de que se extienda. Incluso enseñar

a un familiar mayor a reconocer estafas telefónicas o digitales se convierte en un acto de seguridad comunitaria.

A medida que se extiende esta conciencia, se construye un tejido social más resistente. La seguridad, lejos de ser un asunto técnico reservado a unos pocos, se convierte en una práctica cultural que involucra a todos, un hábito a potenciar. Y como sucede con las normas de convivencia, la repetición y la presión social positiva hacen que las buenas prácticas terminen formando parte de lo cotidiano.

Durante mucho tiempo, los mensajes de concienciación en seguridad digital han recurrido al miedo como estrategia: “Si haces clic en este enlace, perderás tu dinero”, “Si usas una contraseña débil, te hackearán la cuenta”, “Si no actualizas tu sistema, te arriesgas a un virus devastador”... Aunque estas advertencias son ciertas, el exceso de dramatismo suele tener un efecto contraproducente. El miedo constante genera parálisis, rechazo y, en muchos casos, indiferencia. Cuando todo parece peligroso, las personas optan por no pensar demasiado en el problema.

Por eso, en los últimos años está ganando terreno un enfoque diferente: el de la **cultura de la confianza**. En lugar de subrayar solo las consecuencias negativas de un error, este enfoque pone en valor las capacidades de las personas, mostrando que todos podemos aprender y que las conductas seguras están al alcance de cualquiera. Por ejemplo, en vez de decir “si no activas el doble factor de autenticación te hackearán”, el mensaje puede ser “activando este paso extra, blindas tu cuenta como si añadiras una segunda cerradura a tu casa”.

La confianza también se construye con ejemplos positivos y con la demostración de que la seguridad puede ser sencilla. Mostrar a los usuarios que un gestor de contraseñas no es complicado, sino que facilita la vida, o que actualizar el móvil no requiere conocimientos técnicos, son formas de reforzar esta percepción. En este sentido, la comunicación clara y libre de tecnicismos, es fundamental.

Además, la cultura de la confianza fomenta un entorno en el que reportar errores o incidentes no se percibe como un fracaso, sino como una contribución. En las empresas, por ejemplo, cuando un empleado recibe un correo sospechoso y lo comunica de inmediato, está ayudando a proteger al resto. Si ese mismo empleado temiera ser castigado por haberlo abierto, lo más probable es que lo ocultara, lo que agravaría el riesgo.



CONTINÚA EN
PRÓXIMA PÁGINA

El objetivo es que las personas no se relacionen con la seguridad desde la ansiedad, sino desde la **confianza activa**: saber que cuentan con recursos, apoyo y soluciones prácticas. De este modo, la seguridad de la información se transforma en una aliada que empodera en lugar de atemorizar, y que refuerza la **resiliencia colectiva** frente a amenazas cada vez más sofisticadas.

Las próximas décadas traerán retos aún más complejos, pero también abrirán nuevas oportunidades para que la seguridad deje de ser vista como un terreno exclusivo de expertos y pase a formar parte de la vida cotidiana. En este camino, hay tres ejes fundamentales que marcarán la diferencia: los hábitos personales, la educación digital desde edades tempranas y la resiliencia colectiva.

Si en el siglo XX las escuelas enseñaron a los niños a lavarse las manos o a cepillarse los dientes como parte de la salud pública, en el siglo XXI la higiene digital será igual de esencial. Incluir contenidos de seguridad de la información en el currículo escolar no significa dar clases de programación avanzada, sino mostrar a los alumnos cómo funcionan las contraseñas, por qué no deben compartir ciertos datos en redes sociales o cómo identificar un mensaje sospechoso. Este aprendizaje temprano no solo protege a los menores, sino que también se traslada a sus familias: los niños pueden convertirse en embajadores de buenas prácticas en sus hogares, corrigiendo conductas inseguras de padres o abuelos. A largo plazo, una sociedad que interioriza la seguridad digital desde la infancia será mucho menos vulnerable a los engaños masivos.

De la misma manera que vemos en las carreteras carteles que recuerdan la importancia de ponerse el cinturón, o vemos en los hospitales mensajes sobre la vacunación o el tabaquismo, ya empieza a ser habitual encontrar campañas de concienciación sobre seguridad digital. Estos programas adoptan múltiples formas: anuncios en televisión, avisos en cajeros automáticos o en las aplicaciones bancarias, recordatorios en facturas de servicios básicos, o incluso mensajes en redes sociales. Lo importante es que la seguridad deje de ser percibida como un tema opcional o reservado a expertos, y pase a ser un valor cultural compartido y necesario. El reto está en hacer que el mensaje sea comprensible y útil para cualquier ciudadano, independientemente de su edad o nivel educativo.

Hoy en día, muchas aplicaciones y servicios exigen a los usuarios tomar decisiones técnicas que no siempre entienden: elegir la configuración de privacidad, decidir si actualizan o no, gestionar permisos de acceso a la cámara o el micrófono... En el futuro cercano, el diseño de las aplicaciones tenderá a ser más **seguro por defecto**. Esto significa que las configuraciones iniciales estarán orientadas a proteger al usuario, y a no exponer sus datos. Un ejemplo de este enfoque ya lo encontramos en los navegadores que bloquean descargas peligrosas sin necesidad de que el



usuario entienda qué es un archivo ejecutable. Cuanto más intuitivo y automatizado sea el diseño de seguridad, menos dependerá del conocimiento técnico individual y más protegida estará la comunidad en su conjunto.

El objetivo final no es blindar cada sistema, sino crear una sociedad capaz de responder con calma, criterio y responsabilidad a los desafíos digitales.

Las conclusiones que deberíamos extraer de esta serie de artículos son:

1. La seguridad de la información ya no puede entenderse como un problema técnico aislado: **es una cuestión humana y cultural**.
2. Los delincuentes explotan nuestras prisas, emociones y sesgos. Pero esos mismos mecanismos también pueden convertirse en aliados si los usamos para reforzar conductas positivas. Con hábitos entrenados, señales adecuadas y recompensas claras, cada uno de nosotros puede convertirse en la primera línea de defensa.
3. En definitiva, la seguridad de la información empieza por nosotros. Y si logramos que la cultura digital se base en la **confianza, la educación y la resiliencia**, no solo estaremos más protegidos, sino que viviremos en un entorno tecnológico más seguro para todos.

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



**Curso de
Certificación en:**

**Gestión de
Programas**

**P4MGO! PgM
Programme
Management**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tasas Examen: Incluidas
- Basado en el P4MGO! PgM BoK
- 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>



21001: 2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**

Aplicaciones móviles: cuando la falta de seguridad pone en riesgo nuestros datos (I)

La app “Tea” es un caso reciente que ilustra cómo una aplicación popular, pero sin suficientes medidas de protección, puede filtrar información íntima: desde selfies hasta documentos oficiales y mensajes privados fueron publicados online. Y es que muchas personas usan apps sin revisar las garantías de privacidad, por lo que comparten podría terminar expuesto si la seguridad es insuficiente.

PRIMERA PARTE: La cara oculta de las apps: ¿qué hay detrás de lo que instalamos?

En apenas una década, las aplicaciones móviles se han convertido en el centro de nuestra vida digital. Usamos apps para comunicarnos, comprar, gestionar nuestras finanzas, hacer deporte, reservar viajes, editar y guardar fotos, controlar nuestra salud, estudiar idiomas o, simplemente, entretenernos. Para muchas personas, el teléfono inteligente es una extensión de su identidad, y en él depositan información extremadamente sensible, casi sin darse cuenta.

Sin embargo, mientras disfrutamos de esa comodidad, rara vez pensamos en los riesgos que puede conllevar instalar una aplicación aparentemente inocente. La realidad es que el ecosistema de apps es tan amplio y diverso que las garantías de seguridad varían enormemente. Y aunque las tiendas oficiales realizan controles, estos no siempre detectan fallos de diseño, prácticas opacas de recopilación de datos o brechas que pueden exponer información personal sin que el usuario llegue a saberlo.

Muchas personas asumen que si una app está disponible en una tienda oficial, debe ser segura. Pero esto no es necesariamente cierto, como múltiples

ejemplos han demostrado. Sin ir más lejos, la app “Tea”, orientada a que las mujeres pudieran obtener consejo en aplicaciones de citas, sufrió en julio de 2025 una grave brecha de seguridad cuando se descubrió que una base de datos heredada, almacenada en un servicio externo, estaba mal configurada, lo que permitió el acceso no autorizado a un volumen enorme de datos personales. Entre lo filtrado había unos 72.000 archivos de imagen, incluyendo alrededor de 13.000 selfies y fotografías de documentos de identidad que las usuarias habían enviado como parte del proceso de verificación. También se accedió a otras 59.000 imágenes correspondientes a publicaciones, comentarios o mensajes privados dentro de la app.

Pero la cosa no quedó ahí: poco después se supo que la filtración afectaba también a las conversaciones privadas. Un investigador de seguridad externo reveló que alrededor de 1,1 millones de mensajes directos (Dms), muchos tratando temas sensibles como abortos, infidelidades, relaciones íntimas o datos de contacto, habían quedado expuestos. Ante la gravedad del asunto, Tea desactivó su función de mensajería mientras investigaba el alcance.



CONTINÚA EN
PRÓXIMA PÁGINA





Bien conocido es que los desarrolladores pueden cometer errores, adoptar prácticas de programación poco cuidadas, o no actualizar sus sistemas con suficiente rapidez. Estas carencias pueden generar vulnerabilidades explotables o provocar filtraciones por descuido, aspectos sobre los que hemos escrito en esta sección de Tecnología y Sentido Común.

Además, estamos ante una peculiaridad específica con las apps, ya que el mercado de aplicaciones móviles es extremadamente competitivo, con miles de desarrolladores independientes creando productos con recursos limitados, lo cual puede llevar a que la seguridad quede en un segundo plano frente a la funcionalidad o la rapidez de lanzamiento.

Estas inseguridades en las apps pueden incluir, de forma más o menos habitual:

- **Transmisión de datos sin cifrar**, lo que permite que información sensible pueda ser interceptada en redes públicas.
- **Permisos excesivos** que la app no necesita para funcionar pero que le permiten acceder al almacenamiento de fotos o documentos, contactos, ubicación o micrófono.
- **Almacenamiento inseguro** de archivos o contraseñas dentro del dispositivo.
- **Código desactualizado** que utiliza librerías antiguas con fallos conocidos.
- **Falta de controles internos** para verificar que los datos no quedan expuestos accidentalmente.

Estos fallos tienen repercusiones directas en la vida de los usuarios, como ya se ha ejemplificado.

A esto se suma otra dimensión menos visible: muchas aplicaciones gratuitas monetizan la información que recopilan. Rastreo de ubicación, hábitos de uso, contactos, identificadores del dispositivo, patrones de navegación, etc. Todos estos datos constituyen un valioso recurso comercial, y el problema no es únicamente que recojan esos datos, sino que **no siempre explican claramente para qué los usan**, cómo los almacenan o con quién los comparten. Y cuando un servicio acumula más información de la que controla adecuadamente, el riesgo de fugas aumenta.

El usuario medio acepta las condiciones sin leerlas, pulsa "Aceptar" y continúa. Pero, en ocasiones, ese simple clic significa abrir la puerta a un seguimiento constante y a una exposición innecesaria.

Muchos usuarios sienten que tienen cierto dominio de su privacidad, y suelen usar frases como "yo no publico nada importante" o "solo uso apps conocidas".

Sin embargo, la información expuesta no siempre es consciente. Datos aparentemente irrelevantes, como cada cuánto abrimos una aplicación, qué lugares visitamos, con quién interactuamos o qué horario de actividad tenemos, pueden formar perfiles extremadamente precisos.

En un mundo donde la vida se digitaliza rápidamente, comprender los riesgos de las apps inseguras no es una cuestión técnica: es una necesidad básica de autoprotección digital. Y en los próximos números de Tecnología y Sentido Común exploraremos en mayor profundidad esta situación.

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



**Curso de
Certificación en:**

**Gestión por
Procesos de
Negocio**

**P4MGO! BPM
Business
Process
Management**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tasas Examen: Incluidas
- Basado en el P4MGO! BPM BoK
- A tu ritmo con toda comodidad

MidMgmt®

MPPM®

MGEIT®

eGob®

Tutorías en Directo

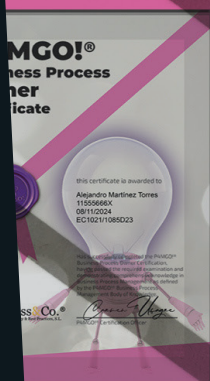
Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>



21001:2018
EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS

Aplicaciones móviles: cuando la falta de seguridad pone en riesgo nuestros datos (I)

En esta segunda parte de nuestro artículo sobre las apps móviles y su seguridad, entraremos en mayor detalle en cómo se producen esas inseguridades, y las cuestiones a las que debemos prestar atención durante la selección, instalación o uso de las mismas.

SEGUNDA PARTE: Cómo y por qué las apps inseguras exponen datos personales

Después de entender el contexto general, como hicimos en el artículo del mes pasado de Tecnología y Sentido Común, es importante profundizar en los mecanismos que hacen que una app pueda convertirse en una amenaza para nuestra privacidad o seguridad. Ojo, que no estamos hablando de aplicaciones directamente maliciosas, sino de aplicaciones legítimas cuyo funcionamiento interno puede dar lugar a desagradables sorpresas. Aunque el funcionamiento interno de las aplicaciones puede parecer complejo, los riesgos pueden explicarse de forma sencilla y accesible.

En muchas aplicaciones, el primer punto crítico aparece al instalarla: la solicitud de permisos. Por ejemplo: ¿Por qué una app para editar fotos necesita leer nuestros contactos? ¿Por qué un juego de rompecabezas pide acceso a la ubicación en tiempo real? ¿Por qué una app de linterna solicita permiso para grabar audio?



CONTINÚA EN
PRÓXIMA PÁGINA



Aunque pueda parecer absurdo, estas prácticas son habituales, y muchas personas ni siquiera verifican lo que la app les está exigiendo. Algunos permisos se utilizan para mejorar la publicidad dirigida; otros, para vender datos agregados a terceros; y otros, simplemente, son restos de un diseño deficiente en el que nadie revisó qué era realmente necesario.

Cuando un usuario otorga permisos excesivos, la aplicación puede:

- identificar localizaciones precisas a lo largo del día,
- analizar rutinas y desplazamientos,
- acceder a imágenes privadas,
- leer contactos o información de otros servicios,
- o activar sensores como el micrófono o la cámara.

Esto no significa que todas las apps realicen espionaje activo, pero **sí que tienen la capacidad técnica de hacerlo** si el desarrollador, un atacante o un error lo permite.

Otro de los focos de riesgo se encuentra en el almacenamiento. Una app puede recopilar datos legítimos, pero almacenarlos en carpetas mal protegidas. En otros casos, las contraseñas se guardan como texto plano o los tokens de autenticación se escriben en un archivo accesible a otras aplicaciones. Para un atacante con acceso físico o remoto, esto supone una puerta abierta a esas aplicaciones mal configuradas o desarrolladas.

Además, muchas aplicaciones dejan archivos temporales sin cifrar, como fotos procesadas, documentos descargados, registros de actividad, o copias de seguridad incompletas. Y la "basura digital", de la misma forma que en su día lo era la basura física, puede convertirse en un auténtico tesoro para quien busque información confidencial.

Nuestro tercer foco de riesgo lo encontramos en las comunicaciones. Cuando abrimos una app de mensajería, de un banco o de un servicio de compras, asumimos que la información viaja cifrada, pero no siempre es así. Algunas aplicaciones usan versiones antiguas de protocolos seguros, envían datos sensibles sin un algoritmo de cifrado adecuado, o combinan elementos cifrados con elementos no protegidos.

El resultado es que si nos conectamos a una red WiFi pública, cualquier persona con herramientas básicas podría interceptar información potencialmente sensible, como nombres, emails o incluso contraseñas, si estamos usando esas aplicaciones que no cifran completamente sus comunicaciones.

La cuarta pata de la inseguridad de las aplicaciones móviles está en la Nube. Muchas apps almacenan datos en servidores externos del fabricante de las mismas. Si esos servidores están mal configurados, tienen vulnerabilidades en su software, o son accesibles sin autenticación adecuada, la información puede quedar expuesta. No se necesita un "gran hackeo"; basta con un enlace mal protegido o una



base de datos sin contraseña y la información estará en manos de quien no debe.

En 2021 los investigadores de Check Point Research revelaron que más de 100 millones de usuarios de Android habían visto expuestos sus datos por culpa de malas configuraciones en servicios en la nube usados por sus apps. Concretamente, en 23 aplicaciones analizadas, algunas con millones de descargas, se detectaron bases de datos públicas, sin los controles de autenticación adecuados.

Esto permitió que cualquiera, conociendo la URL correcta, accediera a información personal sensible: correos electrónicos, contraseñas, geolocalizaciones, identificadores de dispositivos, chats privados, e incluso detalles de pagos.

Entre las apps afectadas había desde herramientas de diseño de logos, o apps de contabilidad, hasta apps de transporte o entretenimiento. Este escándalo demostró que el uso de la nube, y en particular de servicios populares como bases de datos en tiempo real o almacenamiento en nube, no garantiza por sí solo la seguridad: la configuración correcta y consciente es fundamental.

Finalmente, una app puede ser segura, pero si usa herramientas de terceros que no lo son, podemos sufrir impactos inesperados. Es lo que se suele denominar **cadena de suministro**. Servicios de publicidad, librerías de análisis, módulos de ubicación, motores de reconocimiento, o SDKs incluidos por comodidad, pueden recopilar información adicional sin que el desarrollador principal sea plenamente consciente. Y si son troyanizados por ciberdelincuentes, el éxito en su afán de robo de información está garantizado.

Debido a las cadenas de dependencias que puede contener una sola app, los datos del usuario pasan por múltiples manos sin control directo, y la complejidad del ecosistema hace difícil saber quién tiene acceso a qué.

El artículo del próximo mes, que da fin a esta serie, se centrará en explicar cómo podemos tratar de protegernos de esta problemática, y cómo incorporar a nuestra cultura de la protección digital el uso de apps móviles.

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



Curso de Certificación en: Gobierno de la Inteligencia Artificial

ISO 38507 AI Governance Leader

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 15 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- 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>



21001:2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**



Aplicaciones móviles: cuando la falta de seguridad pone en riesgo nuestros datos (y III)

En esta tercera parte de nuestro artículo dedicado a la seguridad de las aplicaciones móviles, y tras analizar las inseguridades que pueden incluir, nos centraremos en cómo deberán ser aplicaciones seguras y cómo debemos integrarlas correctamente en nuestra cultura de protección digital.

TERCERA PARTE: El futuro de las apps seguras: hábitos, protección y cultura digital

Para afrontar este problema, no basta con regular o vigilar: también es necesario educar al usuario y promover buenas prácticas tanto en desarrolladores como en plataformas. La seguridad es un esfuerzo conjunto que se construye desde múltiples frentes, como no nos cansamos de repetir desde esta sección de la revista.

El primer paso hacia un uso más seguro es comprender que instalar una app equivale a confiarle parte de nuestra vida. Los usuarios pueden adoptar hábitos simples pero poderosos, que dificultarán algunos de los problemas que ya vimos en el artículo del mes pasado de esta serie:

- Revisar permisos antes de aceptarlos.
- Eliminar apps que no se usan.
- Preferir herramientas con buena reputación o que pasen auditorías públicas.
- Desactivar la ubicación de su terminal cuando no se esté usando.
- Comprobar si la aplicación ofrece opciones de privacidad extendidas.



CONTINÚA EN
PRÓXIMA PÁGINA



El objetivo no es desconfiar de todo, sino **elegir con criterio**.

Por otro lado, la seguridad en apps debería enseñarse igual que se enseñan normas básicas de salud o de circulación. Por ejemplo:

- En escuelas, mediante talleres sobre privacidad y protección de datos.
- En familias, enseñando a identificar apps sospechosas.
- En empresas, formando a empleados sobre riesgos de instalación indebida.

A medida que la sociedad desarrolle una correcta "higiene digital", disminuirá la posibilidad de caer en prácticas inseguras.

Pero claro, si las apps no se desarrollan correctamente, los usuarios poco podemos hacer, salvo no usarlas.

Por ello, cada vez más países promueven la filosofía de "seguridad desde el diseño", que es, por ejemplo, una base fundamental del Esquema Nacional de Seguridad de España. Esta aproximación implica que los desarrolladores deben incorporar determinadas medidas de protección desde el primer momento en que se plantea la aplicación, tales como:

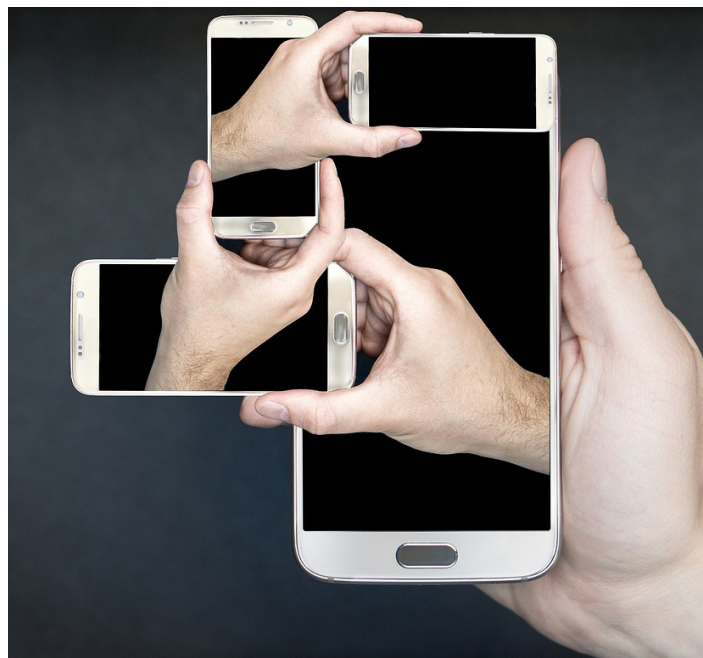
- uso de metodologías de desarrollo seguro,
- cifrado por defecto de datos en tránsito y en reposo,
- permisos estrictamente controlados y minimizados,
- revisiones periódicas del código, a ser posible, por terceros,
- no recopilación de datos innecesarios,
- anonimización cuando la identidad no sea necesaria,
- o políticas de almacenamiento seguro.

La idea es que la seguridad no debe ser un añadido, sino parte esencial del proceso de construcción, y una funcionalidad esencial de la aplicación.

Por supuesto, también puede haber un frente legal para resolver algunos de los problemas citados.

Las leyes de privacidad y protección de datos están avanzando en todos los países y áreas económicas, junto con iniciativas para lograr una mejor soberanía tecnológica. Por ello, en el futuro veremos:

- exigencias más estrictas para el uso de datos sensibles,
- sanciones por almacenamiento inseguro,
- prohibición de prácticas opacas en apps orientadas al público infantil,
- y auditorías obligatorias en aplicaciones de alto riesgo.



Es un camino lento, pero indispensable para equilibrar el poder entre usuarios y desarrolladores, aunque quizá suponga el fin de las apps gratuitas, porque, lógicamente, de algún sitio ha de salir el dinero para el desarrollo y mantenimiento del producto.

En última instancia, tanto empresas como usuarios buscan lo mismo: herramientas útiles y seguras. Por ello es necesario crear una cultura de confianza, que implique que:

- las apps expliquen de forma sencilla por qué piden permisos,
- los desarrolladores comuniquen con claridad sus políticas,
- las plataformas verifiquen con rigor la seguridad,
- y los usuarios participen activamente en la denuncia de apps sospechosas.

Cuando la tecnología se basa en la transparencia, el ecosistema es más seguro para todos.

En conclusión, vivimos rodeados de aplicaciones que facilitan nuestro día a día, pero esa comodidad tiene un coste si no existe una cultura de seguridad adecuada.

En esta serie de artículos hemos visto que las apps inseguras pueden exponer documentos, fotos, mensajes, ubicaciones, hábitos e incluso información financiera. Afortunadamente, la solución no pasa por renunciar a la tecnología, sino por usarla con conciencia: ser selectivos, informarnos, cuestionar los permisos y exigir buenas prácticas.

La seguridad no es solo un problema técnico: es un valor social y cultural que debemos construir colectivamente.

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



**Curso de
Certificación en:**

**Gestión de la
Inteligencia
Artificial**

**ISO 42001
AI Management
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: 695,00 €
- 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>



21001:2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**

Domando al caballo desbocado: gobierno y gestión de la IA y sus riesgos (I)

La Inteligencia Artificial ya ha pasado su etapa de hype y se ha convertido en un elemento a tener muy en cuenta en muchos sectores y ámbitos de actividad. Sin embargo, se detecta claramente un afán por glosar sus funcionalidades y ventajas, obviando que, como toda tecnología, debe ser adecuadamente gestionada y gobernada. En esta serie de artículos profundizaremos en el tema, comenzando en este número con los estándares que pueden o deben servirnos de guía para ello.

Parte 1: Gobernar la inteligencia artificial: por qué los estándares importan

Durante décadas, la inteligencia artificial fue percibida como una tecnología lejana, propia de laboratorios de investigación, universidades o grandes empresas tecnológicas. Hoy, sin embargo, la IA forma parte de la vida cotidiana de millones de personas. Interactuamos con sistemas inteligentes cuando usamos buscadores, recibimos recomendaciones en plataformas digitales, hablamos con asistentes virtuales, solicitamos un crédito, accedemos a un servicio público o incluso cuando se filtran currículos en procesos de selección.

Este cambio de escala ha sido rápido y profundo. En muy poco tiempo, los sistemas de IA han pasado de ser herramientas experimentales a **infraestructuras críticas de decisión**, capaces de influir en oportunidades laborales, en acceso a servicios, en diagnósticos médicos o en la información que consumimos a diario. Y precisamente por esa capacidad de influencia surge una pregunta clave: **¿Cómo nos aseguramos de que estos sistemas funcionan bien, de forma fiable, justa y responsable?**

La respuesta no está únicamente en mejorar los algoritmos o aumentar la potencia de cálculo. Está, sobre todo, en **cómo se gobiernan y gestionan** estos sistemas a lo largo de todo su ciclo de vida.



CONTINÚA EN
PRÓXIMA PÁGINA





controles, evaluaciones de riesgo, documentación y mejora continua.

Un sistema de IA puede ser técnicamente brillante, pero si no está bien gobernado y gestionado, su **calidad real**, entendida como fiabilidad, coherencia y adecuación al propósito, se resiente. En otras palabras: un buen algoritmo no garantiza un buen resultado si se utiliza mal, se entrena con datos inadecuados o se despliega sin supervisión. Cuando hablamos de “calidad” en inteligencia artificial, no nos referimos solo a métricas técnicas como precisión o velocidad, sino que incluye, entre otros, factores como la consistencia de los resultados, la ausencia de sesgos injustificados o la trazabilidad de las decisiones.

Durante los primeros años de expansión de la IA, el foco estuvo casi exclusivamente en la innovación técnica: modelos más grandes, más rápidos, más precisos. Sin embargo, a medida que los sistemas comenzaron a desplegarse en entornos reales, aparecieron problemas que no podían resolverse solo con código.

Algunos ejemplos ampliamente conocidos incluyen:

- Sistemas que discriminaban involuntariamente a determinados colectivos.
- Modelos que ofrecían resultados difíciles de explicar incluso para sus creadores.
- Decisiones automatizadas que afectaban a personas sin posibilidad de revisión humana.
- Errores que se reproducían de forma masiva porque nadie había previsto cómo detectarlos a tiempo.

Estos problemas no siempre se deben a una “mala intención” o a un sesgo inconsciente, sino a la ausencia de marcos claros de gestión y control. Cuando una organización desarrolla o utiliza IA sin reglas internas bien definidas, la tecnología puede comportarse de maneras inesperadas o indeseables. De ahí la importancia capital del concepto de **gobernanza de la inteligencia artificial**, entendido como un conjunto de principios, procesos, responsabilidades y controles que determinan cómo se decide diseñar, entrenar, desplegar, supervisar y mejorar un sistema de IA. En este contexto, conviene diferenciar dos conceptos estrechamente relacionados:

• **Gobernanza de la IA**, que se refiere al marco estratégico y de toma de decisiones. Define quién decide qué, con qué criterios y con qué responsabilidades. Incluye aspectos éticos, legales, organizativos y sociales.

• **Gestión de la IA**, que se centra en la implementación práctica de esa gobernanza. Incluye procesos operativos,

Los estándares internacionales existen para resolver un problema recurrente: cuando muchas organizaciones enfrentan desafíos similares, es ineficiente que cada una invente su propia solución desde cero. Los estándares recogen consenso experto, buenas prácticas probadas y enfoques comunes que permiten aspectos como hablar un lenguaje compartido, comparar prácticas entre organizaciones, demostrar diligencia y responsabilidad o reducir riesgos y aumentar la confianza.

En el ámbito de la inteligencia artificial, este papel lo está desempeñando principalmente la ISO (International Organization for Standardization), en colaboración con otros organismos internacionales y nacionales. En muchos sectores, cumplir con normas ISO es sinónimo de calidad, fiabilidad y buena gestión. La implicación de ISO en la IA responde a una constatación clara: la inteligencia artificial no es solo **una tecnología más, sino una tecnología transversal, capaz de afectar a múltiples sectores y dimensiones de la sociedad**.

Por ello, ISO ha desarrollado una familia de estándares específicamente orientados a la inteligencia artificial, que abordan:

- Terminología y conceptos comunes.
- Gestión de riesgos.
- Sistemas de gestión organizativos.
- Evaluación de impactos.
- Mejora continua y supervisión.

En el siguiente artículo de esta serie veremos qué estándares ISO concretos se están utilizando hoy día, cómo una organización puede implementar correctamente un sistema de gestión de IA y ejemplos prácticos de “hacer las cosas bien”.

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>



**Curso de
Certificación en:
Excelencia
en el Servicio
ISO 23592
Service
Excellence
Leader**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Basado en la Norma ISO 23592
- 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>



21001: 2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**





Domando al caballo desbocado: gobierno y gestión de la IA y sus riesgos (II)

En el primer artículo de esta serie introdujimos y justificamos la necesidad de gobernar y gestionar los sistemas de IA, y la importancia de que existan estándares al respecto. En esta entrega, mostraremos una panorámica de cómo aplicarlos.

Parte 2: Cómo aplicar correctamente los estándares ISO de inteligencia artificial

En la primera parte vimos por qué la inteligencia artificial necesita marcos de gobernanza y por qué los estándares internacionales se han convertido en una referencia imprescindible. Sin embargo, una duda habitual, especialmente fuera de los círculos técnicos, es qué significa realmente “aplicar un estándar ISO de IA” en la práctica. ¿Se trata de documentación burocrática? ¿De auditorías complejas? ¿De imponer límites que frenen la innovación?

La realidad es bastante distinta. Bien aplicados, los estándares ISO no actúan como freno, sino como estructura. Ayudan a que las organizaciones entiendan qué están haciendo con la IA, por qué lo hacen y cómo pueden hacerlo mejor. Y, sobre todo, contribuyen a que los resultados generados por los sistemas de IA sean más fiables, más coherentes y más alineados con los objetivos humanos y organizativos.

Uno de los principales valores de los estándares ISO es que traducen principios generales, como responsabilidad, transparencia o gestión del riesgo, en procesos concretos y repetibles. En el ámbito de la IA, esto es especialmente importante, porque muchas decisiones críticas se toman de forma implícita o dispersa. Por ejemplo, en una organización que desarrolla o utiliza sistemas de IA suelen coexistir:

- Equipos técnicos, que entrenan modelos.
- Áreas de negocio, que definen objetivos.
- Departamentos legales, que evalúan el cumplimiento normativo.
- Responsables de ética, calidad o riesgos.
- Usuarios finales, que interactúan con los resultados.



CONTINÚA EN
PRÓXIMA PÁGINA





Sin un marco común, cada uno de estos actores puede tener una visión parcial o incluso contradictoria del sistema. Los estándares ISO ayudan a alinear estas perspectivas, estableciendo reglas claras sobre quién decide, cómo se documenta y cómo se revisa el funcionamiento de la IA.

El estándar más relevante en este ámbito es ISO/IEC 42001, que define los requisitos para establecer un sistema de gestión de inteligencia artificial a nivel organizativo. Aunque suene abstracto, la idea es muy concreta: tratar la IA con el mismo rigor con el que muchas organizaciones ya gestionan la calidad, la seguridad de la información o el medio ambiente (con otros estándares ISO, por cierto).

Un sistema de gestión de IA inspirado en este estándar suele incluir, entre otros elementos:

- Una política de uso de la IA, aprobada por la Alta Dirección.
- Objetivos claros sobre para qué se utiliza la IA y qué límites se establecen.
- Procesos para identificar y evaluar riesgos.
- Responsabilidades definidas (quién aprueba un sistema, quién lo supervisa, etc.).
- Mecanismos de seguimiento y mejora continua.

Al aplicar un sistema de gestión de IA alineado con ISO/IEC 42001, el enfoque se basa en:

1. Definición del propósito: Se documenta claramente qué decisiones puede tomar la IA y cuáles no. Por ejemplo, la IA puede recomendar acciones, pero no denegar servicios sin revisión humana.
2. Identificación de riesgos: Se analizan posibles problemas: sesgos en las respuestas, errores repetitivos, o falta de explicaciones comprensibles para los usuarios.
3. Controles y supervisión: Se establecen métricas de calidad, revisiones periódicas y canales para que los usuarios reporten errores.
4. Mejora continua: Los resultados del sistema se revisan y se ajustan los modelos o los procesos cuando aparecen desviaciones.

El resultado no es solo un sistema más “ético”, sino uno más consistente, más comprensible y más fiable, lo que mejora la calidad del servicio y reduce reclamaciones.

El siguiente estándar en importancia, a mi juicio es el ISO/IEC 38507, que se centra en las implicaciones de gobernanza corporativa para el uso de IA. El paso lógico después de

implantar un sistema de gestión de la IA con éxito es gobernarla adecuadamente para que se aplique en la organización de forma ordenada y alineada con el marco de gobierno corporativo.

Otro estándar clave es ISO/IEC 23894, centrado específicamente en la gestión de riesgos asociados a la IA. La aportación principal de este enfoque es cambiar la lógica habitual: en lugar de esperar a que un sistema falle, se analiza qué podría salir mal antes de que ocurra. En IA, los riesgos no son solo técnicos, ya que incluyen, por ejemplo, interpretaciones erróneas de los resultados, dependencia excesiva de sistemas automatizados, pérdida de control humano o impactos negativos en determinados colectivos. Este estándar propone integrar la gestión del riesgo de IA en los procesos generales de la organización, lo que evita que la IA se convierta en una “caja negra” aislada del resto de decisiones empresariales.

Pensemos en una administración pública que utilice IA para priorizar solicitudes de ayudas o recursos. Aquí, la calidad del sistema no se mide solo por eficiencia, sino por equidad, transparencia y legitimidad social. Aplicar una gestión de riesgos alineada con ISO/IEC 23894 implicaría analizar si los datos históricos pueden reflejar desigualdades previas; evaluar cómo se comunicarán las decisiones a los ciudadanos; definir procedimientos para corregir errores y atender reclamaciones; y garantizar que siempre exista una vía de revisión humana. Cuando estos aspectos se gestionan de forma estructurada, la calidad del trabajo del sistema de IA mejora significativamente: no solo “clasifica bien”, sino que lo hace de forma comprensible y defendible ante la sociedad.

Aunque pueda parecer menor, uno de los grandes aportes de los estándares ISO en IA es la claridad conceptual. Normas como ISO/IEC 22989 establecen definiciones comunes para términos clave, evitando malentendidos que pueden tener consecuencias prácticas importantes. Una documentación clara, alineada con estándares, contribuye a que los sistemas de IA sean más auditables y más fáciles de mejorar, lo que repercute directamente en la calidad de sus resultados.

Un temor frecuente es que los estándares frenen la innovación. En la práctica, ocurre lo contrario. Cuando una organización tiene claros sus procesos y responsabilidades, puede innovar con mayor seguridad y rapidez, porque sabe qué riesgos está dispuesta a asumir, tiene mecanismos para detectar errores lo antes posible, y puede escalar soluciones con menor incertidumbre.

En este sentido, los estándares ISO actúan como infraestructura invisible: no llaman la atención, pero sostienen la calidad y la fiabilidad de todo el sistema.

En nuestro próximo artículo, que concluirá esta serie, abordaremos qué ocurre cuando no se aplican estos estándares, qué riesgos reales asumen las organizaciones, cómo la mala gobernanza se traduce en mala calidad, conflictos y pérdida de confianza, y por qué estos riesgos no son teóricos, sino muy reales.

Escuela de Gobierno

eGob®

<https://escueladegobierno.es>

**Curso de
Certificación en:**

**Diseño de
Servicios
Excelentes**

**ISO 24082
Service
Excellence
Designer**

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: Inmediata
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe del Curso: 695€
- Tasas Examen: Incluidas
- Basado en la Norma ISO 24082
- 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>



21001: 2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**

Domando al caballo desbocado: gobierno y gestión de la IA y sus riesgos (y III)

En las dos partes anteriores de este artículo hemos visto cómo los estándares ISO ofrecen un marco sólido para gobernar y gestionar la inteligencia artificial, y cómo su correcta aplicación mejora la calidad, fiabilidad y confianza en los sistemas de IA. Sin embargo, para comprender plenamente su importancia, es necesario analizar el escenario opuesto: ¿qué ocurre cuando estos principios no se aplican, o se aplican de forma superficial?

Parte 3: Cuando las cosas salen mal: riesgos reales, agentes de IA y pérdida de control

Los riesgos asociados a una mala gestión de la IA no son hipotéticos ni futuristas. Muchos de ellos ya se están manifestando, especialmente con la aparición de una nueva generación de sistemas: los **agentes de inteligencia artificial** capaces de actuar de forma autónoma sobre dispositivos, aplicaciones y entornos digitales reales.

Tradicionalmente, la mayoría de los sistemas de IA funcionaban como herramientas pasivas: analizaban datos y ofrecían recomendaciones, pero la acción final recaía en una persona. En los últimos tiempos, esta frontera ha empezado a difuminarse.

Los llamados agentes de IA no solo generan texto o análisis, sino que interactúan con interfaces gráficas de usuario, ejecutan acciones en sistemas operativos, controlan aplicaciones, y toman decisiones encadenadas para cumplir un objetivo. En otras palabras, ya no se limitan a “decir qué habría que hacer”, sino que hacen cosas. Y cuando estas acciones se realizan sobre dispositivos personales o corporativos, el impacto potencial crece de forma exponencial.

Desde el punto de vista del usuario, la promesa es muy atractiva: un agente de IA que reserve viajes, gestione correos, modifique documentos, instale software o configure sistemas sin intervención humana constante. Esto promete eficiencia, ahorro de tiempo y reducción de carga cognitiva. Sin embargo, desde la perspectiva de la gobernanza y la gestión del riesgo, esta delegación plantea preguntas críticas:

- ¿Qué límites tiene el agente?
- ¿Qué entiende exactamente por “objetivo”?
- ¿Qué ocurre si interpreta mal una instrucción?
- ¿Cómo se supervisan sus acciones?
- ¿Quién es responsable si algo sale mal?

Estas preguntas están en el corazón de los estándares ISO sobre IA, pero en muchos despliegues reales se están abordando de forma insuficiente o tardía.



CONTINÚA EN
PRÓXIMA PÁGINA



Un ejemplo especialmente ilustrativo es el debate generado en torno a Claude, el asistente desarrollado por la compañía Anthropic, cuando se le dotó capacidades experimentales que permitían al sistema interactuar con ordenadores y aplicaciones como lo haría una persona.

Estas capacidades, diseñadas con fines de investigación y productividad, mostraron rápidamente tanto su potencial como sus riesgos, ya que el agente podía navegar por interfaces complejas, ejecutar secuencias de acciones, cometer errores difíciles de anticipar y, lo más importante, hacerlo a gran velocidad. Aunque se implementaron salvaguardas, el caso sirvió para evidenciar un problema clave: **cuando una IA actúa sobre un dispositivo, los errores dejan de ser abstractos y se convierten en consecuencias directas.**



Un clic incorrecto, una mala interpretación o una acción repetida de forma sistemática puede devenir en un borrado de información, la filtración de datos sensibles, la modificación de configuraciones críticas o la generación de efectos en cadena difíciles de revertir.

Los principales riesgos de este tipo de agentes pueden agruparse en varias categorías claras:

1. Pérdida de control humano efectivo: Aunque formalmente exista supervisión humana, en la práctica el ritmo de acción de un agente puede superar la capacidad de supervisión real. Cuando una persona revisa resultados a posteriori, el daño puede ya estar hecho. Los estándares ISO insisten en la necesidad de definir **niveles claros de autonomía**, pero cuando esto no se hace bien, la frontera entre “asistente” y “actor autónomo” se vuelve difusa.

2. Ambigüedad en la responsabilidad: Si un agente ejecuta una acción no deseada, ¿quién es responsable? ¿El desarrollador del sistema? ¿La organización que lo desplegó? ¿El usuario que dio una instrucción imprecisa y le cedió el control de su equipo? Sin una gobernanza clara, estas preguntas quedan sin respuesta. ISO insiste en la **asignación explícita de responsabilidades**, precisamente para evitar estas zonas grises que erosionan la confianza y complican la gestión de incidentes.

3. Riesgos de seguridad de la información: Un agente con acceso a dispositivos puede, de forma no intencionada, por ejemplo, exponer credenciales, copiar o enviar información sensible, o interactuar con sistemas sin comprender su criticidad. Estos riesgos no siempre derivan de ataques externos, sino de **fallos de diseño y gestión**. Un sistema que no distingue adecuadamente entre información sensible y no sensible puede convertirse en una fuente involuntaria de filtraciones.

4. Escalado rápido de errores: Uno de los aspectos más peligrosos de los agentes de IA es su capacidad para repetir acciones erróneas de forma sistemática. Un error humano suele ser puntual, pero un error automatizado puede reproducirse cientos o miles de veces en segundos. Sin mecanismos de detección temprana y parada automática, elementos clave en los sistemas de gestión de IA propuestos por ISO, estos errores pueden adquirir una dimensión crítica.

Todos estos riesgos tienen un efecto directo sobre la calidad del trabajo generado por la IA. Un sistema puede ser técnicamente avanzado y, aun así producir resultados incorrectos, generar

acciones no deseadas, perder coherencia con el propósito original, erosionar la confianza de usuarios y clientes. Desde esta perspectiva, la calidad deja de ser una cuestión de rendimiento y pasa a ser una cuestión de **control, contexto y responsabilidad**. Un agente que actúa “bien” desde el punto de vista técnico, pero fuera de los límites adecuados, es un sistema de baja calidad en términos reales.

Más allá de los efectos técnicos, una mala gestión de la IA puede tener consecuencias profundas para las organizaciones, tales como pérdida de reputación, conflictos legales, retirada apresurada de sistemas o desconfianza generalizada hacia futuras iniciativas de IA.

Uno de los mensajes centrales de los estándares ISO es que **no todo lo técnicamente posible es organizativamente aceptable**. La capacidad de un agente de IA para controlar un dispositivo no implica que deba hacerlo sin límites claros. Por tanto, gobernar bien la IA implica definir qué usos son apropiados, establecer barreras técnicas y organizativas, formar a las personas que interactúan con estos sistemas y asumir que la supervisión humana sigue siendo esencial. Este enfoque no frena la innovación, sino que la hace **sostenible y socialmente aceptable**.

A lo largo de este artículo hemos visto que los estándares ISO en gobierno y gestión de la inteligencia artificial no son un ejercicio teórico ni una moda regulatoria. Son una respuesta práctica a un problema muy real: cómo integrar sistemas cada vez más autónomos en entornos humanos sin perder control, calidad ni confianza. Casos como el de Claude y otros agentes con control operativo muestran que los riesgos ya no están en el futuro. Están aquí, y crecen al mismo ritmo que las capacidades de la tecnología.

La lección es clara: **la calidad de la inteligencia artificial no depende solo de lo inteligente que sea el sistema, sino de lo bien que esté gobernado**. Cuando se ignoran estos principios, los riesgos se multiplican. Cuando se aplican correctamente, la IA puede convertirse en una herramienta poderosa, fiable y alineada con los intereses humanos. Y en ese equilibrio entre innovación y responsabilidad es donde los estándares ISO encuentran su razón de ser.



Curso de Certificación en:

Gestión de Centros de Operaciones de Seguridad (SOC)

SOC Management Leader

Docente:
Alejandro Aliaga

- Formato: Grabado con Tutorías
- Tutorías en directo: Lunes Tardes
- Disponibilidad: Inmediata
- Plazo de Vigencia: 60 Días
- Carga Lectiva: 20 Horas
- Importe del Curso: 995€
- Tasas Examen: Incluidas
- En tu horario, a tu ritmo.
- Con toda comodidad
- Solicita tu admisión

MidMgmt®

MPPM®

MGEIT®

eGob®

Tutorías en Directo



+ 34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>



21001: 2018
EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS



Evaluando el factor humano: Human Risk Management

En artículos anteriores hemos tratado el tema de la concienciación de los usuarios de los sistemas de información, como uno de los factores que influye positivamente en que en nuestras vidas personales o profesionales se mantenga una adecuada postura de seguridad. Sin embargo, pocas veces se dispone de métricas que permitan conocer cuál es el riesgo real para la seguridad que suponen las personas que conforman la organización. Y es aquí donde aparece un interesante concepto: la gestión del riesgo humano (o HRM, Human Risk Management).

En los entornos de atención al usuario de las organizaciones de cualquier tamaño son habituales los chascarrillos o bromas privadas sobre cuál es el origen de la mayoría de incidencias: los usuarios. Hay que se refiere a “un problema en la Capa 8”, en referencia a las siete capas del modelo ISO OSI (Open Systems Interconnection), y aludiendo a que el usuario es esa octava capa que no aparece en el modelo. También hay quien utiliza el acrónimo PEBKAC para indicar que la causa raíz de la incidencia es la persona usuaria del sistema (Problem Exists Between Keyboard and Chair). Y en parte, puede que no les falte razón.

Sin embargo, cuando se trata de seguridad de la información, la cosa deja de tener gracia y se acaban las bromas y los chascarrillos. Se calcula que el 78% de los ciberincidentes sucedidos en 2025 se debieron a algún aspecto relacionado con la identidad de los usuarios: robo de credenciales, venta de éstas en el mercado negro, etc. Y ante el panorama que se abre en la seguridad de la información con la expansión del uso de la Inteligencia Artificial, más si cabe es necesario poder gestionar uno de los riesgos que los tecnólogos no somos capaces de mitigar con tecnología por

debajo del nivel de riesgo aceptable: el que representan los humanos que hacen uso de esa tecnología.

Se pueden poner múltiples mecanismos de seguridad, obtener varias certificaciones al respecto, disponer de todo tipo de siglas (SOC, SIEM, EDR, etc.), pero un clic en un lugar equivocado, un comportamiento fuera de lo normalizado, o un empleado enfadado puede poner gravemente en riesgo la seguridad de la organización. Siempre se ha dicho que la cadena se rompe por el eslabón más débil, y en este caso, en muchas ocasiones, ese eslabón es el usuario. Y para tratar de mitigar este riesgo, la ortodoxia nos prescribe la concienciación y la formación como las medicinas que han de ayudar a las organizaciones a estar más seguras, una vez implantadas las medidas técnicas necesarias, claro.

Pero, tras realizar un ambicioso programa formativo y de concienciación, ¿cuánto hemos reducido ese riesgo?. Esta pregunta no suele hacerse en las organizaciones, ya que se tiende a pensar en que, una vez finalizadas esas acciones, el personal ya tiene grabado en su “sistema operativo mental” esas normas, directrices o consejos. Y esta es una asunción muy naif, porque cualquiera se da cuenta que es la práctica y la repetición lo que crea la costumbre, y con esta, la experiencia y la maestría.



**CONTINÚA EN
PRÓXIMA PÁGINA**

Hablamos de pasar del estado de Incompetencia Inconsciente al estado de Competencia Inconsciente, es decir, a poder hacer las cosas (en este caso, evitar comportamientos de riesgo) sin tener que pensar, casi de forma mecánica.

En este contexto, aparecen herramientas que se plantean apoyar a las organizaciones en conseguir que, de forma efectiva, ese riesgo asociado al factor humano se reduzca de forma tangible, y sobre todo, medible. Y además, de forma personalizada y flexible, planteando a ruta de concienciación y formación más adecuada a la situación de cada empleado. Hablamos de herramientas que, además, intentan identificar situaciones personales de los empleados que puedan acabar siendo un riesgo para la seguridad de la organización. Me estoy refiriendo, por ejemplo, a situaciones de burnout (o estar quemado), al síndrome del edificio enfermo, o a mandos que no respetan las horas de descanso del personal y siguen enviando comunicaciones fuera del horario de trabajo, lo que afecta al bienestar digital del personal.

Los sistemas de HRM plantean herramientas para:

- Lanzar campañas de phishing y similares al personal.
- Enviar campañas generales o segmentadas de concienciación.
- Evaluar los resultados de esas campañas.
- Enviar documentos o píldoras sobre contenidos de seguridad o bienestar digital.
- Realizar encuestas para detectar determinadas situaciones personales.
- Generar métricas personales, de grupo o de la organización que ayuden a identificar las necesidades formativas y de concienciación del personal.
- Planificar un camino formativo y de concienciación para cada persona de la organización, en función de las diferentes métricas que elabora el sistema.
- Comparar las situaciones de partida y actual, y adaptar las acciones a realizar a la evolución de la organización respecto del riesgo evaluado.

Con este tipo de productos, un responsable de seguridad puede responder a preguntas que una Alta Dirección preocupada por cómo una deficiente seguridad de la información puede impactar en la organización, tales como:

- ¿Cómo está de concienciado nuestro personal respecto a los riesgos de seguridad de la información?



- ¿Conocen los mandos intermedios la situación al respecto de sus equipos?
- ¿Sobre qué empleados hay que hacer más esfuerzos para evitar que ellos mismos sean un riesgo para la organización, bien por falta de concienciación, bien porque estén quemados?
- ¿Cuál ha sido la efectividad del uso del sistema HRM para mejorar nuestra postura general de seguridad?
- ¿Cuál es el retorno de inversión de disponer de uno de estos sistemas, frente al riesgo mitigado por los procesos de concienciación y formación?

Como conclusión, recuerde el lector que no se puede mejorar lo que no se mide, y en organizaciones de mediano tamaño es muy complejo medir la postura de seguridad del personal sin un sistema que los pueda ir evaluando de forma individualizada conforme pasa el tiempo y se lleven a cabo iniciativas que busquen mitigar el riesgo asociado al factor humano.

Con este artículo finalizamos temporada de Tecnología y Sentido Común. Espero los once artículos de la temporada que cerramos hayan sido de interés para el lector, y que nos acompañe en la 12ª temporada, a partir de septiembre. No me queda más que desearles a todos ustedes unas felices vacaciones, ¡y nos vemos a la vuelta!



**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 del Curso: 695€
- Tasas Examen: Incluidas
- Basado en la Norma ISO 37000
- 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>



21001: 2018
**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**



El Liderazgo de la Mujer en la Normalización

El futuro de la competitividad está vinculado a la participación de la mujer en la normalización española y mundial.

Me resulta difícil escribir esta reflexión sobre la igualdad de género en el ámbito de la normalización, pues desde siempre he considerado que la mujer está tan capacitada o más para desempeñar todo tipo de funciones profesionales en la sociedad. Pero, aunque cada vez son más los que piensan como yo, la realidad todavía no acaba de situar a la mujer profesional al mismo nivel que el hombre profesional.

Primero quiero destacar la importancia de la generación de estándares para la competitividad de una nación. Las normas definen estándares técnicos y formas de trabajo que ayudan a las organizaciones a ser más eficaces y competitivos en sus mercados. Quién participa en la creación de las normas está influyendo en cómo se diseñan los productos y servicios que ofrecen las organizaciones. Por lo tanto, participar en la normalización es contribuir a la construcción de las reglas que configuran la productividad de nuestra sociedad.

La presencia de la mujer en estas actividades de creación de estándares es fundamental, pues las normas deben estar co-creadas teniendo en cuenta todas las perspectivas incluyendo las de género. La diversidad influye directamente en la calidad y adecuación de las normas producidas. No se trata solo de que haya mujeres presentes, deben estar en los estamentos normativos de liderazgo, en los que se toman decisiones (presidencia de comités de normalización, coordinadoras de grupos de trabajo, etc.).

La norma **ISO 53800** establece las directrices para la promoción e implementación de la igualdad de género y el empoderamiento de las mujeres. Proporciona un marco, recursos, políticas, herramientas y buenas prácticas para promover e implementar la igualdad de género.



CONTINÚA EN
PRÓXIMA PÁGINA





Como son los casos ejemplares los que generan pasiones y animan a las organizaciones a promover a sus profesionales femeninas a los ámbitos de liderazgo en la normalización, permitidme la libertad de citar solo unos ejemplos relevantes de los muchos que hay en la normalización española:

D^a. ELENA SANTIAGO Directora General CEN y CENELEC, que declara: “Estoy convencida de que, con el esfuerzo y entusiasmo de nuestra comunidad, con determinación y valentía, la integración de género en las Normas Europeas será pronto lo normal”.

D^a. VAL DÍEZ presidenta del comité UNE CTN 194 de Igualdad de Género, que además fue reconocida con el Premio UNE 2024 a la presidencia más destacada. Este comité ha canalizado la influencia española en el comité de ISO a cargo de la elaboración de la Norma ISO 53800, primer estándar global de igualdad de género y empoderamiento de las mujeres en las organizaciones.

D^a. ARANCHA GARCÍA presidenta del comité UNE CTN 26 de vehículos de carretera, indica: “En un entorno totalmente globalizado y altamente competitivo como el que afronta la industria de la automoción, la normalización es una herramienta estratégica para hacer frente a los retos desde un plano innovador y de desarrollo sostenible”.

D^a. CARLOTA BUSTELO RUEDA presidenta del comité CTN 50/SC 1 Gestión documental y aplicaciones indica: “Es muy enriquecedora la participación en comités internacionales, donde a pesar de las diferentes culturas, idiomas y contextos legislativos, compartimos problemas y conseguimos normalizar soluciones”.

D^a. EVA BEJARANO presidenta del comité CTN 53 de Plásticos y Caucho, para ella: “la normalización contribuye a resolver los retos que se plantea la sociedad en relación con los plásticos, para mejorar la calidad de vida de las personas y asegurar la sostenibilidad medioambiental”.

D^a. BEATRIZ NOVEL presidenta del comité internacional IEC SC 23E sobre equipamiento eléctrico y de seguridad, que además fue galardonada con el premio Thomas A. Edison de la Comisión Electrotécnica Internacional (IEC), siendo el primer profesional español en recibir este reconocimiento.

La creación de nuevos estándares está vinculada inexorablemente a la co-creación que involucre al sector femenino. Todo CEO y Alto Directivo debe tener interiorizado esta realidad.

Javier Peris
Presidente de UNE-SC40
Gobierno y Gestión de Servicios de TI.

**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.



**Normalización
Española**

**Progreso
compartido**

une.org



Evento

CIERRE DE TEMPORADA

Revistas "Tecnología & Sentido Común"
y "Stakeholders.news"

bete gratis

logía &
ido Común

2022
EMIOS
PIENS

r de



#TYSC / PÁG. 56

TECNOLOGÍA Y
SENTIDO COMÚN

Tecnología y Sentido Común y Stakeholders.news celebran el cierre de temporada

10 de julio 2026

11:00 a 15:00

El pasado 10 de julio, las revistas hermanas Tecnología y Sentido Común y Stakeholders.news cerraron la temporada 2025/26 con un evento celebrado en la sede de UNE, Asociación Española de Normalización.

El acto se inició con las intervenciones de Javier Peris, director de las revistas, y de Paloma García López, Subdirectora General de UNE, dando la bienvenida a todos los presentes en el evento. En su intervención, la Sra. García recordó además la apuesta de UNE y de las instituciones de estandarización por las normas de gobierno y gestión en tiempos de la Inteligencia Artificial. Javier Peris utilizó este turno de presentación para detallar el orden del día del evento, y rememoró, para quien no lo conocía, los orígenes de Tecnología y Sentido Común como programa de radio en 2015, y que tuvo que cambiar de formato tras la pandemia de la COVID-19. Asimismo, profundizó en la motivación para editar Stakeholders.news, en el sentido de que creía muy conveniente divulgar la cultura de la gestión de portafolios, programas y proyectos en la sociedad. Finalizó esta intervención recordando que éste era un evento participativo, en el que cualquiera podía preguntar a los participantes, y tras la apertura, presentó a Marcelino Lominchar, escritor de la obra "Historias de la contrahistoria de España".

On July 10, the fellow magazines Tecnología y Sentido Común and Stakeholders.news wrapped up the 2025/26 season with an event held at the headquarters of UNE, the Spanish Association for Standardization.

The event began with remarks by Javier Peris, director of both magazines, and Paloma García López, Deputy General Director of UNE, who welcomed the audience. In her remarks, Mrs. García also highlighted the commitment of UNE and standardization institutions to governance and management standards in the age of Artificial Intelligence. Javier Peris used his introductory remarks to outline the event's agenda and, for those unfamiliar with it, recalled the origins of Tecnología y Sentido Común as a radio program in 2015, and why it changed its format following the COVID-19 pandemic. He also elaborated on his motivation for launching Stakeholders.news, explaining that he believed it was very important to promote a culture of portfolio, program, and project management throughout society. He concluded his remarks by noting that this was a participatory event, where anyone could ask the speakers any question. And following the opening remarks, he introduced Marcelino Lominchar, author of the book Historias de la contrahistoria de España (Stories of Spain's Counterhistory).



CONTINÚA EN
PRÓXIMA PÁGINA

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

En su charla, el Sr. Lominchar glosó algunos de los contenidos de su nueva obra literaria, centrada principalmente en los logros de personajes históricos españoles poco conocidos o deliberadamente ignorados, alrededor de los conceptos de invención e innovación, una situación que él calificó de injusta. Aludió a que una de las principales críticas que se realizan sobre nuestro país es que hemos sido poco innovadores a lo largo de la Historia, a lo que el autor contrapuso los logros de varias personas. Por ejemplo, con el caso del mayor inventor español, Leonardo Torres Quevedo, o con un prácticamente desconocido Jerónimo de Ayanz. A éste último se le deben invenciones como la escafandra de buceo en 1602, pero no para el buceo marítimo, sino en aguas subterráneas en minas. Igualmente, fue el padre de las bombas hidráulicas, de los sistemas de ventilación de minas (precursores del aire acondicionado), o de la máquina de vapor en 1608, que como es bien conocido, se adjudica habitualmente al escocés James Watt alrededor de 1769, probablemente, porque la patentó.

En este punto, el Sr. Lominchar apuntó a que quizá el fallo de los inventores españoles es comunicativo, o de falta de mercado o de inversión, o de no acertar con el momento adecuado o de fomentar la adopción de sus inventos. Y ahí radica, a juicio de este autor, la diferencia fundamental entre inventar e innovar. Básicamente, en contar con un ecosistema apropiado, algo que Ayanz no tuvo en su momento.

En la obra del Sr. Lominchar también se mencionan los casos de Agustín de Betancourt, Fray Domingo de Soto, Félix de Azara, Abbas Ibn Firnas (que planeo con una alas de tela y madera frente al Emir de Córdoba en el S. IX) o Mariano Díez Tobar. Inventores y científicos españoles que inspiraron a otros mucho más conocidos, como Isaac Newton o Charles Darwin, que fueron lectores de las obras de estos españoles antes de realizar sus descubrimientos.

Como conclusión de su ponencia, el autor dejó dos ideas-fuerza: ser el primero no garantiza cambiar la Historia, y que el mayor enemigo de la innovación no es la falta de ideas, sino la falta de relato.

In his talk, Mr. Lominchar discussed some of the content of his new literary work, which focuses primarily on the achievements of little-known or deliberately ignored historical Spanish figures, focused on the concepts of invention and innovation, a situation he described as unfair. He noted that one of the main criticisms leveled at our country is that we have been uninnovative throughout history, a claim the author countered by highlighting the achievements of several individuals. For example, he cited the case of Spain's greatest inventor, Leonardo Torres Quevedo, and the virtually unknown Jerónimo de Ayanz. The latter is credited with inventions such as the diving suit in 1602 (not for marine diving, but for use in underground mine waters). Likewise, he was the pioneer of hydraulic pumps, mine ventilation systems (precursors to air conditioning), and the steam engine in 1608, which, as is well known, is usually attributed to the Scotsman James Watt around 1769, likely because he patented it.

At this point, Mr. Lominchar noted that perhaps the shortcoming of Spanish inventors lies in communication, or a lack of market or investment, or failing to seize the right moment, or in promoting the adoption of their inventions. And therein lies, in this author's view, the fundamental difference between inventing and innovating: essentially, having an appropriate ecosystem, something Ayanz did not have at that time.

Mr. Lominchar's work also mentions the cases of Agustín de Betancourt, Fray Domingo de Soto, Félix de Azara, Abbas Ibn Firnas (who flew with wings made of cloth and wood in front of the Emir of Córdoba in the 9th century), and Mariano Díez Tobar. These Spanish inventors and scientists inspired other, much better-known figures, such as Isaac Newton and Charles Darwin, who had read the works of these Spaniards before making their own discoveries.

In conclusion, the author highlighted two key ideas: being the first does not guarantee that you will change history, and that the greatest enemy of innovation is not a lack of ideas, but a lack of narrative.



CONTINÚA EN
PRÓXIMA PÁGINA



n fue el mayor inventor español de

ca lideró las revoluciones

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>



Suscríbete gratis

REVISTA
**Tecnología &
Sentido Común**

#19
**2022
PREMIOS
SAPIENS**

Alejandro
Blasco

PROTECTOR

10

LA Nueva
Administ

VÍCTOR ALMORAL

Por Proce

MADELANE CASTE

MESA
Modera Jav...



MAN...
SER...
Seco...
Futu...
Segu...



MAN...
SER...
Seco...
Futu...
Segu...



MAN...
SER...
Seco...
Futu...
Segu...



Tras la conferencia del Sr. Lominchar, se dio paso a la primera de las mesas redondas previstas para el evento. En concreto, la dedicada a la revista Tecnología y Sentido Común, y que estuvo conformada por Manuel D. Serrat, Ignacio Alamillo, Domingo Gaitero, Marlon Molina, Marcos Navarro, Victor Almonacid y Marta Martín, todos ellos colaboradores de la revista. Durante la mesa redonda, Javier Peris, su director, lanzó a los participantes diferentes preguntas sobre los temas tratados en sus respectivas secciones en esta temporada que se cierra, o sobre el enfoque o los temas que tienen previsto tratar en las mismas en la decimosegunda temporada, que comienza en septiembre. Fue una mesa en la que se habló mucho de Inteligencia Artificial, tanto de sus ventajas como de sus riesgos, en diferentes ámbitos de la sociedad, y sobre todo, de la obligatoriedad de la supervisión humana en todo lo que a la IA se refiere.

Following Mr. Lominchar's lecture, the event moved on to the first of the scheduled roundtable discussions. Specifically, the session dedicated to the magazine Tecnología y Sentido Común, which featured Manuel D. Serrat, Ignacio Alamillo, Domingo Gaitero, Marlon Molina, Marcos Navarro, Victor Almonacid, and Marta Martín, all of them contributors to the magazine. During the round, Javier Peris, the magazine's editor-in-chief, posed various questions to the participants regarding the topics covered in their respective sections during the current season, which is coming to a close, as well as the approach and topics they plan to address in the twelfth season, which begins in September. The discussion focused heavily on artificial intelligence, both its advantages and risks across various sectors of society, and, above all, on the necessity of human oversight in all matters related to AI.



CONTINÚA EN
PRÓXIMA PÁGINA

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>



Suscríbete gratis

REVISTA
**Tecnología &
Sentido Común**

**2022
PREMIOS
SAPIENS**

Alejandro Blasco
Juan J. Urbión
Víctor Almonaco
Por Procesos
Magdalena Calvo

MESA RED
Modera Javier P...

JUAN J. URBIÓN
Sección
Proyectos
el Futuro

JUAN J. URBIÓN
Sección
Proyectos
el Futuro

JUAN J. URBIÓN
Sección
Proyectos
el Futuro

JUAN J. URBIÓN
Sección
Proyectos
el Futuro

JUAN J. URBIÓN
Sección
Proyectos
el Futuro

JUAN J. URBIÓN
Sección
Proyectos
el Futuro

JUAN J. URBIÓN
Sección
Proyectos
el Futuro

JUAN J. URBIÓN
Sección
Proyectos
el Futuro

JUAN J. URBIÓN
Sección
Proyectos
el Futuro

JUAN J. URBIÓN
Sección
Proyectos
el Futuro

JUAN J. URBIÓN
Sección
Proyectos
el Futuro

JUAN J. URBIÓN
Sección
Proyectos
el Futuro

La siguiente mesa redonda, igualmente moderada por el director de Stakeholders.news, contó con los colaboradores habituales de la misma. Juan Jesús Urbizu, Juan Manuel Domínguez, Charo Fresneda, Luis Morán, José Luis Portela, y José Antonio Puentes, siguiendo un formato muy similar a la anterior mesa redonda, desgranaron los elementos más significativos de sus colaboraciones con la revista en la temporada que se cierra, y aportaron alguna pincelada de cómo afrontan la sexta temporada que se inicia tras las vacaciones veraniegas. Se habló de temas relacionados con la gestión del cambio, la resiliencia organizativa como un músculo que hay que ejercitar, o el uso de la Inteligencia Artificial en el "change the business" para evitar que genere disrupción en los equipos del "run the business". También hubo alguna intervención que remarcó el gravísimo problema que hay en España con los salarios, que, comparados con los de 2001 han perdido la mitad de su poder adquisitivo.

The next roundtable, also moderated by the editor-in-chief of Stakeholders.news, featured the publication's regular contributors. Juan Jesús Urbizu, Juan Manuel Domínguez, Charo Fresneda, Luis Morán, José Luis Portela, and José Antonio Puentes. Following a very similar format to the previous roundtable, they highlighted the most significant aspects of their contributions to the magazine during the season that is coming to a end, and offered a glimpse of how they are approaching the sixth season, which begins after the summer break. Topics discussed included managing change, organizational resilience as a muscle that must be exercised, and the use of Artificial Intelligence in "changing the business" to prevent it from causing disruption to the teams responsible for "running the business." There were also remarks highlighting the extremely serious problem in Spain regarding wages, which have lost half their purchasing power compared to 2001 one.

RONDA "STAKEHOLDERS.NEWS"

12:30 a 13:15

			
JUAN JESÚS URBIZU	JUAN MANUEL DOMÍNGUEZ	CHARO FRESNEDA	LUIS MORÁN
Sección: Organización Resilientes	Sección: El Lado Humano	Sección: Personas y Procesos	
			
JOSÉ ANTONIO PUENTES	JOSÉ LUIS PORTELA	LUIS GUARDADO	
Sección: Entendiendo Puentes	Sección: El Salvador		



CONTINÚA EN
PRÓXIMA PÁGINA



REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Tras las mesas redondas, los asistentes pudieron disfrutar de la ponencia “Los tres mosqueteros de la Era Digital”, a cargo de Ramsés Gallego, primer español incluido en el ISACA Hall of Fame, en la que, como es habitual en este experto conferenciante, utilizó imágenes alegóricas y un **storytelling** muy cuidado para transmitir las ideas que deseaba transmitir. En esta ocasión, comenzó recordando que la coexistencia de tecnologías, modelos de gobierno y gestión, y falta de coherencia en ciertos ámbitos, hace que la situación del mundo sea extremadamente compleja. El Sr. Gallego utilizó a los personajes de la novela clásica “Los Tres Mosqueteros”, de Alexandre Dumas, para representar, con sus características personales, a los diferentes tipos de gobiernos que se requieren en las organizaciones. En su opinión Athos representa al Gobierno Corporativo; Porthos, al Gobierno de Tecnologías de la Información; Aramis, al Gobierno del Datos; y D’Artagnan, al Gobierno de la IA. En opinión del ponente, vivimos en un mundo en el que tenemos que Gobernarlo y Gestionarlo todo a la vez y en todas partes, haciendo un guiño a la película de 2022 del director Dan Kwan, y terminó con la más que famosa frase de los Mosqueteros del Rey: “Uno para todos, y todos para uno”-

Following the roundtable discussions, attendees enjoyed the presentation “The Three Musketeers of the Digital Age” by Ramsés Gallego, the first Spaniard inducted into the ISACA Hall of Fame. As is typical for this expert speaker, he used allegorical imagery and carefully crafted storytelling to convey his key ideas. On this occasion, he began by noting that the coexistence of technologies, governance and management models, and a lack of consistency in certain areas, makes the global situation extremely complex. Mr. Gallego used the characters from Alexandre Dumas’s classic novel The Three Musketeers to represent, through their personal traits, the different types of governance required in organizations. In his view, Athos represents Corporate Governance; Porthos, Information Technology Governance; Aramis, Data Governance; and D’Artagnan, AI Governance. In the speaker’s view, we live in a world where we have to govern and manage everything at once and everywhere (a nod to director Dan Kwan’s 2022 film) and he concluded with the famous motto of the King’s Musketeers: “One for all, and all for one.”



CONTINÚA EN
PRÓXIMA PÁGINA

scríbete gratis

DE DIRECCIÓN Y GESTIÓN

makers news



REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

críbete gratis

ISTA

nología & entido Común



2022 PREMIOS SAPIENS

Para cerrar el evento, la organización, de la mano de Ramsés Gallego y Javier Peris, hizo entrega de los premios Tecnología y Sentido Común 2026 y Stakeholders.news 2026. En esta ocasión, el primero de ellos se otorgó a ISACA International, por el establecimiento de su oficina en la Unión Europea, siendo recogido el galardón por Chris Dimitriadis, **Chief Global Strategy Officer de ISACA**.

To close the event, the organizers, led by Ramsés Gallego and Javier Peris, presented the 2026 Tecnología y Sentido Común and Stakeholders.news 2026 awards. On this occasion, the first award was given to ISACA International for establishing its office in the European Union. The award was accepted by Chris Dimitriadis, ISACA's Chief Global Strategy Officer.



CONTINÚA EN
PRÓXIMA PÁGINA



GA DE P
Ramsés Gallego

olo
tic

VÍCTOR ALMONACID

Por Procesos



#TYSC / PÁG. 66



PREMIOS

Tecnología & Sentido Común
2026

13:45 a 14:00

PREMIO RE
S
2026

"Tecnología & Sentido Común"
the award recognizes the best project and
initiative in the field of digital transformation and
innovation, in the field of technology, for the year
2026.

"Tecnología & Sentido Común 2026" is
an initiative of ISACA International
for the development of the European Office and
the initiative with the European Commission.
Madrid, July 10, 2025

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

gratis

& común



El segundo de los premios entregados en el acto fue concedido a IFEMA Madrid, por la Gobernanza, Dirección, Gestión y Ejecución del Circuito Urbano de Madrid, MADRING que ha permitido en 11 meses, desde cero, construir el circuito de Fórmula 1 urbano de Madrid, siendo recogido en esta ocasión por Carlos Jiménez, Director de Operaciones de la compañía.

Al terminar los actos protocolarios, Javier Peris volvió a agradecer a los presentes su asistencia, y les conminó a seguir disfrutando de los contenidos de ambas revistas. A continuación, los asistentes pudieron disfrutar de un animado *networking* y degustar un exclusivo *catering*, como viene siendo marca de la casa en los eventos de las revistas Tecnología y Sentido Común y Stakeholders.news.

The second award presented at the ceremony went to IFEMA Madrid for the governance, leadership, management, and execution of the Madrid Urban Circuit (MADRING), which made it possible to build Madrid's urban Formula 1 circuit from scratch in just 11 months. The award was accepted on this occasion by Carlos Jiménez, the company's Chief Operations Officer.

Once the formal proceedings concluded, Javier Peris once again thanked those present for attending and encouraged them to continue enjoying the content of both magazines. Afterward, attendees were able to enjoy lively networking and sample exclusive catering, a hallmark of events hosted by the magazines Tecnología y Sentido Común and Stakeholders.news.



CONTINÚA EN
PRÓXIMA PÁGINA



#TYSC / PÁG. 68

Stakeholders

.news

Revista Mensual Líder de la Hispana de la
Dirección y Gestión de Proyectos, Programas
su premio



"Stakeholders.news"
la Revista Mensual Líder de la Hispana
de la Alta Dirección y los Profesionales en Gobierno,
Dirección y Gestión de Proyectos, Programas y Proyectos
otorga su premio:

"Stakeholders.news 2026" a:
IFEMA MADRID

por la Dirección, Gestión y Ejecución
del Circuito Urbano de Madrid, MADRID.

Madrid, 10 de julio de 2026

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>



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

Curso de Certificación en:
Ejecución Estratégica y Cambio Organizacional
P4MGO!® Essentials

Docente:
Javier Peris

- Formato: Grabado
- Disponibilidad: On Demand
- Carga Lectiva: 30 Horas
- Importe del Curso: 345€
- Tareas Examen: Incluidas
- A tu ritmo
- En tu horario
- Desde donde te encuentres
- Con toda comodidad

Disponibilidad Inmediata

Solicita tu admisión en:
+34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
ISO EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Gestión de Portfolios
P4MGO! Pfm Portfolio Management

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tareas Examen: Incluidas
- Basado en el P4MGO! Pfm Bok
- A tu ritmo con toda comodidad
- Requisito Previo P4MGO! Essentials

Tutorías en Directo

Solicita tu admisión en:
+34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
ISO EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Gestión de Programas
P4MGO! Pgm Programme Management

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tareas Examen: Incluidas
- Basado en el P4MGO! Pgm Bok
- A tu ritmo con toda comodidad

Tutorías en Directo

Solicita tu admisión en:
+34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
ISO EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Gestión de Proyectos
P4MGO! Pjm Project Management

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 20 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tareas Examen: Incluidas
- Basado en el P4MGO! Pjm Bok
- A tu ritmo con toda comodidad

Tutorías en Directo

Solicita tu admisión en:
+34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
ISO EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Gestión de Productos Digitales
P4MGO! Pdm Product Digital Management

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tareas Examen: Incluidas
- Basado en el P4MGO! Pdm Bok
- A tu ritmo con toda comodidad
- Requisito Previo P4MGO! Essentials

Tutorías en Directo

Solicita tu admisión en:
+34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
ISO EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Gestión por Procesos de Negocio
P4MGO! BPM Business Process Management

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tareas Examen: Incluidas
- Basado en el P4MGO! BPM Bok
- A tu ritmo con toda comodidad

Tutorías en Directo

Solicita tu admisión en:
+34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
ISO EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Gestión de Servicios y Operaciones
P4MGO! S&O Service & Operations Management

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tareas Examen: Incluidas
- Basado en el P4MGO! S&O Bok
- A tu ritmo con toda comodidad
- Requisito Previo P4MGO! Essentials

Tutorías en Directo

Solicita tu admisión en:
+34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
ISO EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Oficinas de Gestión
P4MGO! PMO Management Offices

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tareas Examen: Incluidas
- Basado en el P4MGO! PMO Bok
- A tu ritmo con toda comodidad
- Requisito Previo P4MGO! Essentials

Tutorías en Directo

Solicita tu admisión en:
+34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
ISO EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Centros de Excelencia
P4MGO! CoE Centres of Excellence

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tareas Examen: Incluidas
- Basado en el P4MGO! CoE Bok
- A tu ritmo con toda comodidad
- Requisito Previo P4MGO! Essentials

Tutorías en Directo

Solicita tu admisión en:
+34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
ISO EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS

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

Curso de Certificación en:
Gobierno de la Ejecución Estratégica y del Cambio Organizacional
P4MGO! Gov Strategic Execution & Organizational Change Governance

Dirección Académica:
Javier Peris

- Formato: Grabado con Tutorías
- Disponibilidad: On Demand
- Plazo de Vigencia: 90 Días
- Carga Lectiva: 24 Horas
- Tutorías en directo: Lunes Tardes
- Importe Matrícula: 695,00 €
- Tareas Examen: Incluidas
- Basado en el P4MGO! Gov Bok
- A tu ritmo con toda comodidad
- Requisito Previo P4MGO! Essentials

Tutorías en Directo

Solicita tu admisión en:
+34 96 109 44 44
admisiones@escueladegobierno.es
<https://escueladegobierno.es>

21001: 2018
ISO EDUCATION ORGANIZATIONS MANAGEMENT SYSTEMS



21001: 2018
EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS

Deja de perder el tiempo intentando Gestionarlo
y aprende definitivamente a Gobernarlo.



Time Slot Governance TSG4 White Belt
Porque lo que no es Método es Improvisación

