

“Radio Security”

ESPECIAL

DE **Tecnología & Sentido Común**



ESPECIAL

AGOSTO
2026

La ciberseguridad
de los sistemas
GNSS

08

Fraudes masivos
a golpe de SMS,
la técnica del SMS
BLASTING

12

Seguridad en
los sistemas
satelitales

16

El espacio ya
no es un
entorno seguro

20

El espacio ya no
es un entorno
seguro (II)

24

El nuevo campo
de batalla no se
ve, se transmite

28

La lucha contra
los SMS Blasters
continúa

32

Ciberseguridad
a baja altitud

36

Inteligencia
de señales en
entornos hostiles

40

La transformación
silenciosa del SOC

44

El extraño caso de
las interferencias
aleatorias al sistemas
GNSS en Europa

48



ESPECIAL “Radio Security”

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 Administracion
Alex Aliaga - Radio Security
Marta Martín - Mentas 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



ALEX ALIAGA

Profesional Especializado en la Gestión de la seguridad, tanto desde el punto de vista tecnológico como desde el punto de vista estratégico. Con más de 20 años de experiencia en el sector, ha trabajado tanto en España como en otros países ayudando a las empresas en la gestión, y mitigación de los riesgos TIC, aplicando siempre las mejores prácticas y controles para aportar siempre la protección adecuada. Es colaborador habitual en diversos congresos de seguridad, así como, medios de comunicación, radio y prensa escrita, a nivel internacional donde sus publicaciones técnicas y estratégicas son muy apreciadas. Puede hablarte de ciberseguridad en 3 idiomas.

(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€
- Tareas 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€
- Tareas 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€
- Tareas 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€
- Tareas 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€
- Tareas 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€
- Tareas 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€
- Tareas 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€
- Tareas 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€
- Tareas 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€
- Tareas 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€
- Tareas 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€
- Tareas 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>



**Seguridad en los
sistemas satelitales**



**El espacio ya no es un
entorno seguro (II)**



**Ciberseguridad
a baja altitud**



**La transformación
silenciosa del SOC**

Copyright

02

Índice de Contenidos

04

Este mes te recomiendo leer...

por JAVIER PERIS

07

La ciberseguridad de los sistemas GNSS

08

Fraudes masivos a golpe de SMS, la técnica del SMS BLASTING

12

Seguridad en los sistemas satelitales

16

El espacio ya no es un entorno seguro

20

El espacio ya no es un entorno seguro (II)

24

El nuevo campo de batalla no se ve, se transmite

28

La lucha contra los SMS Blasters continúa

32

Ciberseguridad a baja altitud

36

Inteligencia de señales en entornos hostiles

40

La transformación silenciosa del SOC

44

El extraño caso de las interferencias aleatorias al sistemas GNSS en Europa

48

El Liderazgo de la Mujer en la Normalización

NORMALIZACIÓN

52

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

EVENTOS

56

Index

#TYSC

Premios recibidos



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



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

itSMF
ESPAÑA

Premio 2022 ESET al Periodismo y Divulgación en Seguridad Informática



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

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

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

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



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



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



Agradecimiento de la Asociación Valenciana de Informática Sanitaria AVISA



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



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



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



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**



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

La ciberseguridad de los sistemas GNSS

Arrancamos una nueva temporada con la misma pasión de siempre y muchas ganas de compartir contenido técnico, útil y riguroso. En los próximos artículos exploraremos temas clave en el ámbito de la tecnología y las radiocomunicaciones, analizando avances, retos y casos prácticos que marcan el pulso del sector. Si te interesan los sistemas críticos, la innovación aplicada y los entornos operativos exigentes, estás en el lugar adecuado.

La ciberseguridad en los sistemas GNSS: una cuestión crítica para las infraestructuras espaciales

Los sistemas GNSS (Global Navigation Satellite System) son un pilar fundamental de nuestras sociedades digitalizadas. No hablamos solo de la navegación en smartphones o vehículos; su funcionalidad trasciende lo cotidiano y se extiende a sectores estratégicos como la aviación, la logística, la sincronización de redes eléctricas, la emisión de TDT o la gestión de flotas. GPS es el más conocido, pero no el único: el sistema europeo GALILEO, el ruso GLONASS y el chino BeiDou forman parte de este ecosistema global que nos proporciona datos de posicionamiento y temporización en tiempo real.

Estos sistemas dependen de una constelación de satélites que orbitan la Tierra, y que, junto a estaciones terrestres y segmentos de control, forman parte de lo que debemos considerar como una infraestructura crítica. Su correcto funcionamiento no solo sostiene servicios básicos, sino que también da soporte a operaciones de defensa, control de

fronteras o monitorización de emergencias. Sin embargo, su creciente exposición a ciberamenazas ha convertido la protección de estas infraestructuras en un asunto urgente.

Amenazas reales, consecuencias críticas
Durante años, los sistemas GNSS se consideraban lo suficientemente aislados o robustos como para resistir ataques dirigidos. Esa visión, a día de hoy, resulta ingenua. Los incidentes que han afectado a estos sistemas, algunos documentados con detalle, evidencian que el coste técnico y económico de interferirlos ha descendido notablemente.

Una de las amenazas más frecuentes es el spoofing, una técnica de suplantación mediante la cual se emiten señales GNSS falsas que confunden a los receptores, alterando su percepción de la ubicación o el tiempo. Esto permite, por ejemplo, desviar la ruta de un buque, redirigir drones o falsear registros de posicionamiento. El caso del petrolero británico Stena Impero, desviado en el Estrecho de Ormuz, o los continuos ataques registrados en Ucrania tras la invasión rusa, son ejemplos muy claros de su uso con fines estratégicos.



CONTINÚA EN
PRÓXIMA PÁGINA





El jamming, por su parte, se basa en la emisión de señales de RF para saturar o enmascarar las legítimas, provocando denegaciones de servicio.

Es una técnica ampliamente conocida, pero no por ello menos eficaz, especialmente en entornos donde la disponibilidad de señal es crítica. En su variante más sofisticada, conocida como meaconing, el atacante graba señales auténticas y las reemite con retardo y mayor potencia, induciendo errores en los receptores. La reciente interferencia en los sistemas de navegación de aviones comerciales en el Pacífico Occidental, en el contexto de la tensión geopolítica con China, ilustra la dimensión global del problema.

Estos ataques no son teoría ni ejercicios de laboratorio. El ataque contra el sistema KA-SAT de Viasat, perpetrado el 24 de febrero de 2022 — horas antes del inicio de la ofensiva militar rusa en Ucrania—, supuso la desconexión de miles de terminales satelitales en Europa y afectó incluso a parques eólicos en Alemania, donde más de 5.800 turbinas perdieron la conectividad. Una acción quirúrgica que evidencia cómo una única operación puede comprometer al mismo tiempo servicios civiles y capacidades críticas de defensa.

Una defensa que debe ser sistémica

Proteger el entorno GNSS no implica únicamente reforzar los propios satélites. Hay que considerar toda la arquitectura: segmentos espaciales, redes terrestres, estaciones de control, software, firmware y canales de comunicación. Esta visión integral es la única que permite reducir la superficie de ataque real.

La Unión Europea, consciente de esta necesidad, está impulsando iniciativas que refuerzan la resiliencia satelital y la soberanía tecnológica. El proyecto IRIS², aprobado recientemente por el Parlamento Europeo, persigue desplegar una constelación de satélites seguros que garanticen comunicaciones cifradas, resistentes a ciberataques y accesibles para usos civiles, institucionales y de defensa. Es un paso decisivo para no depender exclusivamente de sistemas extranjeros y para mitigar los riesgos asociados a posibles interferencias o manipulaciones externas.

Además, existen iniciativas como el proyecto STRIKE³, cuya finalidad es analizar de forma sistemática la actividad interferente sobre las señales GNSS a nivel mundial. Este proyecto ha logrado identificar más de 50.000 eventos intencionados de interferencia, agrupados en más de 300 patrones diferenciados. A partir de esta caracterización, se trabaja en la estandarización de mecanismos de detección y respuesta frente a este tipo de ataques, así como en el desarrollo de bancos de pruebas que evalúen la resistencia de los receptores GNSS frente a amenazas reales.

La ciberseguridad satelital no es opcional

La dependencia de los servicios GNSS es absoluta en sectores como el transporte marítimo, la aviación, la gestión del espacio aéreo, los sistemas financieros, la sincronización de redes eléctricas, la localización de personas, o la respuesta ante emergencias. El impacto de una disrupción coordinada puede alcanzar dimensiones catastróficas. Un estudio del gobierno británico estimó que una caída de los sistemas GPS podría provocar pérdidas económicas superiores a los 1.000 millones de dólares diarios durante los primeros cinco días.

Por tanto, proteger los satélites y las redes GNSS debe considerarse una prioridad dentro de cualquier estrategia nacional de ciberseguridad. Esta protección pasa necesariamente por introducir capacidades de detección temprana, análisis de inteligencia de amenazas, automatización de respuesta ante incidentes y un robusto programa de pruebas frente a técnicas de spoofing, jamming o manipulación remota de los controladores terrestres.

El uso de inteligencia artificial, la monitorización constante del espectro radioeléctrico y la colaboración internacional para el intercambio de señales anómalas son pilares que deben formar parte de cualquier hoja de ruta estratégica.

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**

Fraudes masivos a golpe de SMS, la técnica del SMS BLASTING

El ecosistema global de telecomunicaciones móviles atraviesa una fase crítica marcada por la intensificación de ciberamenazas que explotan vulnerabilidades “legacy” heredadas de versiones anteriores del protocolo GSM. A pesar de la modernización progresiva hacia redes 5G, la persistencia de 2G en algunas ubicaciones, como tecnología de respaldo mantiene abierta una puerta que los ciberdelincuentes están aprovechando con eficiencia.

Dentro de este contexto, debemos destacar el reciente auge de los denominados “sms blasters”, dispositivos capaces de emular estaciones base falsas para inyectar mensajes SMS maliciosos directamente en los terminales de los usuarios, se ha convertido en un fenómeno técnico y operativo que redefine el panorama del fraude digital.

No es algo que deba sorprendernos, la llegada de los llamados “SMS Blasters” marca un antes y un después en las posibilidades del cibercrimen y los retos a los que nos enfrentamos los defensores. Atrás quedaron los días en que los filtros de los operadores bastaban para detener el fraude por mensajes de texto. Organizaciones criminales en Europa y Asia han perfeccionado el uso de falsas estaciones base portátiles, capaces de enviar cientos de miles de mensajes fraudulentos por hora, completamente fuera del alcance de

los controles tradicionales y generando millones de víctimas potenciales en zonas urbanas de alta densidad.

Los SMS Blasters explotan vulnerabilidades en el protocolo GSM, en particular, la falta de autenticación mutua y de un cifrado robusto en conexiones cuando estas son forzadas a usar la red 2G. Lo más perturbador es la simplicidad con la que el ataque puede desplegarse: basta con un dispositivo del tamaño de una torre de PC y un sistema de alimentación portable para su emisión. Los atacantes operan desde furgonetas, mochilas o bicicletas, eligiendo ubicaciones con alta concentración de teléfonos.

Este renacimiento del smishing –mucho más directo y difícil de bloquear– obliga a los operadores, fabricantes de dispositivos y empresas de ciberseguridad a repensar todo el modelo de detección y respuesta frente a este tipo de ataques.

No nos cansaremos en esta sección, de demostrar que la ciberseguridad va más allá del protocolo IP y las redes, existen ataques no convencionales” como el que se muestra en este artículo que demuestra la necesidad de explorar este tipo de vectores de ataque en los sistemas de comunicaciones.



CONTINÚA EN
PRÓXIMA PÁGINA



Cómo opera un dispositivo SMS BLASTER

A nivel físico, un SMS Blaster consiste en una estación base falsa equipada con un sistema de transmisión de alta potencia y múltiples antenas. El dispositivo emula la presencia de una estación base legítima (BTS), presentando al UE una señal más fuerte que la que le ofrece su operador de telefonía móvil, lo que fuerza a los teléfonos a conectarse automáticamente e incluso a degradarse a la red 2G cuando originalmente operaban bajo 4G o 5G.

Una vez que el dispositivo móvil ha realizado el "handover" (cambio de estación móvil), la estación falsa generada por el atacante, aprovecha la ausencia de autenticación mutua –la característica que solo es obligatoria en 3G, 4G y 5G– para enviar mensajes SMS arbitrarios con remitentes suplantados y contenido fraudulento.

El atacante no necesita conocer los números de teléfono de las víctimas: cualquier móvil en el radio de acción recibirá el mensaje al conectarse a la falsa estación. Esto elimina la necesidad de bases de datos filtradas de usuarios y hace viable la operación cibercriminal a escala masiva. En ataques recientes, se han reportado casos de uso en furgonetas camufladas que enviaron un millón de mensajes en tres días, con los equipos operando desde el maletero y moviéndose de un punto a otro de la ciudad

Ataques cada vez más frecuentes

El fenómeno del sms blasting ha dejado de ser anecdótico para convertirse en una tendencia global documentada en múltiples jurisdicciones. En Corea del Sur, el ataque a KT supuso la primera brecha confirmada de este tipo en el país, con cerca de 19.000 dispositivos afectados en un solo incidente. La magnitud del evento obligó a las autoridades a replantear sus mecanismos de monitorización de tráfico.

En Reino Unido, la condena de un estudiante chino por desplegar un blaster en el maletero de un vehículo en Londres demostró la facilidad con la que estos dispositivos pueden integrarse en la vida urbana sin levantar sospechas. Casos similares en Nueva Zelanda, Tailandia, Indonesia y Omán refuerzan la naturaleza transnacional de la amenaza y la participación recurrente de actores vinculados a organizaciones chinas.

Japón, tradicionalmente cauto en su aproximación a incidentes de telecomunicaciones, emitió en 2025 una alerta pública tras detectar sms blasters activos en Tokio y Osaka. Filipinas y Brasil también han reportado múltiples arrestos, lo que indica que la amenaza no distingue entre mercados emergentes y desarrollados. En Bangkok, las autoridades capturaron a un grupo criminal que, desde una furgoneta adaptada con una

estación base, envió casi un millón de mensajes en tres días empleando suplantación avanzada de bancos y simulando sitios web personalizados

Implicaciones de seguridad de este tipo de ataques

Los ataques mediante SMS Blaster representan una amenaza significativa para la seguridad tanto de las infraestructuras móviles como de los usuarios finales. El usuario muchas veces no percibe que sus mensajes provienen de una red fraudulenta, ya que el SMS Blaster puede replicar metadatos y campos de remitente para simular al banco, gobierno u otros servicios confiables, dificultando la detección manual del ataque y aumentando la efectividad del ataque.

Una vez más, es importante la formación y concienciación en materia de ciberseguridad al usuario final para evitar que este caiga en engaños. Una buena higiene en ciberseguridad cada vez es más necesaria; como usuarios de sistemas de comunicaciones debemos conocer a qué riesgos nos enfrentamos y cómo podemos defendernos.

Conclusión

El carácter ubicuo y portátil de estos dispositivos ha permitido su uso -que conocemos- en ciudades de Asia, Europa y América Latina, multiplicando la escala y la velocidad de las campañas de los cibercriminales. El hecho de que ataquen simultáneamente a cualquier terminal dentro de su área de influencia –sin conocer previamente los números de teléfono–, convierte este vector en una amenaza impredecible y masiva. Esta técnica, por tanto, sienta un preocupante precedente: los sistemas de filtrado, bloqueo y monitorización, largo tiempo perfeccionados por las operadoras de telecomunicaciones, resultan en estos casos inútiles, pues los mensajes jamás pasan por las infraestructuras protegidas. Además de dejar latente la necesidad de invertir mucho más en ciberseguridad orientada a protocolos de comunicaciones más allá del wireless, bluetooth, etc.

Desde la perspectiva del usuario final, la situación es aún más delicada. La imposibilidad técnica de detectar manualmente si el mensaje proviene verdaderamente de un operador, banco o servicio gubernamental incrementa el riesgo de engaño. La suplantación de remitentes y la personalización de los textos con ingeniería social avanzada facilita el robo de credenciales, datos personales y códigos de autenticación, abriendo la puerta al fraude financiero, secuestro de datos y pérdida de privacidad en tiempo real.

Además, la migración forzada a redes 2G y la explotación de vulnerabilidades históricas del protocolo GSM reafirman la urgencia de abandonar tecnologías legacy y blindar los dispositivos ante todo tipo de conexión sospechosa.

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

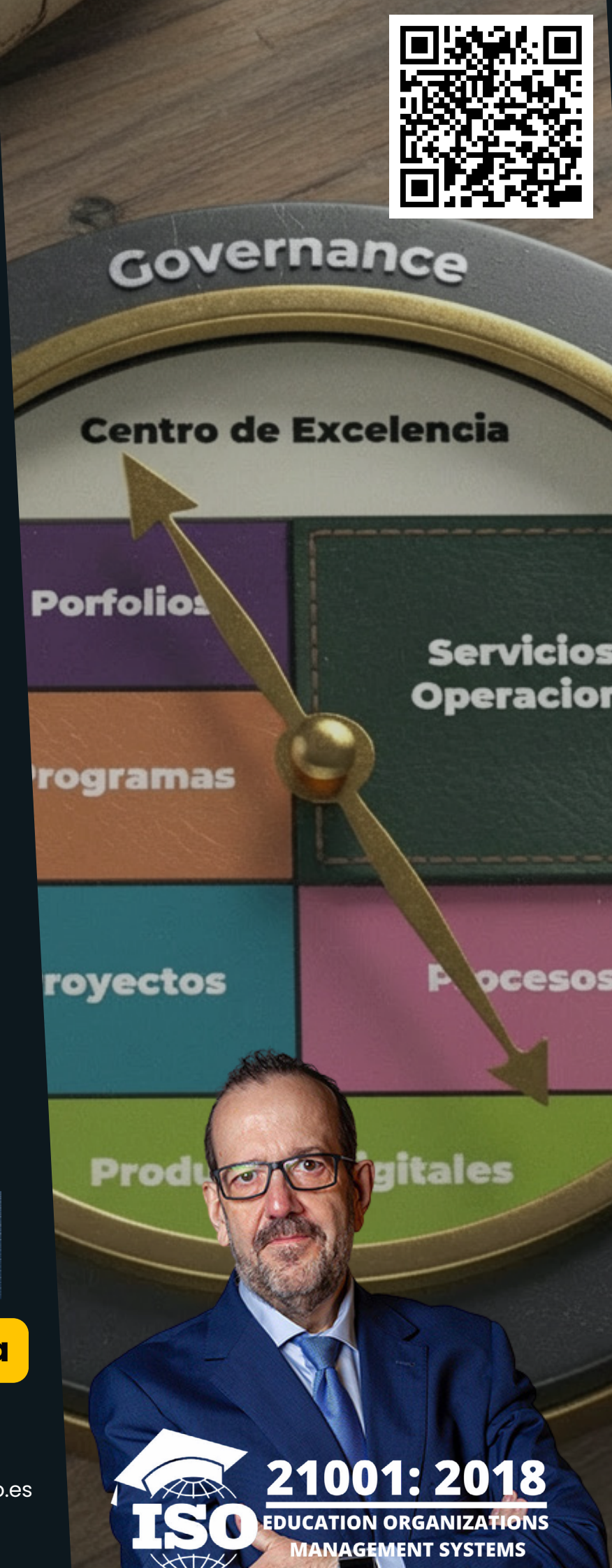
admisiones@escueladegobierno.es

<https://escueladegobierno.es>



21001:2018

**EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS**





Seguridad en los sistemas satelitales

Desde el lanzamiento del Sputnik 1 el 4 de octubre de 1957, la humanidad no solo ha conquistado el espacio, sino que ha tejido una red de dependencia a su alrededor. Hoy, los satélites son los encargados de las comunicaciones transoceánicas, la vigilancia del medio ambiente y el sostenimiento de los sistemas PNT (Positioning, Navigation, and Timing), que son la base del funcionamiento de nuestras sociedades, desde el GPS hasta las transacciones financieras.

A lo largo de todas las publicaciones de esta sección, hemos venido advirtiendo que estos activos orbitales se están convirtiendo en un eslabón crítico y frágil dentro de la cadena de seguridad mundial. La OTAN no solo comparte esta apreciación, sino que la ha formalizado y elevado a la categoría de alerta estratégica con la publicación de su documento *Cybersecurity of NATO's Space-based Strategic Assets*. La alianza atlántica reconoce así lo que los expertos señalan desde hace años: el espacio es un dominio operativo más, tan crucial y conflictivo como el terrestre, el marítimo o el cibernético.

La cruda realidad es que muchos de los sistemas militares estratégicos dependen, en gran medida, de activos basados en el espacio para funciones de inteligencia, vigilancia, reconocimiento y mando y control. Y, sin embargo, persiste una brecha alarmante entre la dependencia y la protección. Aunque la concienciación

va en aumento, las estaciones terrestres —los puntos de anclaje con la Tierra—, los complejos sistemas de mando y control, y el personal asociado a la gestión y operación de estas instalaciones, constituyen un vector de amenazas subestimado que demanda, con urgencia, protocolos más estrictos y controles de seguridad reforzados.

Una lectura detenida del documento de la OTAN revela una necesidad imperiosa de estudiar y abordar de forma coordinada los retos de ciberseguridad que afectan a estos activos estratégicos, tanto para la organización como para sus estados miembros. Esta urgencia se ha visto ratificada por las lecciones extraídas del conflicto entre Rusia y Ucrania, donde la guerra electrónica y los ataques cibernéticos contra infraestructuras espaciales han dejado de ser una hipótesis teórica para convertirse en una realidad operativa.

Investigaciones sobre la seguridad de las comunicaciones: La ilusión de la protección

En el núcleo de este problema yace una suposición generalizada —y peligrosamente errónea—: la creencia de que todos los enlaces por satélite están, por defecto, altamente protegidos y cifrados debido a la naturaleza crítica de sus misiones.



CONTINÚA EN
PRÓXIMA PÁGINA



Sin embargo, un reciente y meticuloso estudio llevado a cabo por un equipo de investigadores de ciberseguridad ha desmantelado esta premisa, revelando una realidad tan alarmante como generalizada: aproximadamente el 50% de estos enlaces transportan tráfico IP en texto claro. Esta práctica expone flujos de datos internos de alta sensibilidad a cualquier atacante pasivo con un equipo de consumo relativamente asequible, sin necesidad de capacidades estatales sofisticadas.

Los hallazgos del equipo de investigadores son una prueba tangible de la necesidad de replantearse la seguridad de los sistemas satelitales.

Lograron capturar y decodificar datos de una sensibilidad extrema: llamadas de voz y mensajes de texto de usuarios de varios operadores de comunicaciones; tráfico procedente de conexiones WiFi a bordo de aviones en pleno vuelo; comunicaciones operacionales de infraestructuras críticas, como plataformas petrolíferas *offshore*; e incluso transmisiones que revelaban en tiempo real la ubicación geográfica de personal, equipos e instalaciones sensibles.

Escaneando y decodificando los streams de datos: El arte de escuchar lo que no está cifrado

La metodología empleada por los investigadores demuestra la accesibilidad de esta vulnerabilidad. Para extraer la información del satélite y posteriormente decodificarla, los analistas utilizaron hardware convencional: una parabólica similar a las empleadas para la recepción de televisión por satélite y una tarjeta capturadora de señal satelital (DVB-SX). El verdadero trabajo, no obstante, radicó en el software. Para alcanzar sus objetivos, tuvieron que reescribir controladores específicos y desarrollar decodificadores personalizados capaces de extraer e interpretar las cabeceras y el payload (carga útil) de los mensajes. Fue un proceso de ingeniería inversa metódico, tras el cual los resultados comenzaron a emerger de forma alarmante.

Uno de los servicios más críticos que lograron decodificar fue el de Voz sobre IP (VoIP). Observaron grandes volúmenes de tráfico no cifrado de varios operadores, transmitido sin la protección básica de un túnel IPsec. En una captura de apenas dos minutos, se registraron 142 conversaciones de voz completas, acompañadas de sus metadatos asociados: identidades de llamante y destinatario (números de teléfono completos), servidores SIP involucrados y detalles técnicos sobre los códecs de compresión utilizados.

A través de otros *streams* de datos, la exposición fue aún más grave. Los investigadores fueron testigos de inicios de sesión realizados a través del protocolo Telnet —notoriamente inseguro y no cifrado— dirigidos a un sistema de gestión de inventario. Este descuido permitió la captura de credenciales de acceso en texto claro, entregando las llaves digitales de sistemas potencialmente críticos a cualquier espía pasivo.

Conclusiones

Más allá de la mera exposición de datos sensibles, el estudio subraya una lección estratégica de primer orden: la protección que realizamos en las estaciones terrenas puede no ser suficiente si el eslabón satelital permanece desprotegido. Se hace necesaria la realización de auditorías de seguridad exhaustivas y continuadas sobre estos sistemas, como paso previo e indispensable para definir un plan de acción que aplique medidas y controles de seguridad robustos, diseñados específicamente para estos protocolos y, en concreto para el segmento espacial.

Como ya reflejaba el artículo de la OTAN, existe una necesidad urgente de estudiar y abordar los retos de ciberseguridad de estos activos que, en la mayoría de los casos, son de naturaleza estratégica. Este estudio no es un caso aislado; es un punto más en una cadena de evidencias. En la historia reciente existen numerosos casos documentados de “hacks” a sistemas satelitales, desde la toma de control de satélites de observación terrestre hasta la interrupción masiva de servicios como el sufrido por la red Viasat al inicio del conflicto en Ucrania.

Desde esta tribuna, una vez más, queremos incidir en la preocupante urgencia de abordar estos retos de forma decidida. Mejorar la seguridad de las comunicaciones globales exige una mirada que vaya más allá de los protocolos ampliamente conocidos y auditados en entornos corporativos. Es imperativo concienciar a la industria, a los gobiernos y a la ciudadanía de que la ciberseguridad debe extenderse también a esos protocolos de comunicaciones inalámbricas menos comunes, pero no por ello menos críticos. El espacio, la última frontera, se ha convertido en nuestro nuevo y más expuesto flanco de seguridad. Ignorarlo no es una opción.

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**

El espacio ya no es un entorno seguro

Desde el lanzamiento del Sputnik1, el 4 de octubre de 1957, la humanidad ha utilizado el espacio con fines de comunicaciones, vigilancia del medio ambiente, realización de experimentos científicos, sistemas PNT (Position, Navigation and Timing), entre muchos otros fines.

A lo largo de todas las publicaciones de esta sección de la revista, ya comentábamos que los satélites se están convirtiendo en un punto frágil dentro de la cadena de seguridad mundial. Y, no es de extrañar, que la OTAN lo haga constar a través de la publicación del documento Cybersecurity of NATO's Space-based Strategic Assets.

Muchos de los sistemas militares estratégicos dependen, en gran medida, de activos basados en el espacio. Y es que, aunque cada vez existe más conciencia, las estaciones terrestres, los sistemas de mando y control y el personal asociado a la gestión y operación de estas instalaciones todavía necesitan más atención y mayores controles de seguridad.

Si leemos con atención el documento, podremos observar que existe una necesidad urgente de estudiar y abordar los retos relacionados con la ciberseguridad de estos activos estratégicos dentro de la OTAN y de sus estados miembros; mucho más tras los eventos que se han producido durante el conflicto entre Rusia y Ucrania.

Investigaciones sobre la seguridad de las comunicaciones

Y es que, a pesar de la sensibilidad de los datos transmitidos, existe una suposición generalizada —y peligrosamente errónea— de que todos estos enlaces por satélite están altamente protegidos. Sin embargo, un reciente estudio llevado a cabo por investigadores de ciberseguridad revela una realidad alarmante: aproximadamente el 50% de estos enlaces transportan tráfico IP en texto claro, exponiendo flujos de datos internos de alta sensibilidad a cualquier atacante pasivo con equipo de consumo.

Los investigadores lograron capturar datos realmente sensibles como llamadas y mensajes de texto de usuarios de T-Mobile en EE.UU., tráfico procedente de conexiones WiFi a bordo de aviones, comunicaciones procedentes de infraestructuras críticas como, por ejemplo, plataformas petrolíferas offshore, e incluso transmisiones que revelaban ubicaciones de personal, equipos e instalaciones.



CONTINÚA EN
PRÓXIMA PÁGINA





Escaneando y decodificando los streams de datos

Para conseguir extraer la información del satélite y decodificarla, los analistas usaron una parabólica como las que se usan para la recepción de televisión por satélite y una tarjeta capturadora de satélite (DVB-SX). Para conseguir sus objetivos, tuvieron que reescribir algunos drivers y generar decodificadores para extraer las cabeceras y el payload de los mensajes. Tras esta tarea, poco a poco los resultados fueron apareciendo y se consiguió obtener información muy diversa.

Uno de los servicios que pudo decodificarse fue el servicio de Voz sobre IP (VoIP). Se observó tráfico no cifrado de varios operadores que era transmitido sin un túnel IPsec. En una captura de solo 2 minutos se registraron 142 conversaciones de voz, junto con metadatos como identidades de llamante/llamado (números de teléfono), servidores SIP y detalles de códecs.

A través de otros streams de datos, los investigadores observaron inicios de sesión a través de **telnet no cifrado** a un sistema de gestión de inventario, lo que revelaba credenciales en texto claro, entre muchos otros datos.

Conclusiones

Más allá del impacto evidente de la exposición de datos, queda patente, que proteger los enlaces satelitales no es una opción, y que urge tomar medidas urgentemente; medidas que como auditorías exhaustivas que permitan definir planes de acción concretos. No hablamos

de recomendaciones abstractas, ni de acciones que puedan quedarse sin aplicar, hablamos de la aplicación de medidas y controles que cierren brechas reales y eviten que actores malintencionados sigan aprovechando estos fallos estructurales. Quizás no seamos conscientes, pero el espacio se ha convertido en un nuevo campo de batalla para las grandes potencias y, como es habitual, los ciberdelincuentes tratarán de explotarlo.

El propio documento de la OTAN así lo reflejaba: la ciberseguridad de estos activos estratégicos sigue siendo un reto pendiente. Y no es un caso aislado. Como ya venimos advirtiendo en esta sección, la historia reciente acumula múltiples ejemplos documentados de intrusiones, interferencias y “hackeos” contra sistemas satelitales que muchos consideraban intocables.

Desde esta tribuna queremos insistir en la urgencia de actuar con un objetivo claro, generar una cultura de ciberseguridad que va más allá de los límites habituales. La seguridad de las comunicaciones ya no puede limitarse a proteger solo los protocolos más conocidos y auditados. Es imprescindible ampliar el foco y blindar también aquellos protocolos inalámbricos menos visibles, pero igual de necesarios para sostener operaciones críticas. Ignorarlos nos expone a un riesgo que, como demuestra esta investigación, es tan real como evitable.

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**



El espacio ya no es un entorno seguro (II)

En el artículo anterior analizábamos cómo el espacio ha dejado de ser un dominio neutro para convertirse en un nuevo campo de batalla, un entorno donde la tecnología, la geopolítica y la ciberseguridad convergen de forma cada vez más evidente. Lejos de la imagen romántica de la exploración espacial, la órbita terrestre se ha transformado en una infraestructura crítica global, indispensable para el funcionamiento de las sociedades modernas y, por tanto, en un objetivo prioritario en cualquier escenario de conflicto entre estados.

Entre aquel primer análisis y este segundo, se ha producido un hecho especialmente revelador que confirma esta tendencia y acelera el debate estratégico: China ha llevado a cabo simulaciones destinadas a estudiar cómo podría interrumpir el funcionamiento de la red de satélites Starlink, la megaconstelación desplegada por SpaceX en órbita baja. El matiz es importante, porque no se trata de destruir físicamente los satélites —una acción de alto impacto político y técnico—, sino de algo mucho más sutil, flexible y acorde con la lógica de los conflictos modernos: aprender a “silenciar” la red de forma localizada y temporal si la situación geopolítica así lo requiriera.

Este enfoque revela una realidad que ya resulta imposible de ignorar. Starlink ha dejado de ser únicamente un servicio comercial de conectividad para zonas remotas y se ha consolidado como un activo estratégico de primer orden. Su papel en la guerra de Ucrania fue decisivo para mantener operativas comunicaciones críticas cuando las infraestructuras terrestres habían sido destruidas o inutilizadas. En ese contexto, una red privada, gestionada por una empresa, fue capaz de influir de manera directa en la resiliencia operativa de un país en guerra, alterando el equilibrio táctico sobre el terreno.

China observa con atención esa capacidad, especialmente en relación con un posible escenario de tensión o conflicto en torno a Taiwán. En ese marco, el acceso a comunicaciones seguras, resilientes y difíciles de degradar se convierte en un factor clave. De ahí el desarrollo de técnicas de guerra electrónica orientadas a interferir señales satelitales mediante enjambres de interferencia, plataformas aéreas de gran altitud o tecnologías de energía dirigida. No hablamos de ciencia ficción, sino de capacidades que ya se están probando y que encajan perfectamente en las doctrinas modernas de negación de acceso y control del espectro electromagnético.



**CONTINÚA EN
PRÓXIMA PÁGINA**



Un nuevo campo de batalla

Este movimiento no es aislado. A la luz de lo ocurrido en Ucrania, los estados-nación están adaptando con rapidez sus doctrinas militares para competir en el espacio, un dominio que sigue estando, en gran medida, poco regulado y donde conviven satélites civiles, comerciales y militares en un equilibrio cada vez más frágil. La órbita terrestre, especialmente la órbita baja, se encuentra ya saturada y alberga sistemas esenciales para la navegación, la observación de la Tierra, la predicción meteorológica, las comunicaciones, la sincronización temporal y la toma de decisiones estratégicas.

Muchos de estos satélites han sido ya víctimas de ciberataques, interferencias o intentos de compromiso de sus segmentos terrestres, como se ha documentado en distintos incidentes en los últimos años. Esta tendencia no solo continuará, sino que previsiblemente se intensificará. El ataque directo y visible contra un satélite sigue siendo una opción extrema, mientras que el ciberespacio ofrece una vía más discreta, negable y eficaz para degradar capacidades sin cruzar determinadas líneas rojas diplomáticas.

En esta carrera espacial 2.0, las capacidades cibernéticas desempeñan un papel central. Los adversarios no solo buscarán interceptar información sensible, sino también interrumpir operaciones, degradar servicios o introducir incertidumbre en la cadena de mando y control. Las estaciones terrestres, los enlaces de comunicación, los centros de procesamiento de datos y los sistemas de monitorización se convierten en objetivos tan valiosos como los propios satélites.

Por este motivo, las organizaciones y empresas vinculadas al sector espacial deben situar la ciberseguridad como un eje prioritario de sus estrategias. Y cuando hablamos de ciberseguridad en el espacio, no nos referimos únicamente al satélite como elemento aislado, sino a todo

el ecosistema que lo rodea. La famosa supply chain, una vez más, emerge como uno de los vectores de ataque más atractivos para los adversarios.

La industria espacial depende de una cadena de suministro extremadamente compleja, que incluye fabricantes de hardware especializado, desarrolladores de software, integradores, operadores de red y proveedores externos de servicios. Cada uno de estos eslabones representa una posible puerta de entrada. Si un actor malicioso logra comprometer un componente aparentemente menor, puede introducir vulnerabilidades persistentes en sistemas que, una vez lanzados al espacio, son muy difíciles —o directamente imposibles— de parchear o sustituir. En el ámbito espacial, las consecuencias de un fallo de seguridad pueden ser desproporcionadas y afectar a múltiples países y sectores simultáneamente.

Implicaciones estratégicas y dependencia tecnológica

La clave de todo este escenario no reside únicamente en el detalle técnico, sino en lo que revela a nivel geopolítico. Por primera vez en la historia, el espacio se comporta como una infraestructura estratégica global plenamente integrada en nuestra vida cotidiana. Desde las comunicaciones a la agricultura de precisión, desde la logística global a la gestión de emergencias, desde la defensa hasta la economía digital, dependemos de señales invisibles que descienden desde la órbita. Y esas señales pueden ser interferidas, degradadas o controladas.

Al mismo tiempo, emerge con fuerza el debate sobre la soberanía tecnológica. Para Europa, depender de una red privada, global y controlada por un actor externo como pueda ser Starlink, plantea preguntas incómodas pero inevitables. ¿Quién gobierna realmente la infraestructura espacial de la que depende nuestra economía digital? ¿Qué margen de maniobra existe en caso de crisis? ¿Qué capacidades propias deben desarrollarse para garantizar autonomía estratégica en el espacio?

El cielo deja así de ser un espacio neutro y se transforma en un territorio de rivalidad abierta. La órbita baja ya no es solo un ámbito técnico, sino el escenario donde se disputa el flujo de información global. Cada satélite, cada antena, cada terminal terrestre se convierte en una pieza de un tablero geopolítico en constante movimiento, donde la ventaja no siempre la otorga la fuerza bruta, sino la capacidad de interferir, degradar y resistir.

La pregunta que se impone es inevitable: ¿estamos preparados para un mundo en el que la geopolítica también se libra en órbita y donde el espacio resulta tan determinante como el suelo que pisamos?

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

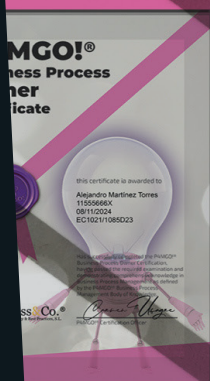
Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>



21001:2018
EDUCATION ORGANIZATIONS
MANAGEMENT SYSTEMS



El nuevo campo de batalla no se ve, se transmite

Durante décadas, la radio ha sido sinónimo de fiabilidad. Invisible, silenciosa y omnipresente, ha sostenido la aviación civil, la navegación marítima, los sistemas de emergencia y buena parte de la infraestructura crítica global sin levantar sospechas.

Sin embargo, esa confianza histórica empieza a resquebrajarse. Hoy, las señales de radio ya no son únicamente un medio de comunicación: se han convertido en un vector de ataque tal y como hemos ido reflejando en esta sección a lo largo de múltiples artículos.

Como ya hemos visto en artículos anteriores, las señales de radio no solo transportan datos. En muchos sistemas modernos, forman parte indispensable de infraestructuras críticas. Determinan, entre otras muchas funciones, dónde está un avión, cuándo aterriza, qué ruta sigue un barco o cómo se sincroniza una red eléctrica.

Estos sistemas funcionan porque los receptores confían en lo que reciben. Interpretan que una señal con la frecuencia correcta, la modulación esperada y la estructura válida es legítima. Pero hoy en día, y como ya hemos visto en artículos anteriores, ya no podemos fiarnos de lo que recibimos, los ciberdelincuentes han encontrado la manera de suplantar señales reales para realizar actos ilícitos que pueden tener consecuencias desastrosas.

Lo inquietante es que esta debilidad no es teórica. En la actualidad, las señales no siempre llevan una "firma" que permita distinguir lo auténtico de lo falso. Para un receptor estándar, una señal bien construida es indistinguible de la real,

aunque haya sido generada desde una habitación con un SDR conectado a un portátil.

Los SDR, un arma de doble filo

Actualmente, un SDR comercial, software libre y conocimiento técnico bastan para reproducir ataques funcionales. El SDR actúa como una navaja suiza de la radiofrecuencia. Permite generar cualquier señal, en casi cualquier banda, con control total sobre modulación, fase y potencia. En manos defensivas es una herramienta de análisis formidable. En manos maliciosas, se puede convertir en un arma que puede tener impacto en el mundo físico.

La barrera ya no es económica, sino intelectual. Y ese conocimiento está publicado, documentado y enseñado. Esto obliga a replantear el modelo de seguridad: no se puede basar en la dificultad técnica cuando la técnica se ha democratizado.

Este problema no es solo tecnológico. Es estratégico. Afecta a infraestructuras críticas, a la seguridad aérea y a la resiliencia de sistemas civiles en contextos de crisis o conflicto híbrido. Ignorarlo no lo hará desaparecer.

De la teoría a la práctica: ataques reales

Las noticias más recientes confirman que la interferencia deliberada de señales GNSS no es solo una posibilidad técnica, sino un fenómeno que está ocurriendo en el mundo real.



CONTINÚA EN
PRÓXIMA PÁGINA

En septiembre de 2025, el avión que transportaba a la presidenta de la Comisión Europea, **Ursula von der Leyen**, experimentó una importante pérdida de señal GPS mientras sobrevolaba Bulgaria, obligando a la aeronave a dar vueltas durante casi una hora antes de aterrizar con sistemas de navegación alternativos. Las autoridades europeas atribuyeron el incidente a interferencias de GPS que se sospecha provienen de emisiones deliberadas de radiofrecuencia, posiblemente relacionadas con actividades de guerra electrónica por parte de Rusia.

Este episodio no fue aislado. En 2024, otro vuelo con el entonces ministro de Defensa del Reino Unido, Grant Shapps, sufrió una interferencia similar cerca de Polonia, y varias aerolíneas reportaron fallos de navegación en vuelos entre Helsinki y Tartu.

En el ámbito marítimo, organizaciones como Windward han registrado **más de 13.000 buques con interferencias GPS**, con tramas AIS que muestran posiciones imposibles o movimientos erráticos que ponen en riesgo la seguridad de la navegación. El sistema **AIS**, que transmite posiciones de barcos por radio en VHF, es conocido por ser vulnerable a inyección de paquetes falsos o transmisiones maliciosas, permitiendo que un actor externo cree tramas de posición incorrectas.

No solo la navegación satelital está en el punto de mira. Las intrusiones en señales de radiodifusión o telecomunicaciones tradicionales son un caso práctico de manipulación. El **"broadcast signal intrusion"** se ha usado en radio y TV para secuestrar transmisiones legales utilizando transmisores que superan la potencia o interceptan frecuencias, algo que demuestra que incluso servicios de difusión masiva son vulnerables a interferencias intencionadas en radio.

Un ejemplo dramático no relacionado con GNSS o navegación pero centrado en radio como medio de control es el incidente de septiembre de 2024 en Líbano y Siria, donde miles de **walkie-talkies y pagers explotaron simultáneamente**, armas diseñadas para parecer dispositivos de comunicación y que lesionaron a miles, deshabilitando canales críticos de coordinación. Es importante entender que los sistemas afectados por interferencias o manipulación no se limitan a la aviación o la navegación marítima. El GNSS proporciona **tiempo preciso y sincronización** a redes eléctricas, sistemas de telecomunicaciones, servicios financieros (timestamps para transacciones), transporte terrestre y marítimo, logística y hasta redes de emergencias.

Esto significa que cualquier actor con acceso a equipamiento de transmisión adecuado puede, en teoría, interferir con estos sistemas, comprometiendo la disponibilidad de servicios esenciales o provocando errores operativos graves. La radio, antes vista como un recurso confiable, se ha convertido en un punto de fragilidad crítica que requiere atención urgente por



parte de los responsables de seguridad nacional y los operadores de infraestructuras estratégicas.

Las comunicaciones radio ya no son seguras, debemos prepararnos para protegerlas como un activo más

El aire que nos rodea está lleno de señales cuya integridad antes se daba por sentada. Hoy esa confianza se tambalea ante ataques reales. Las señales de radio, desde GPS hasta ADS-B, pueden ser bloqueadas, manipuladas o suplantadas por actores con habilidades técnicas crecientes y acceso a herramientas democratizadas.

Este fenómeno ya ha tenido efectos comprobados, desde interrupciones de navegación en vuelos de alto perfil hasta miles de incidentes diarios de interferencia en aviones civiles. Ignorar esta realidad no solo es imprudente, es incompatible con la seguridad de las sociedades altamente conectadas de hoy.

La ciberseguridad y la ciberdefensa deben extenderse más allá de los circuitos y las redes informáticas para proteger también **los canales físicos de comunicación que sustentan la operativa de nuestras infraestructuras más críticas**. La radio ya no es un sitio seguro por defecto; es un dominio que hay que defender con la misma intensidad con la que se protege cualquier red digital.

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**





La lucha contra los SMS Blasters continúa

Los dispositivos móviles se han convertido en el eje central de todas nuestras comunicaciones, y en un dispositivo esencial sin el que ya no sabemos vivir. Las personas y las organizaciones dependemos de estos dispositivos para desempeñar nuestra vida cotidiana y nuestro trabajo; nos permiten acceder a recursos del trabajo, de nuestro banco y, en muchas ocasiones, contienen información relevante de nuestras vidas personales y/o profesionales.

Tanto es así, que cada vez más, se han convertido en un objetivo para los ciberdelincuentes, que son conscientes de que contienen las llaves de acceso a mucha información personal y profesional de sus usuarios. Varias investigaciones de reputadas empresas lo demuestran, y ya en el 2023 una empresa de ciberseguridad muy conocida en el sector indicaba que pudo rastrear más de 34 millones de ataques a dispositivos móviles entre los que podemos destacar ataques de malware, fraude, etc.

A medida que los clientes y usuarios enfrentan un mayor riesgo cibernético, existe una necesidad urgente de examinar las amenazas, vulnerabilidades y oportunidades para mejorar la seguridad. Son muchas las preguntas que debemos hacernos como guardianes de la seguridad:

- Cuáles son las ciberamenazas de mayor prioridad contra los dispositivos móviles que aprovechan los delincuentes?
- ¿Por qué son vulnerables los dispositivos móviles?
- ¿Qué factores podrían cambiar la (in)seguridad de los dispositivos móviles en los próximos años?

Pero si hemos de destacar un ataque que está en plena ebullición, y del que ya hemos visto multitud de noticias es el "SMS Blasting"

¿Qué es un SMS BLASTER y cómo actúa?

Un SMS Blaster es un dispositivo **que se hace pasar por una estación base de telefonía móvil**, con tamaño aproximado a una antigua torre de ordenador y dotado de múltiples antenas. Los delincuentes suelen ocultarlo en el maletero de un coche, en una mochila o incluso integrarlo en entornos urbanos sin llamar la atención.

Una vez activado, el dispositivo **finje ser una antena legítima con señal más fuerte**, provocando que los móviles de la zona se conecten automáticamente a él. El rango de difusión suele estar entre **500 y 2.000 metros**, por lo que los atacantes prefieren actuar en zonas de alta densidad: centros comerciales, áreas turísticas, zonas de negocios o recintos donde se concentra mucha gente.



CONTINÚA EN
PRÓXIMA PÁGINA

En funcionamiento, el SMS Blaster **envía mensajes masivos sin necesidad de conocer números concretos ni pasar por las operadoras**, algo que se asemeja técnicamente al uso de un **IMSI Catcher**, aunque en este caso se explota para fraudes escalables.

Usos ilícitos más comunes

Los ciberdelincuentes han encontrado un uso malicioso muy rentable para esta tecnología, llevando a cabo campañas de **smishing** a gran escala. Algunos ejemplos de usos ilícitos son:

- **Phishing bancario:** mensajes del tipo “Su cuenta ha sido bloqueada, haga clic aquí para desbloquear”.

- **Estafas de paquetería:** “Su envío requiere pago urgente de gastos de aduana”.

- **Premios falsos:** “¡Ha ganado un iPhone! Complete sus datos para reclamarlo”.

- **Suplantación institucional:** mensajes apócrifos de Hacienda, Seguridad Social u otras administraciones.

En todos estos casos, los mensajes suelen enlazar a **páginas web falsas** donde se induce al usuario a introducir datos sensibles: credenciales bancarias, DNI, tarjetas, etc., lo que permite a los atacantes realizar fraude financiero o vender esos datos en mercados oscuros

Facilidad de acceso y mercado de equipos

Lo preocupante es que, a pesar de la naturaleza crítica de estos dispositivos, **la tecnología está disponible en el mercado** y se vende abiertamente (en algunas webs muy conocidas) como “difusor” o “sistema de notificación SMS”, muchas veces sin verificación de identidad del comprador ni control sobre el uso final.

Algunos kits comerciales ofrecen alcances de hasta varios kilómetros y capacidades de envío de **decenas de miles de SMS por hora**, con precios que, aunque altos para un usuario individual, son razonables para organizaciones criminales organizadas

Aunque no existen datos globales de ataques por SMS Blaster, sí se puede observar un **crecimiento explosivo del smishing** en general, que es el canal que estos dispositivos aprovechan y que está altamente explotado por los ciberdelincuentes que hacen uso de estos dispositivos:

- En los últimos tres años los **mensajes de phishing con enlaces maliciosos han aumentado un 119%**, y los intentos de **smishing se han disparado un 2.524%** en el mismo periodo.

- En 2023, **el smishing ya representaba el 28% del total de ataques de phishing**, situándose como uno de los principales vectores de fraude digital.

- A nivel mundial, se estima que en 2024 se recibieron **más de 147 millones de mensajes de smishing por día**, lo que refleja un auge de las campañas masivas de SMS fraudulentos.

- En España y América Latina, informes de ciberseguridad muestran que los intentos de **estafas por mensajes falsos (phishing SMS)** han aumentado entre un **44% y un 85%** en el último año, impulsados por la automatización y el uso de IA.



• A nivel global, **los ataques a móviles** han crecido alrededor de un **29% en la primera mitad de 2025**, con un fuerte peso de troyanos bancarios que aprovechan SMS y enlaces maliciosos para robar credenciales.

Estos números indican que, aunque el SMS Blaster es solo una pieza del ecosistema, aprovecha el conocimiento y las TTPs de los ataques de smishing combinándolos con dispositivos que simulan ser una antena de telefonía falsa para hacer llegar los SMS a los usuarios, saltándose así las restricciones que están poniendo los operadores para proteger a los usuarios de este tipo de ataques.

Conclusión

El SMS Blaster es un ejemplo extremo de cómo la tecnología se vuelve contra el usuario: algo, que bien usado, podría ser útil para alertas de emergencia o comunicaciones legítimas se convierte en un arma de **fraude masivo** aplicado en zonas urbanas densas. Como ya venimos advirtiendo en esta sección, muchos de los ataques combinan técnicas conocidas (smishing) con el uso de tecnologías inalámbricas que tienen una mayor efectividad al no disponer todos los usuarios de medidas de protección frente a estos ataques con protocolos inalámbricos.

Recibir SMS falsos sólo es una aplicación de lo que puede hacer esta tecnología, por eso nuestros equipos de seguridad deben ser conscientes de los riesgos que suponen algunas tecnologías inalámbricas, y por tanto buscar y aplicar los controles más adecuados para mejorar la seguridad. Muchas veces nos centramos en todo lo que tiene que ver con amenazas de internet conocidas, o al tráfico tcp/ip en redes dejando de lado la seguridad de los dispositivos frente a ataques con protocolos inalámbricos.

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**



Ciberseguridad a baja altitud

Ya lo venimos anunciando desde hace mucho tiempo en esta sección, durante décadas, el modelo de ciberseguridad empresarial se ha construido alrededor de un paradigma relativamente claro: proteger sistemas IT, redes corporativas y, más recientemente, infraestructuras cloud e IoT con protocolos conocidos como TCP/IP, dejando de lado muchos otros protocolos que pueden suponer una amenaza clara para nuestras infraestructuras.

Ese modelo que comentamos, funcionaba porque la superficie de ataque estaba razonablemente delimitada. Sabíamos dónde estaban los activos críticos, qué protocolos utilizaban y cómo segmentar las redes para defenderlos. Pero la tecnología avanza, y este escenario está cambiando con una rapidez asombrosa.

Es el caso del crecimiento de las operaciones UAV y plataformas aéreas autónomas, estas abren una superficie de ataque completamente nueva, donde los vectores tradicionales de ciberseguridad se combinan con vulnerabilidades propias del dominio de las ondas (RF) y de los sistemas de control de vuelo.

UNA INFRAESTRUCTURA DIGITAL EN EL AIRE

Cuando se habla de drones o UAV suele pensarse en aplicaciones relativamente simples: fotografía aérea, inspección industrial o logística puntual. Sin embargo, la visión que están desarrollando diferentes países es mucho más ambiciosa, incluye transporte logístico automatizado, vigilancia ambiental, inspección de infraestructuras, agricultura de precisión, movilidad aérea urbana y sistemas de respuesta en emergencias. Para soportar estas operaciones se está desarrollando una infraestructura tecnológica compleja que integra sensores, plataformas aéreas, redes de comunicaciones, sistemas de posicionamiento y plataformas de control que deben securizarse.



CONTINÚA EN
PRÓXIMA PÁGINA

Si un atacante compromete estas plataformas puede obtener acceso indirecto a toda la flota de drones. En este sentido, los sistemas de gestión de UAV se convierten en objetivos especialmente atractivos para campañas de intrusión.

Además, muchas operaciones dependen de integraciones con servicios externos: APIs de meteorología, sistemas de gestión logística, plataformas de análisis de datos o redes móviles. Cada una de estas integraciones introduce nuevos vectores potenciales de ataque en la cadena de suministro digital.

ATAQUES QUE NOS DEMUESTRAN LA NECESIDAD DE INVERTIR EN SEGURIDAD

Quizás estén pensando que estamos lejos de que este tipo de ataques puedan llevarse a cabo, pero nada más lejos de la realidad. Uno de los casos más conocidos ocurrió en 2011 con la captura de un UAV de reconocimiento de EEUU. Los atacantes consiguieron tomar el control con un ataque GPS spoofing que engañó al sistema de navegación del dron para hacerlo aterrizar en una ubicación falsa que el sistema interpretó como su base original.

Muchos de los ataques contra UAV se producen en la **capa de comunicaciones**, especialmente en el espectro radioeléctrico y en los sistemas de navegación GNSS. Segundo, los ataques no requieren necesariamente acceso al sistema interno del dron; en muchos casos basta con manipular el entorno de señales en el que opera.

Esto rompe con la lógica tradicional de la ciberseguridad empresarial, donde la mayoría de controles se diseñan para proteger software, redes IP y sistemas de autenticación

LA CIBERSEGURIDAD Y LOS ANÁLISIS DE RIESGOS DEBEN ADAPTARSE

Los drones operan en entornos dinámicos, dependen de comunicaciones inalámbricas y se mueven constantemente entre diferentes dominios de red. Un mismo dispositivo puede estar conectado a enlaces RF propietarios, redes celulares, sistemas satelitales y plataformas cloud en cuestión de minutos. Desde el punto de vista del modelo de riesgo, esto implica que el perímetro se vuelve completamente difuso.

Además, los vectores de ataque ya no se limitan a software vulnerable o credenciales comprometidas. Ahora debemos considerar ataques sobre GNSS, interferencias en espectro radioeléctrico, manipulación de sensores o compromisos en firmware de vuelo.

Muchos SOC actuales no están preparados para monitorizar este tipo de señales. Sus herramientas están diseñadas para analizar logs, tráfico IP o eventos de endpoints, no para detectar anomalías en enlaces RF o inconsistencias en telemetría aeronáutica. Y aunque no parezca relevante, debemos empezar a pensar en los SOC verticales especializados en tecnologías y

protocolos. En España ya hemos empezado con el SOC 5G gracias al ENS5G, pero esto sólo es el principio.

LA CIBERSEGURIDAD TAMBIÉN DEBE MIRAR HACIA EL CIELO

En punto en el que nos encontramos ahora mismo, y con las lecciones aprendidas de los conflictos bélicos actuales, no podemos dejar de mirar hacia arriba y considerar que algunas amenazas pueden venir desde el cielo.

Durante años, los **Security Operations Centers** han evolucionado para responder a una superficie de ataque que crecía principalmente en el dominio digital. Primero fueron las redes corporativas, después los endpoints, más tarde el cloud, y finalmente el IoT y los entornos OT. Cada una de esas fases obligó a los SOC a incorporar nuevas fuentes de telemetría, nuevas herramientas de análisis y nuevas capacidades de detección.

El uso de UAV para llevar a cabo ataques, hace que se tenga que considerar este nuevo dominio (el del aire) donde las plataformas aéreas autónomas y sus sistemas dependen de comunicaciones RF que no generan directamente logs en todos los casos, sino que debe atenderse a sus señales radio para conocer su comportamiento.

Esto plantea una evolución inevitable. El SOC del futuro no podrá limitarse a observar lo que ocurre dentro de una red corporativa, deberemos evolucionar hacia SOC's verticales especializados en comunicaciones RF y sus amenazas. Para hacerlo posible, los SOC deberán incorporar también nuevas capacidades tecnológicas. Herramientas basadas en **software defined radio (SDR)** permitirán capturar y analizar señales en diferentes bandas de frecuencia, identificar transmisiones sospechosas o detectar patrones de interferencia. Sensores de espectro desplegados en entornos críticos podrán alimentar plataformas de análisis con datos sobre actividad RF anómala. Antenas direccionales, sistemas de triangulación y plataformas de análisis de señal se convertirán en nuevas fuentes de telemetría para los analistas de seguridad.

El reto no es únicamente tecnológico. También es operativo. Los analistas deberán aprender a correlacionar eventos que hasta ahora pertenecían a dominios distintos: actividad de red, anomalías en enlaces RF, desviaciones en navegación GNSS o comportamientos inesperados en plataformas autónomas.

En otras palabras, la defensa de las infraestructuras digitales del futuro exigirá **SOC capaces de operar en entornos ciber-físicos**. Centros de operaciones que no sólo monitoricen servidores, endpoints o identidades, sino también sensores, drones, enlaces de radio y sistemas autónomos que operan fuera del perímetro tradicional.

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**



Inteligencia de señales en entornos hostiles

La inteligencia de señales ha evolucionado desde la interceptación clásica de comunicaciones de radio hasta convertirse en un ecosistema complejo donde convergen radiofrecuencia, análisis espectral avanzado, aprendizaje automático y correlación multi-dominio. En este contexto, las constelaciones de satélites en órbita baja (como Starlink) han introducido un nuevo vector que altera profundamente las reglas del juego.

Starlink, por si todavía no lo sabías, dispone de miles de satélites LEO, que no solo ofrece conectividad resiliente dotando de acceso a Internet en lugares donde no llega otro tipo de conectividad, sino que también generan una huella electromagnética característica que puede ser explotada por actores maliciosos con capacidades SIGINT avanzadas.

Cada terminal emite patrones de señal específicos, modulaciones características y comportamientos que, si bien están cifrados en su contenido, no ocultan completamente su existencia; las señales pueden ser detectadas, aunque no podamos descifrar el contenido de las comunicaciones. Basándonos en estas afirmaciones, un adversario no necesitaría descifrar el tráfico para detectar, localizar o incluso perfilar a los usuarios que hacen uso de starlink. Y es aquí donde, como ya venimos advirtiendo en nuestros artículos, las comunicaciones inalámbricas pueden ser un nuevo vector de ataque que, sin bien todavía no están ampliamente explotadas, pueden provocar serios problemas si no empezamos a considerarlas como vectores de ataque en nuestro modelo de amenazas.

Señales que generan patrones y permiten perfilar a los usuarios

Por otro lado, la proliferación de sensores pasivos y activos, junto con infraestructuras de monitorización distribuidas, permite a ciertos estados y, no solo a los estados, construir mapas dinámicos del espectro radioeléctrico. Hoy en día, existen muchísimos sistemas SDR (radios definidas por software) que están conectadas a Internet y que cubren amplísimas zonas del planeta.

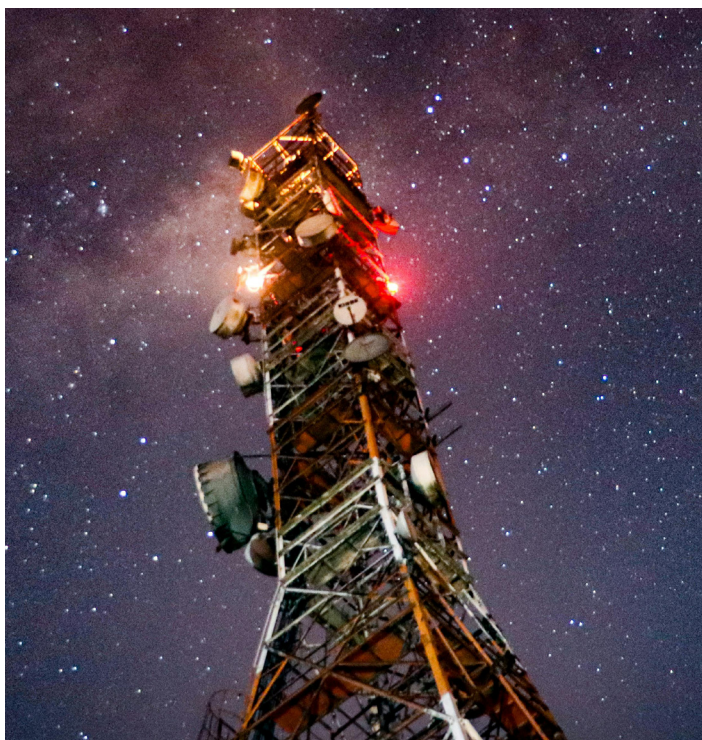
La detección no se basa en vulnerabilidades del protocolo en sí, sino en la explotación de propiedades físicas inherentes a la transmisión; la detección de las señales, la capacidad de ubicarlas e incluso de perturbarlas.

Así pues, la inteligencia de señales (SIGINT) aplicada a redes satelitales no se limita a la interceptación como podríamos pensar, sino que se extiende a la geolocalización precisa, el análisis de patrones de uso y la identificación de nodos activos en tiempo casi real. Este cambio de paradigma obliga a replantear la percepción de seguridad que muchos usuarios asocian con estas tecnologías.



CONTINÚA EN
PRÓXIMA PÁGINA





La detección de dispositivos Starlink no requiere necesariamente acceso a la red ni capacidades de intrusión activa. En su lugar, los sistemas SIGINT pueden operar de forma completamente pasiva, capturando emisiones en el espectro radioeléctrico y analizando sus características. Esto ofrece a los threat actors, la capacidad de realizar una observación sin ser delatados, usando técnicas pasivas que difícilmente pueden ser detectadas.

Las firmas electromagnéticas de Starlink se manifiestan en múltiples dimensiones: frecuencia, tiempo, potencia y modulación. Cada una de estas dimensiones puede ser explotada para identificar la presencia de un terminal. Por ejemplo, la modulación utilizada en los enlaces ascendentes presenta características específicas que, una vez catalogadas, permiten distinguir estas señales de otras transmisiones en las mismas bandas.

En consecuencia, el uso de Starlink en determinados entornos hostiles debe considerarse desde una perspectiva de exposición electromagnética y/o de aumento de la superficie de ataque. La invisibilidad percibida por el uso de sistemas inalámbricos no se corresponde con la realidad técnica, donde cada transmisión deja un rastro susceptible de ser explotado.

Estrategias de mitigación

Frente a estas amenazas, existen diversas estrategias que pueden reducir la exposición, aunque ninguna ofrece una protección absoluta. La primera línea de defensa consiste en minimizar la firma electromagnética mediante el uso controlado del terminal. Esto implica limitar la duración y frecuencia de las conexiones, así como evitar patrones predecibles.

Además, la ubicación del terminal juega un papel crucial. El uso en entornos urbanos densos puede dificultar la geolocalización debido a la reflexión y dispersión de señales.

Conclusiones

Tecnologías como Starlink evidencian que la innovación en protocolos, cifrado y arquitectura de red no elimina la exposición inherente al medio físico sobre el que operan. La propagación electromagnética sigue siendo un vector observable, medible y explotable, independientemente del nivel de sofisticación de las capas superiores.

Tradicionalmente, los modelos de amenazas han tendido a centrarse en vectores lógicos, vulnerabilidades software o debilidades en la gestión de identidades, relegando a un plano secundario los riesgos asociados a la capa física. Sin embargo, el contexto actual demuestra que esta aproximación resulta incompleta. La capacidad de detectar, geolocalizar y perfilar emisores a partir de su huella radioeléctrica introduce un conjunto de amenazas que, en muchos casos, ni siquiera se contemplan explícitamente en los procesos de análisis de riesgos.

Este vacío es especialmente relevante en el ámbito de las infraestructuras críticas, donde la adopción de tecnologías inalámbricas se ha acelerado por razones de flexibilidad, resiliencia y despliegue rápido. En estos entornos, la baja percepción del riesgo asociado a la emisión puede traducirse en exposiciones no controladas, difíciles de auditar y, en consecuencia, no mitigadas. La ausencia de este vector en el modelado de amenazas no implica su inexistencia, sino más bien una falta de visibilidad sobre su impacto real.

En este escenario, resulta imprescindible incorporar una visión más amplia y rigurosa del riesgo asociado a las comunicaciones inalámbricas. Esto implica no solo entender las propiedades técnicas de los sistemas utilizados, sino también integrar la dimensión electromagnética en los procesos de diseño, evaluación y operación.

Esto no va solo de Starlink. Starlink es el ejemplo visible, pero el problema es estructural y afecta a cualquier sistema inalámbrico. Cada enlace radio, cada uplink, cada handshake en RF introduce una superficie de exposición que no se suele cuantificar. No porque no exista, sino porque no se está midiendo. Y lo que no se mide, no se protege.

A partir de aquí, la conversación interesante no es si estas capacidades existen, porque existen, sino cómo de preparadas están nuestras organizaciones para convivir con ellas. Qué estamos incorporando realmente en nuestros modelos de riesgo, qué estamos ignorando y, sobre todo, por qué.

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**



La transformación silenciosa del SOC

Para comprender el estado actual de SOC (Security Operations Center), es necesario retroceder a sus orígenes. Aunque no existe un punto exacto de partida, su evolución está estrechamente ligada a los Network Operations Centers (NOC) de los años 90. De ellos hemos heredado no solo su estructura, sino también una forma de operar que, con el paso del tiempo, ha evidenciado ciertas limitaciones que, a día de hoy, condicionan su efectividad.

En la actualidad, las organizaciones se enfrentan a un escenario marcado por la sofisticación de los adversarios y una presión constante sobre los analistas. Aunque la misión del SOC permanece intacta, el modelo sobre el que se sustenta ha quedado desalineado con la realidad.

Hablar de un “SOC moderno” no implica referirse a un estándar cerrado o a una arquitectura única. Más bien apunta a una dirección: la necesidad de adaptar capacidades, procesos y estructuras a un entorno dinámico, donde la eficiencia operativa y la capacidad de respuesta marcan la diferencia.

EL AGOTAMIENTO DEL MODELO POR NIVELES

Durante años, los SOC han adoptado estructuras organizativas inspiradas en los servicedesk tradicionales, basadas en niveles jerárquicos (L1, L2, L3) y en un modelo de escalado progresivo. Este enfoque, empieza a mostrar signos claros de ineficiencia. El volumen de alertas y la complejidad de los incidentes han transformado este esquema en un cuello de botella.

En muchos casos, los analistas de primer nivel, asumen tareas críticas, filtrando grandes volúmenes de eventos y tomando decisiones con información incompleta. Esto deriva en análisis superficiales, fatiga operativa y un aumento del riesgo de incidentes no detectados.

Ante esta realidad, numerosas organizaciones están intentando, no siempre con éxito, migrar hacia operaciones de gestión de la ciberseguridad mucho más autónomas.

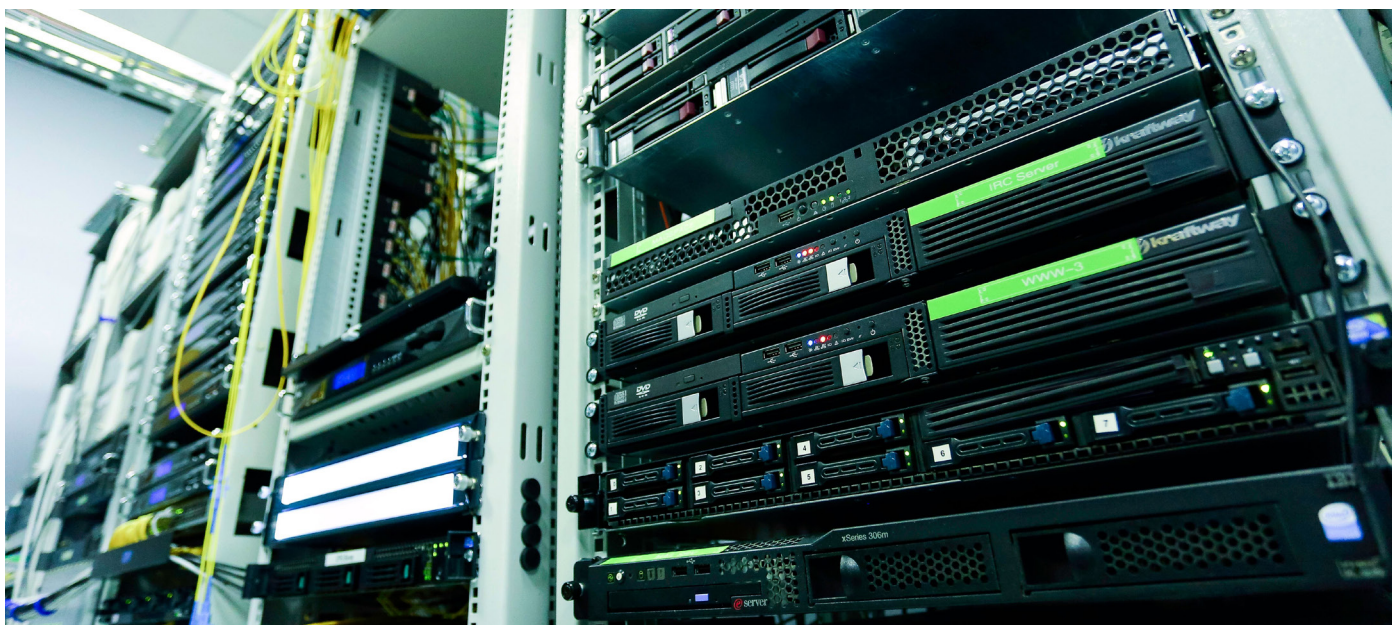
HACIA OPERACIONES DE SEGURIDAD MÁS AUTÓNOMAS

El concepto de operaciones de seguridad autónomas no debe interpretarse como una eliminación del factor humano. Por el contrario, implica un rediseño de los procesos para hacerlos más ágiles, adaptativos y eficientes, maximizando el valor del talento disponible.

Es aquí donde emerge el enfoque de Detection & Response Development Lifecycle (DR-DLC), que introduce principios propios de la ingeniería de software. Este modelo promueve la adopción de conceptos como _ detection as code (DaS), donde las reglas de detección se gestionan bajo criterios de control de versiones, integración continua, automatización y aseguramiento de la calidad.



CONTINÚA EN
PRÓXIMA PÁGINA



Este enfoque permite a los equipos desarrollar, validar y desplegar nuevas capacidades de detección de forma ágil y controlada, reduciendo errores y mejorando la eficiencia operativa. En última instancia, supone un paso hacia la profesionalización de la ingeniería de detección dentro del SOC.

MÁS ALLÁ DE LA TECNOLOGÍA

La transformación del SOC no es, en esencia, un problema tecnológico. Básicamente, nos centramos en incorporar nuevas herramientas, pero este no es el camino, antes conviene detenerse. Revisar cómo trabajamos. Definir procedimientos. Establecer protocolos claros. Estandarizar operaciones. Construir, en definitiva, una base sólida sobre la que poder evolucionar.

Es precisamente cuando esa base existe, cuando enfoques como *Detection as Code* o el *Detection & Response Development Lifecycle (DR-DLC)* aportan un valor diferencial.

Con la inteligencia artificial ocurre algo similar. Incorporar agentes, modelos de lenguaje o capacidades avanzadas de automatización no garantiza, por sí mismo, una mejora operativa. Sin gobierno, sin procesos bien definidos, sin criterios claros... el impacto es limitado.

Ahora bien, cuando esos elementos están en su sitio, el efecto es evidente. La tecnología empieza a trabajar a favor del SOC: acelera la detección, mejora la respuesta y permite optimizar indicadores clave como el MTTR o el MTTR.

La verdadera revolución, por tanto, no está en la herramienta. Está en la forma de trabajar.

Primero rediseñar el SOC. Después, adaptar la tecnología. Ese es el orden. Y también la diferencia entre evolucionar... o simplemente parecer que se evoluciona. # Referencias

CONCLUSIONES

La evolución de los SOC no está llegando a través de grandes anuncios ni de cambios disruptivos visibles para el negocio. Se está produciendo de forma gradual, impulsada por una realidad operativa que ya no puede ignorarse: el volumen de alertas sigue creciendo, la superficie de exposición es cada vez más amplia y la disponibilidad de analistas cualificados continúa siendo limitada.

Durante años, el modelo basado en niveles permitió estructurar los equipos, especializar funciones y escalar las operaciones de seguridad. Sin embargo, las condiciones actuales han puesto de manifiesto sus limitaciones.

Dedicar recursos altamente especializados a tareas repetitivas, depender de procesos manuales para el enriquecimiento de alertas o mantener cadenas de escalado excesivamente largas introduce ineficiencias que afectan tanto a la capacidad de detección como a la velocidad de respuesta.

Los SOC del futuro probablemente serán más pequeños en número, pero mucho más eficientes en capacidad. Menos orientados a procesar alertas y más enfocados en gestionar riesgos. Menos dependientes de estructuras rígidas por niveles y más apoyados en plataformas inteligentes capaces de actuar de forma autónoma dentro de límites previamente definidos.

La transformación silenciosa del SOC ya está en marcha. La cuestión no es si las organizaciones adoptarán este modelo, sino con qué rapidez serán capaces de adaptarse a un entorno donde la velocidad, la eficiencia y la automatización se han convertido en factores determinantes para la resiliencia de las operaciones de seguridad.



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

El extraño caso de las interferencias aleatorias al sistemas GNSS en Europa

Ya hemos hablado en multitud de ocasiones de los sistemas GNSS y de la dependencia tecnológica que existe hoy en día, en esta sección.

Hoy vamos a ver un caso realmente extraño, durante los últimos meses, numerosos operadores aéreos y organismos de monitorización han detectado un incremento significativo de incidentes de pérdida de señal sobre amplias zonas del norte y este de Europa. Lo que inicialmente parecía un problema puntual terminó revelando un fenómeno mucho más complejo, cuyo análisis ha requerido técnicas avanzadas de ingeniería inversa, procesamiento de señal y análisis orbital.

En los sistemas GNSS, cada satélite transmite un código pseudoaleatorio único que permite al receptor distinguir su señal del ruido de fondo. Mediante un proceso de correlación matemática, el receptor recupera una señal que, en condiciones normales, sería imposible de detectar directamente.

Sin embargo, esa misma arquitectura presenta una debilidad evidente: basta con introducir suficiente energía dentro de la banda de frecuencia utilizada

por el sistema para impedir que el receptor mantenga la sincronización (es como gritar mucho para dejar sordo al receptor). Es el conocido ataque de *jamming*. A diferencia del *spoofing*, donde se generan señales falsas para engañar al receptor, el objetivo del *jamming* consiste simplemente en elevar el nivel de ruido hasta hacer imposible la recepción de la señal legítima. Lo que ha llamado especialmente la atención de los investigadores europeos es que la distribución geográfica de estas interferencias no encaja con el comportamiento habitual de un emisor terrestre.

Entre las investigaciones más relevantes destacan los trabajos desarrollados por la Universidad de Texas en Austin, cuyos investigadores compararon los instantes exactos en los que se producían las interferencias con las efemérides de numerosos satélites. Los resultados mostraron una coincidencia temporal repetitiva con el paso de determinados satélites en órbita baja, lo que abrió una nueva línea de investigación sobre posibles fuentes espaciales de interferencia.

Uno de los satélites que aparece

citado con mayor frecuencia en estos análisis es **Cosmos 2546**, una plataforma militar rusa cuya misión oficial no contempla operaciones de interferencia del GNSS. Algunos estudios sugieren que determinadas emisiones registradas podrían ser compatibles con transmisiones procedentes de este satélite, aunque hasta la fecha no existe una confirmación pública e independiente que permita atribuir de forma inequívoca las perturbaciones observadas.

Desde un punto de vista técnico, un satélite equipado con transmisores suficientemente potentes podría concentrar energía sobre regiones concretas de la superficie terrestre mediante haces dirigidos electrónicamente. Si dichas emisiones coincidieran con las frecuencias empleadas por GPS, Galileo o GLONASS, incluso pequeñas cantidades de potencia adicional serían suficientes para degradar la recepción debido a la extrema debilidad de las señales legítimas.



CONTINÚA EN
PRÓXIMA PÁGINA



Precisamente esa posibilidad ha reabierto el debate sobre la vulnerabilidad de estos sistemas GNSS de lo que tantas veces hemos hablado aquí en esta sección. Una parte de los expertos considera que determinadas interferencias podrían responder a operaciones deliberadas de guerra electrónica. Otros plantean una explicación menos directa: emisiones asociadas a enlaces militares que, aun sin tener como objetivo interferir el GNSS, terminan afectando inevitablemente a los receptores civiles por operar en bandas muy próximas.

Sin entrar en valorar quien es autor, lo que si que está muy claro es que las consecuencias van mucho más allá de la navegación aérea. Los receptores GNSS proporcionan la referencia temporal utilizada por redes eléctricas, infraestructuras de telecomunicaciones, mercados financieros y numerosos sistemas industriales. La pérdida de sincronización puede propagarse rápidamente a otros servicios esenciales, lo que convierte al GNSS en una auténtica infraestructura crítica.

Al mismo tiempo y, debido al incremento de las interrupciones de los sistemas GNSS, vuelve a cobrar protagonismo eLoran, una evolución moderna del histórico sistema LORAN que, al operar en bajas frecuencias y con potencias muy superiores a las del GNSS, ofrece una alternativa terrestre mucho más resistente frente a interferencias electromagnéticas.

A esta tecnología comienzan a sumarse soluciones emergentes basadas en navegación inercial de

muy alta precisión, mapas magnéticos y sensores cuánticos capaces de mantener el posicionamiento incluso durante largos periodos sin cobertura satelital.

Más allá del origen concreto de los incidentes registrados en Europa, el episodio deja una enseñanza evidente: la confianza absoluta en una única tecnología de posicionamiento ya no resulta compatible con el escenario geopolítico actual. La resiliencia del posicionamiento, la navegación y la sincronización pasa por combinar múltiples tecnologías capaces de seguir funcionando cuando el espacio radioeléctrico deja de ser un entorno fiable. En un contexto marcado por la creciente militarización del dominio electromagnético y espacial, esa redundancia deja de ser una mejora tecnológica para convertirse en un requisito esencial de seguridad.

Y con este artículo, llegamos también al momento de la despedida. Han sido más de 37 artículos los que hemos compartido en donde se ha querido concienciar al lector de la importancia de la seguridad de las comunicaciones radio. Agradecer a la revista que haya querido confiar en mi persona para hablar de este tema.

Muchas gracias a los lectores por seguir tan de cerca la sección y esperemos que los artículos hayan sido de su agrado. Un cordial saludo y, nos escuchamos en las ondas.



**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



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

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...



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.

REDONDA "TECNOLOGÍA & SENTIDO COMÚN"

Javier Peris

11:45 a 12:30



CONTINÚA EN
PRÓXIMA PÁGINA



REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>



Suscríbete gratis

REVISTA
**Tecnología &
Sentido Común**

**2022
PREMIOS
SAPIENS**

Llanos C.
Alejandro Blasco
Juan J. Urbión
Sección
Proyectos
el Futuro
Por Procesos
Miguel Ángel Calvo
Cr.

MESA RED
Modera Javier P.

JUAN J. URBÍON
Sección
Proyectos
el Futuro

JUAN J. URBÍON
Sección
Proyectos
el Futuro

JUAN J. URBÍON
Sección
Proyectos
el Futuro

JUAN J. URBÍON
Sección
Proyectos
el Futuro

JUAN J. URBÍON
Sección
Proyectos
el Futuro

JUAN J. URBÍON
Sección
Proyectos
el Futuro

JUAN J. URBÍON
Sección
Proyectos
el Futuro

JUAN J. URBÍON
Sección
Proyectos
el Futuro

JUAN J. URBÍON
Sección
Proyectos
el Futuro

JUAN J. URBÍON
Sección
Proyectos
el Futuro

JUAN J. URBÍON
Sección
Proyectos
el Futuro

JUAN J. URBÍON
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: Organizaciones 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

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
amsés Gallego

olo
tic

La Nueva
Administración
VÍCTOR ALMONACID

Por Procesos



#TYSC / PÁG. 66



PREMIOS

Tecnología &
Sentido Común
2026

13:45 a 14:00

PREMIO RE
S
2026



REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

gratis

& Común



“Stakeholders”, la Re Profesionales ierno,

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



#TYSO / PÁG. 68

Stakeholders

.news

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



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: 20 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

