

“Radio Security”

ESPECIAL

DE **Tecnología & Sentido Común**



ESPECIAL

AGOSTO
2025

Seguridad en
los sistemas
satelitales

08

La guerra invisible
contra los
sistemas GNSS

12

Defendiendo las
comunicaciones de
los drones con IA

16

El espectro
radioeléctrico,
una superficie
de ataque
vulnerable

20

La Guerra Invisible:
“El Rol del WiFi en
las Estrategias
Geopolíticas Mundiales”

24

Security
Operations
Center

28

La Guerra
Electrónica y
el control del
espectro

32

Amenazas no
convencionales
en el mundo del
IoT

36

Desentrañando la
Ciberseguridad en
Redes Tácticas 6G:
Amenazas, Arquitectura
e Inteligencia Artificial

40

Así se protege una
infraestructura
5G frente a
ciberataques

44

Rediseñando los
SOCs para una
detección más
efectiva

48

ESPECIAL “Radio Security”

DE Tecnología & Sentido Común



EQUIPO TYSC

Javier Peris - El Gubernauta
Manuel Serrat - Futuro y Seguridad
Nacho Alamillo - Tecnoregulación en Prospectiva
Juan Carlos Muria - Diario de una Tortuga Ninja
Marlon Molina - Es Tendencia
Ricard Martínez - Ojo Al Dato
Marcos Navarro - Ai Futuro
Víctor Almonacid - La Nueva Administración
Alex Aliaga - Radio Security
Marta Martín - 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

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

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



ESPECIAL
AGOSTO
2025



índice

DE CONTENIDOS

<https://tecnologiaysentidocomun.com>



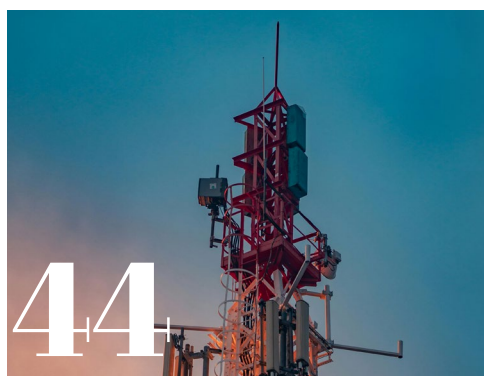
**Defendiendo las
comunicaciones
de los drones con IA**



**La Guerra Invisible:
“El Rol del WiFi en las Estrategias
Geopolíticas Mundiales”**



**Amenazas no
convencionales en el
mundo del IoT**



**Así se protege
una infraestructura 5G
frente a ciberataques**

Copyright

02

Índice de Contenidos

04

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

por JAVIER PERIS

07

**Seguridad en
los sistemas
satelitales**

08

**La guerra invisible
contra los
sistemas GNSS**

12

**Defendiendo las
comunicaciones
de los drones con IA**

16

**El espectro
radioeléctrico,
una superficie de
ataque vulnerable**

20

**La Guerra Invisible:
“El Rol del WiFi en las
Estrategias Geopolíticas
Mundiales”**

24

**Security
Operations
Center**

28

**La Guerra
Electrónica
y el control
del espectro**

32

**Amenazas no
convencionales
en el mundo
del IoT**

36

**Desentrañando la
Ciberseguridad en Redes
Tácticas 6G: Amenazas,
Arquitectura e
Inteligencia Artificial**

40

**Así se protege una
infraestructura 5G
frente a ciberataques**

44

**Rediseñando los
SOCs para una
detección más
efectiva**

48

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

52

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

68

WIS

#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.



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



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

Javier Peris

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

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

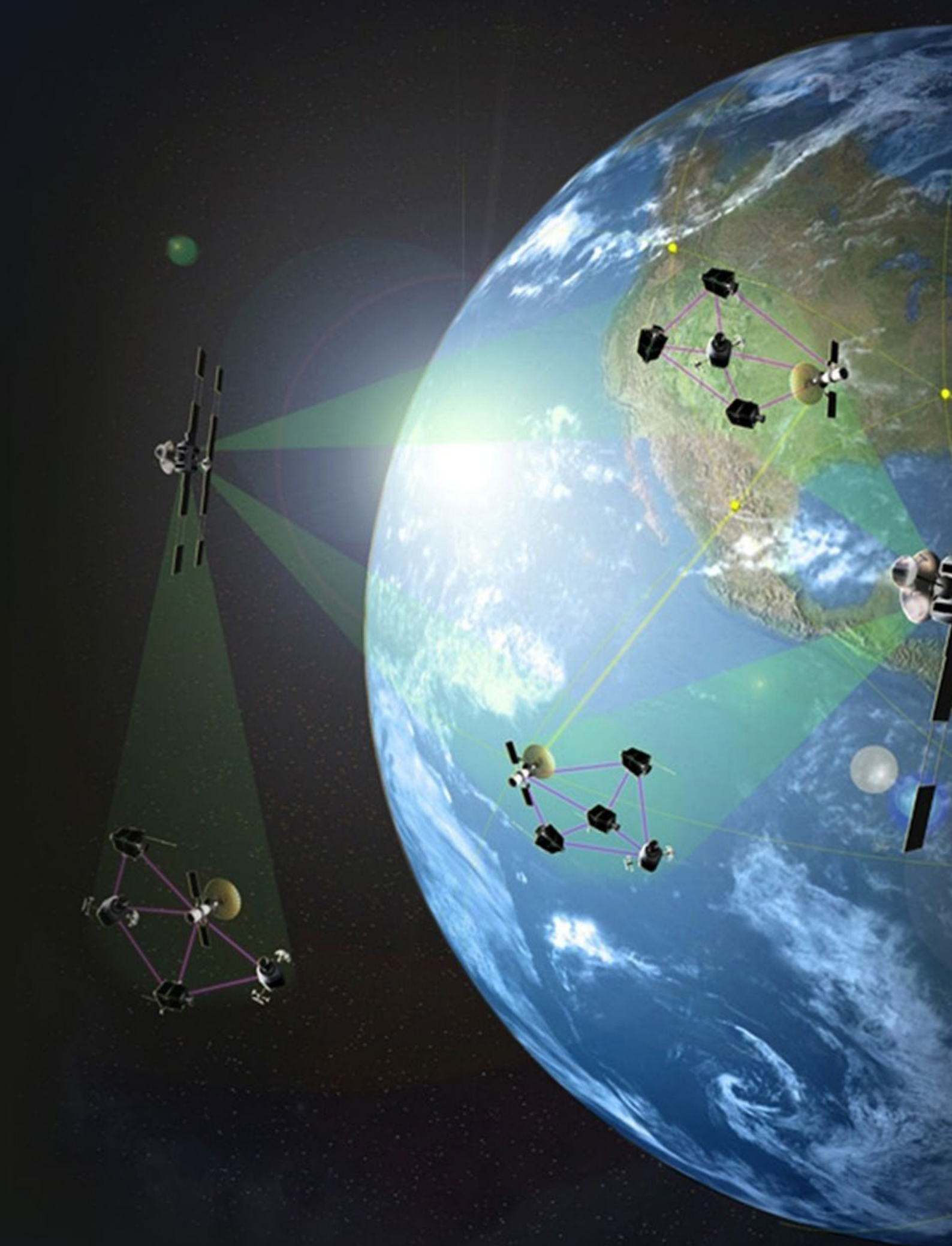
Te aseguro que no es otro método de productividad; es un manifiesto para una verdadera revolución personal.

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

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

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

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



Seguridad en los sistemas satelitales

Introducción

En la actualidad, el sector aeroespacial se ha transformado y se ha convertido en una infraestructura crítica, dejando de ser dominio exclusivo de las autoridades gubernamentales nacionales. No cabe duda de que, existe una dependencia de estos sistemas espaciales para funciones críticas como navegación (PnT), control de operaciones y recopilación de inteligencia. Sin embargo, esta dependencia también ha aumentado la vulnerabilidad de estos sistemas frente a ciberataques.

A lo largo de este artículo, haremos una introducción en la gestión de la seguridad de las comunicaciones satelitales, veremos algunas de las posibles amenazas, y trataremos de dibujar qué controles se deben aplicar para mejorar la seguridad y proteger estas infraestructuras críticas.

Uno de los ataques más relevantes

El ataque a Viasat, empresa norteamericana de comunicaciones por satélite, es uno de los mejores ejemplos de la importancia de proteger este tipo de infraestructuras, y de su importancia tanto en el ámbito civil como militar.

El 24 de febrero de 2022, una hora antes de la invasión militar, se interrumpió el servicio que provee Viasat a través de su sistema KA-SAT. En este suceso, el ataque tuvo repercusión no sólo a miles de usuarios de internet, sino también a diversos parques eólicos conectados que perdieron la capacidad de ser monitorizados, se estima que más de 5800 turbinas perdieron el acceso a internet.



CONTINÚA EN
PRÓXIMA PÁGINA



Muchos de los detalles técnicos acerca de este ataque, siguen siendo un misterio a día de hoy. Pero, aún así, este ataque refuerza, más si cabe, el discurso de la importancia de proteger las infraestructuras satelitales. Pero esta no es la única noticia sobre ataques a sistemas satelitales. En el conflicto entre Rusia y Ucrania hemos podido ver algunos otros ataques que, quizás no han ocupado portadas, pero si han tenido un impacto importante sobre la seguridad de los sistemas satélite.

Ha llegado el momento de tomarse en serio la seguridad satelital

El Pentágono de los Estados Unidos comenzó hace tiempo con un programa de bug bounty para que expertos intenten tomar control de un satélite estadounidense en órbita. Esta audaz iniciativa no solo pone de manifiesto la importancia de la ciberseguridad en el espacio, sino también abre un espacio de reflexión sobre cómo los gobiernos están abordando sus desafíos de seguridad digital.

Hack-A-Sat ha ido ganando importancia en cada edición. A medida que más profesionales participan en este evento más avanza la ciberseguridad de estos sistemas, pero algo destacable es que a mayor participación mayor ha sido la velocidad con la que se ha conseguido comprometer estos sistemas. De hecho, en la 4ª edición el equipo ganador se hizo con el control de un satélite militar estadounidense en tan sólo unas horas.

El incidente de VIASAT sigue siendo un marcador clave cuando se habla de seguridad satelital. De hecho, el NIST ya recoge la necesidad de tener en cuenta la seguridad de los sistemas satelitales. Para ello publicó el NIST IR 8441 un framework para redes satelitales que contempla "terminales, antenas, cargas útiles y otros sistemas que puedan componer un sistema satelital"

Pero, aunque el caso de VIASAT es el más conocido, no es el único que se ha podido observar en los últimos años, otros operadores como SPEEDCAST sufrió también ataques contra su infraestructura lo cual nos indica que para los cibercriminales el segmento satélite sigue siendo apetitoso y está entre sus objetivos.

Riesgos de seguridad en las comunicaciones satélite

Como hemos ido viendo en el artículo, proteger estos sistemas contra amenazas ciber es crucial en este tipo de infraestructuras. Algunos de los riesgos a los que se enfrentan, entre otros, son:

- Intercepción de las comunicaciones:** un cifrado débil, o la ausencia de este, puede hacer que las señales sean susceptibles de interceptación.
- Vulnerabilidades en los sistemas de C&C (Comando y Control):** ya se han dado casos, en los que sistemas de C&C han sido vulnerados y con ello se ha tomado el control de un sistema satélite.
- Riesgos en la cadena de suministro:** ya hemos tenido ataques de este estilo, donde se introducen vulnerabilidades en la cadena de suministro

Conclusiones

La ciberseguridad en el espacio se extiende mucho más allá del ámbito técnico y afecta las relaciones, la cooperación y la competencia internacionales. Es un dominio complejo de proteger donde existen muchos actores con intereses en dominar ese ámbito.

Un incidente cibernético importante podría costar miles de millones en daños, alterar los servicios globales y requerir amplios recursos para mitigación y recuperación. Definir nuevos estándares y controles de seguridad se hace imperativo para salvaguardar el futuro de la explotación espacial y la integridad de la actual infraestructura espacial existente.

P4MGO![®] Essentials

Portfolio, Programme,
Project & Product
Management &
Governance



La guerra invisible contra los sistemas GNSS

Hoy en día, los sistemas de posicionamiento global por satélite (**GNSS**) constituyen una infraestructura clave que proporciona información precisa y fiable sobre la posición y el tiempo. Son parte fundamental de nuestras vidas cotidianas; los utilizamos en vehículos, aplicaciones de smartphones, y en operaciones críticas como el tráfico aéreo, transacciones bancarias y la sincronización de redes eléctricas. Sin embargo, la seguridad de estos sistemas se enfrenta a amenazas cada vez mayores debido a la creciente dependencia global de esta tecnología.

El sistema de posicionamiento más conocido es el **GPS** (Global Positioning System), desarrollado por Estados Unidos, pero existen otros como el europeo **Galileo**, el ruso **GLONASS** y el chino **BeiDou**. Todos estos sistemas son vulnerables a ciberataques y manipulación, lo que pone en riesgo no solo su operación, sino también los sectores que dependen de ellos.

GEOPOLÍTICA DEL POSICIONAMIENTO Y SUS RIESGOS

La seguridad de los sistemas GNSS ha cobrado relevancia como una de las amenazas más serias en los últimos años, sobre todo por su uso intensivo en operaciones civiles y militares. Se estima que más del 90% de las infraestructuras críticas dependen de la precisión y sincronización que ofrecen estos sistemas. Sin embargo, esta dependencia también

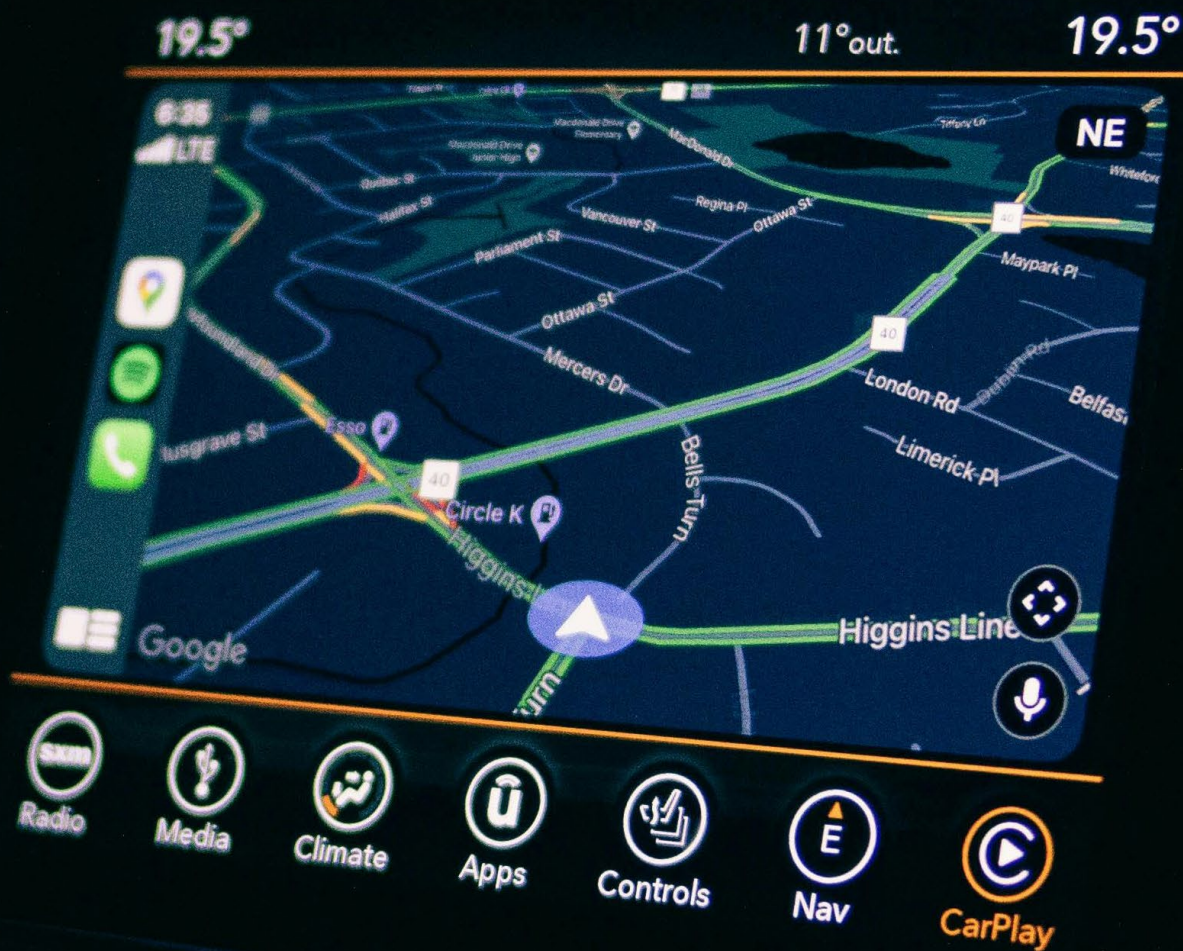
los convierte en objetivos atractivos para actores maliciosos, desde estados-nación hasta grupos hacktivistas y delincuentes comunes.

Uno de los principales riesgos es el **spoofing**, que consiste en enviar señales GPS falsas para que los receptores de un objetivo perciban una ubicación equivocada. Este tipo de ataque puede tener graves consecuencias: desde desorientar aviones y barcos, hasta alterar rutas de transporte y afectar operaciones militares. Por ejemplo, antes de la invasión rusa a Ucrania en 2021, se registraron casos de spoofing que afectaron a buques de guerra de la OTAN en el puerto de Odesa, Ucrania, lo que interrumpió sus operaciones en la región.

Otra amenaza importante es el **jamming**, que implica bloquear las señales de GPS mediante la emisión de señales de radio potentes en la misma frecuencia. Los dispositivos utilizados para este fin son relativamente baratos y fáciles de conseguir, lo que amplía su potencial de uso tanto por actores estatales como no estatales. En el conflicto en Ucrania, se ha observado que las fuerzas rusas emplean jamming para deshabilitar los sistemas de navegación de aeronaves y vehículos, lo que ha provocado interrupciones en toda Europa.



CONTINÚA EN
PRÓXIMA PÁGINA



Estos ataques no solo afectan operaciones militares o logísticas; su impacto puede extenderse a la economía y a infraestructuras críticas como la red eléctrica o los sistemas de telecomunicaciones. La capacidad de interrumpir estas redes es motivo de gran preocupación, especialmente porque, a medida que avanzamos hacia una mayor automatización, el riesgo de sufrir ciberataques aumenta considerablemente.

HACKTIVISMO Y ATAQUES A INFRAESTRUCTURAS CRÍTICAS

En los últimos años, grupos hacktivistas han incrementado sus ataques contra sistemas GNSS. Un ejemplo es **GhostSec**, un colectivo que afirmó haber comprometido equipos GPS utilizados en instalaciones industriales críticas. Estos ataques pueden generar consecuencias catastróficas si se ejecutan con éxito. Los GNSS no solo proporcionan posicionamiento; también sincronizan redes eléctricas y soportan transacciones bancarias, entre otros servicios vitales.

El problema se agrava debido a la cantidad de sistemas GNSS conectados a internet sin medidas de seguridad adecuadas. Algunos estudios han encontrado que muchas de estas infraestructuras exponen públicamente sus interfaces de control, lo que las hace vulnerables a ataques remotos. Incluso, se han identificado módems satelitales en sectores como la energía, telecomunicaciones y transporte que no han cambiado las credenciales predeterminadas, lo que facilita la entrada de actores malintencionados.

Un ataque reciente, denominado **Operación Cataclysm**, dirigido por el grupo **One Fist**, mostró cómo los hacktivistas pueden desactivar módems satelitales utilizados en sectores clave como la aviación y el transporte marítimo. Durante esta operación, los atacantes eliminaron configuraciones críticas de los módems, causando disrupciones en la conectividad satelital. Este tipo de ataques no solo comprometen la integridad de los datos, sino que también pueden causar interrupciones en el suministro de servicios esenciales.

Por otro lado, los ciberataques más sofisticados, como el ransomware, también están afectando al sector espacial. Empresas que proveen servicios y componentes para satélites, como **Viasat**, han sido objeto de ataques que han interrumpido operaciones globales. En 2022, un ataque al sistema KA-SAT de Viasat afectó a 5800 turbinas eólicas en Alemania, lo que demuestra el impacto devastador que pueden tener los ataques a sistemas GNSS y satelitales.

ESTRATEGIAS CLAVE PARA PROTEGER LOS SISTEMAS GNSS DE CIBERATAQUES

A la luz de estas amenazas, diversas agencias de seguridad, como el **Departamento de Seguridad Nacional** de EE. UU. y la **CISA** (Agencia de Seguridad de Infraestructura y Ciberseguridad), han emitido directrices para mitigar los riesgos. Entre las recomendaciones se incluyen medidas para detectar y contrarrestar ataques de spoofing y jamming, además de la implementación de sistemas de **PNT resiliente** (Posicionamiento, Navegación y Temporización). Estos sistemas proporcionan una capa adicional de protección al complementar el GPS con tecnologías terrestres o alternativas satelitales, lo que ayuda a mantener la precisión y disponibilidad de los servicios, incluso en caso de interferencias.



En la **Unión Europea**, se han lanzado iniciativas para fortalecer la seguridad de **Galileo**, su sistema de navegación por satélite. La Agencia Espacial Europea trabaja en mejorar las capacidades de detección de interferencias y el desarrollo de nuevas técnicas criptográficas para proteger las comunicaciones entre los satélites y las estaciones terrestres.

CONCLUSIÓN

A medida que los sistemas GNSS se integran más en la vida moderna y en nuestras rutinas, aumenta la amenaza y el riesgo de sufrir ciberataques en estos activos críticos. Los satélites, sus estaciones terrestres, los enlaces de comunicación, el software que se ejecuta en todos sus sistemas pueden ser vulnerables a ciberataques; no por estar en el espacio están exentos de sufrir un ciberataque. Las posibles consecuencias si un ataque de estas características se materializase serían significativas y potencialmente peligrosas, que no sólo afectarían al activo en sí, sino que se verían afectados gran cantidad de sistemas y sectores que dependen de estos activos, así como de la ciudadanía que hacen uso de los sistemas GNSS.

Defenderse de los ciberataques en el espacio es un desafío complejo que requiere cooperación internacional, en primer lugar es importante conocer la gravedad del riesgo que supondrían un ataque de estas dimensiones. Y, aunque ya existen, muchas iniciativas es complejo atajar de raíz los problemas existentes. Mientras tanto, es importante divulgar y conocer cuáles son los riesgos para que, en aquellas infraestructuras o sistemas informáticos donde se puedan aplicar controles de seguridad y medidas adicionales a las ya existentes, se puedan aplicar de inmediato.

¿Demasiada Iniciativas?

¿Alineamiento Estratégico Cuestionable?

¿Dificultad para Priorizar?

¿Vision basada en Silos o Islas?

¿Falta de foco estratégico en el valor a largo plazo?



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



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

Defendiendo las comunicaciones de los drones con IA

UAVs y el aumento de las amenazas de ciberseguridad

Los Vehículos Aéreos No Tripulados (UAVs), comúnmente conocidos como drones, se han convertido en una tecnología transformadora, revolucionando industrias como la entrega de paquetes y la asistencia en desastres. Sin embargo, la proliferación de drones también ha abierto la puerta a vulnerabilidades de ciberseguridad.

A medida que los drones ganan protagonismo en los dominios civiles y militares, los datos que transportan y transmiten se han convertido en un objetivo valioso para los ciberdelincuentes. Desde la captura de información de vigilancia sensible hasta la manipulación de trayectorias de vuelo, los UAVs son ahora un foco importante en el campo de la ciberseguridad.

Un aspecto crítico que hace vulnerables a los drones es su dependencia de protocolos de comunicación inalámbrica como el sistema de Identificación Remota (RID). RID es un marco regulatorio diseñado para mejorar la seguridad del espacio aéreo, exigiendo que los drones transmitan datos de telemetría, como la ubicación y la información del operador. Sin embargo, tal como se destaca en algunas investigaciones, estos sistemas tienen varias vulnerabilidades que exponen a los drones a ataques de suplantación de identidad e inyección de datos.

ENFOQUES TRADICIONALES EN LA CIBERSEGURIDAD DE UAVS

En los primeros días de despliegue de drones, los métodos convencionales de ciberseguridad se basaban en gran medida en protocolos de seguridad estáticos. Sistemas como cortafuegos y sistemas de detección de intrusiones estáticos (IDS) se utilizaban para monitorear patrones de ataques conocidos. Sin embargo, estos métodos no podían seguir el ritmo de la naturaleza dinámica de las redes de drones, especialmente al considerar la complejidad y rápida movilidad de estos sistemas.

El uso de la **Identificación Remota de Drones (RID)** se introdujo para contrarrestar este problema, permitiendo a los reguladores y autoridades rastrear drones en tiempo real sabiendo en todo momento los datos del operador del mismo.



CONTINÚA EN
PRÓXIMA PÁGINA





No obstante, este protocolo carece de medidas de seguridad básicas como el cifrado y la integridad de datos, lo que lo hace susceptible a una variedad de ataques que podrían tener graves consecuencias para operaciones tanto militares como civiles .

EL PODER DEL APRENDIZAJE AUTOMÁTICO EN LOS SISTEMAS DE DETECCIÓN DE INTRUSIONES

En los últimos años, la integración del **aprendizaje automático (ML)** en los sistemas de seguridad ha marcado un cambio de paradigma en la ciberseguridad de drones. A diferencia de los sistemas IDS tradicionales que dependen de firmas predefinidas de ataques conocidos, los sistemas IDS basados en ML pueden detectar amenazas nuevas identificando desviaciones de patrones de comportamiento normales. Esta adaptabilidad es crucial, especialmente para los drones que operan en entornos cambiantes.

Los algoritmos de aprendizaje automático pueden entrenarse para monitorear grandes cantidades de datos de tráfico de red, aprendiendo a diferenciar entre patrones normales y anómalos.

Al aprovechar grandes conjuntos de datos, los sistemas basados en ML pueden detectar ciberataques sofisticados que los métodos convencionales podrían pasar por alto. En el contexto de los drones, el uso de un sistema de estas características permite mejorar la detección de accesos no autorizados, suplantación de señales de control e incluso vulnerabilidades en el protocolo RemoteID .

VULNERABILIDADES EN LOS PROTOCOLOS DE IDENTIFICACIÓN REMOTA

Los estándares del protocolo RemoteID requieren que los drones transmitan periódicamente sus datos de telemetría. Sin embargo, las implementaciones actuales de RID no logran asegurar estos datos, dejándolos expuestos a ataques de inyección y reproducción. Por ejemplo, un atacante puede inyectar datos RID falsos para simular la presencia de un dron en un área restringida, provocando falsas alarmas y potencialmente paralizando las operaciones del espacio aéreo.

La importancia de asegurar los sistemas RID se hizo evidente en el infame **incidente del aeropuerto de Gatwick** en 2018, donde drones volando cerca del aeropuerto obligaron a desviar más de 1,000 vuelos. Aunque los detalles del ataque no están claros, resaltó la necesidad de sistemas de identificación y rastreo de drones robustos y resistentes a la manipulación. Las tecnologías RID actuales no habrían podido distinguir entre drones reales y falsificados, haciendo que escenarios como este sean un campo fértil para los atacantes.

PRÓXIMOS PASOS EN LA SEGURIDAD DE UAV Y APLICACIONES DE ML

A medida que los drones continúan evolucionando, también lo harán los métodos utilizados para asegurar su operación. Un área emergente de interés es el uso del **aprendizaje por refuerzo** para optimizar las operaciones de los drones en respuesta a posibles amenazas cibernéticas. Al simular diferentes escenarios de ataque, los drones pueden aprender a reaccionar de manera autónoma, mejorando tanto su seguridad como su eficiencia operativa.

Enfoques colaborativos de seguridad Los avances futuros probablemente implicarán la colaboración entre fabricantes de drones, expertos en ciberseguridad y organismos reguladores. Al trabajar juntos, estas partes interesadas pueden crear ecosistemas de drones más resilientes, particularmente mediante la mejora continua de estándares como RID y el desarrollo de métodos de cifrado más sólidos.

Además, la investigación sobre protocolos de comunicación seguros, como los marcos de **radio definida por software (SDR)**, jugará un papel crucial en la mitigación de amenazas cibernéticas .

Una vez más, debemos contemplar la seguridad de las comunicaciones inalámbricas como un vector de ataque a todos nuestros sistemas. Tal y como venimos abordando en la revista, muchas veces no se tienen en cuenta y pueden suponer un grave problema de seguridad.

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



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



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

El espectro radioeléctrico, una superficie de ataque vulnerable

Ante un mundo hiperconectado, las organizaciones incorporan, cada vez más, sistemas de comunicaciones inalámbricos para facilitar la conectividad y movilidad de sus empleados. Sin embargo, con estos beneficios también surgen riesgos importantes de seguridad.

El espectro radioeléctrico es una superficie de ataque vulnerable, poco conocida, difícil de controlar y susceptible a una gran variedad de ataques sofisticados a los que no estamos acostumbrados. En un contexto donde una brecha en las comunicaciones inalámbricas puede comprometer datos y sistemas, proteger estos entornos se vuelve esencial, especialmente en sectores críticos y áreas de alta sensibilidad.

Amenazas a la seguridad: dispositivos no autorizados y exposición en el espectro inalámbrico

En entornos corporativos, los dispositivos no autorizados representan una amenaza latente y creciente para la seguridad de las redes. Con el avance del Internet de las Cosas (IoT) y el uso intensivo de tecnologías como Bluetooth, Zigbee

y dispositivos que hacen uso de las comunicaciones móviles para comunicarse, se ha ampliado de manera significativa la superficie de ataque.

Cualquier equipo que posea interfaces de comunicación inalámbrica pueden introducir un punto de acceso potencial para ciberataques. Y, aunque estamos muy acostumbrados a la protección de redes IP, no lo estamos tanto para proteger nuestro entorno radioeléctrico en una organización y, como llevamos mencionando en esta sección desde hace tiempo, los sistemas inalámbricos suponen una verdadera amenaza para nuestros sistemas.

Para enfrentar estos riesgos, es imprescindible la implementación de sistemas de control de acceso a la red que permitan la identificación y monitorización en tiempo real de todos los dispositivos que intentan acceder a la infraestructura tanto en la parte cableada como en las comunicaciones inalámbricas. Para esta segunda, es importante el despliegue de sistemas de monitorización del espectro que ayuden



a detectar cualquier señal inusual en áreas sensibles, facilitando una respuesta rápida y efectiva en caso de amenaza.

Bluetooth y las Vulnerabilidades de Suplantación de Identidad

El protocolo Bluetooth, omnipresente en dispositivos móviles e IoT, es una tecnología esencial en los entornos empresariales, pero su diseño presenta vulnerabilidades que pueden comprometer la seguridad de la red. Un ejemplo de ello es el ataque de suplantación de identidad conocido como **BIAS** (Bluetooth Impersonation AttackS), que aprovecha fallos en el mecanismo de conexión segura heredado y permite que un atacante se haga pasar por un dispositivo autorizado. Este tipo de ataque degrada la seguridad de la conexión sin que el usuario sea consciente de ello.

Las organizaciones pueden reducir estos riesgos al reforzar las conexiones Bluetooth mediante autenticación avanzada y limitando el acceso no autorizado mediante políticas restrictivas. Implementar la monitorización continua de las conexiones Bluetooth, junto con controles de autenticación más robustos, es crucial para prevenir intentos de suplantación y garantizar la integridad de la comunicación.

La Amenaza Oculta de la Suplantación en Redes Móviles

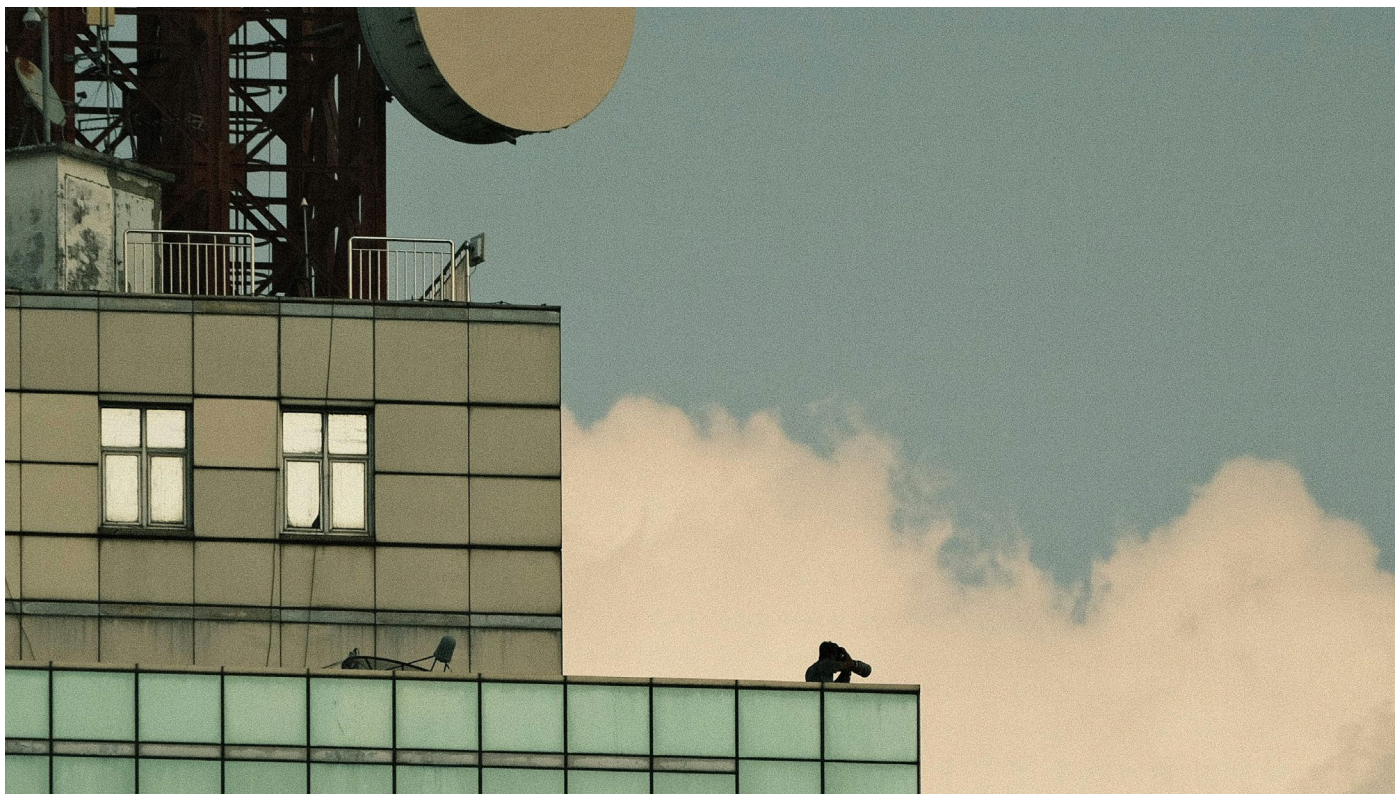
Entre las amenazas más sofisticadas en el ámbito de las comunicaciones inalámbricas están las estaciones falsas de móviles o "Rogue Cell Towers", que engañan a los teléfonos móviles haciéndose pasar por estaciones base legítimas. Estas torres pueden capturar información sensible de los dispositivos, como el **IMSI**, y rastrear su ubicación o interceptar las comunicaciones. Este tipo de ataque explota vulnerabilidades en redes 2G, que carecen de autenticación de red, y puede degradar las conexiones forzando a los dispositivos a conectarse a redes menos seguras.

La detección de estos ataques es compleja, ya que pueden camuflarse entre estaciones base legítimas. Sin embargo, tecnologías de monitorización avanzadas en el espectro radioeléctrico permiten identificar características específicas de las torres cercanas y alertar sobre anomalías que indican la presencia de una falsa torre. Aquí es donde, la caracterización del espectro radioeléctrico del entorno de nuestra organización se vuelve imprescindible, más aún, si estamos hablando de infraestructuras críticas. Para ello, como veremos a continuación, es posible desplegar sensores para la monitorización proactiva del espectro.

Monitorización Proactiva de RF para Espacios Sensibles



**CONTINÚA EN
PRÓXIMA PÁGINA**



La vigilancia continua del espectro radioeléctrico es crucial en áreas de alta seguridad, como salas de juntas, laboratorios y zonas donde se manejan datos sensibles (ya lo vimos en otros artículos anteriores). Sistemas de detección de RF pueden identificar en tiempo real las señales no autorizadas, lo cual es esencial para mantener la integridad de la información en estas áreas.

La protección proactiva mediante **monitorización RF** permite detectar dispositivos no autorizados y actividad de espionaje, facilitando una respuesta rápida a potenciales intentos de intrusión y salvaguardando las comunicaciones y la infraestructura. Frente al crecimiento de dispositivos inalámbricos y el avance de las técnicas de ataque, la vigilancia continua se presenta como una de las estrategias más efectivas para fortalecer la seguridad de los entornos empresariales.

Conclusión

Las empresas de hoy en día se enfrentan a un número cada vez mayor de dispositivos inalámbricos en sus instalaciones, lo que crea un panorama de amenazas complejo y en constante evolución. Estos dispositivos, aunque en su mayoría son inofensivos, representan posibles puntos de entrada para actores maliciosos que buscan comprometer la seguridad de la red empresarial. Para mitigar estos riesgos, **es esencial adoptar un enfoque distinto al que estamos acostumbrados**

Hasta ahora, para proteger dispositivos móviles, solíamos usar sistemas MDM, sin embargo, **la seguridad a nivel de agente no es suficiente**. Es crucial comprender si hay

dispositivos no autorizados en zonas sensibles dentro de las instalaciones. Aquí es donde entran en juego las soluciones de seguridad de red RF. Estas soluciones permiten detectar la presencia de teléfonos móviles, geolocalizarlos e identificar a qué operador pertenecen, lo que permite enviar alertas al SOC (Security Operations Center) en caso de que un dispositivo no autorizado entre en una zona restringida.

Además de los dispositivos no autorizados, las empresas también deben ser conscientes de las vulnerabilidades inherentes a los protocolos inalámbricos. Para hacer frente a estas amenazas, las empresas deben adoptar un enfoque que incluya la monitorización continua del espectro radioeléctrico, la detección de dispositivos no autorizados y la aplicación de políticas de seguridad sólidas. Esto implica utilizar soluciones de seguridad de red RF para detectar y localizar dispositivos, implementar sistemas de control de acceso a la red para evitar el acceso no autorizado y mantenerse al día sobre las últimas vulnerabilidades y amenazas.

Como ya venimos resaltando en todos nuestros artículos, es importante destacar que la seguridad inalámbrica no se limita a los dispositivos móviles y los protocolos Bluetooth y GSM. Otros dispositivos y protocolos inalámbricos, como Zigbee, LoRa, TETRA, DMR, etc. también pueden representar un riesgo para la seguridad. Por lo tanto, **las empresas deben adoptar un enfoque integral que abarque todos los aspectos de la seguridad inalámbrica para proteger sus datos, sus empleados y su reputación.**

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

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



La Guerra Invisible: “El Rol del WiFi en las Estrategias Geopolíticas Mundiales”

La tecnología Wi-Fi ha revolucionado nuestra forma de conectarnos e interactuar con el mundo. Sin embargo, en la sombra de esta innovación, se libra una batalla invisible que puede llegar a poner en riesgo nuestra privacidad y seguridad. Hoy, desentrañamos cómo los sistemas de posicionamiento Wi-Fi (WPS) están revolucionando la geoestrategia y la ciberseguridad, y cómo esto nos afecta a todos.

La Geoestrategia del WiFi: Más Allá de la Conectividad

Introducción a los Sistemas de Posicionamiento Wi-Fi

Los Sistemas de Posicionamiento Wi-Fi utilizan los puntos de acceso Wi-Fi cercanos para determinar la ubicación de dispositivos móviles con una precisión sorprendente. Empresas como Apple y Google lideran estos sistemas, permitiendo a los dispositivos consultar servidores especializados para obtener su ubicación en función de los puntos de acceso detectados.

Seguro que habremos notado en muchísimas ocasiones, sobre todo en aplicaciones de mapas, donde el propio dispositivo móvil solicita acceso al wifi para mejorar la precisión del posicionamiento. Esto es así, porque gracias a ese “mapeo” de las redes wireless que realizando estos dos gigantes tecnológicos, se dispone de un mapa detallado de las conexiones wireless que junto con la posición GPS pueden dar una precisión mucho más exacta

El funcionamiento es muy sencillo, nuestros dispositivos móviles están constantemente “escuchando” -eso creo que ya lo sabemos-, y recolectando información de todas las redes wifi que están a su alcance, es decir, están guardando información de todos los BSSIDs, de su potencia, y algún que otro dato más. Esa información se combina con el posicionamiento GPS en el momento de la detección, para así poder ubicar los puntos de acceso wireless en puntos físicos en los mapas. Es decir, nuestros terminales móviles actúan como sensores alimentando una enorme base de datos con nuestros movimientos; actualizando en silencio, y de forma constante toda la información que reconocen a su alrededor. Sobra decir, que esa información puede ser muy “jugosa” para muchas cosas, y puede ser muy codiciada por gobiernos y agencias de inteligencia.

La Amenaza de la Vigilancia Masiva

Recientes investigaciones han revelado que el WPS puede ser explotado para crear amenazas de privacidad a gran escala. A través de la acumulación de datos obtenidos mapeando los BSSID, un atacante puede generar un mapa global de ubicaciones Wi-Fi en cuestión de días sin necesidad de permisos especiales. Al utilizar técnicas de scraping y recopilación masiva de datos, es posible construir una base de datos detallada de ubicaciones de puntos de acceso. Esta capacidad permite rastrear dispositivos individuales a lo largo del tiempo, exponiendo movimientos y patrones de comportamiento de los usuarios.



**CONTINÚA EN
PRÓXIMA PÁGINA**

La explotación del WPS para vigilancia masiva implica la interceptación de consultas de ubicación y la correlación de datos de diferentes fuentes. Un atacante puede utilizar redes Wi-Fi públicas y privadas para recopilar información de dispositivos conectados, identificando patrones de movilidad y posibles puntos de interés. Esta información es valiosa no solo para el espionaje comercial, sino también para operaciones militares y de inteligencia.

El uso indebido del WPS no solo compromete la privacidad personal, sino que también puede facilitar la vigilancia masiva y el espionaje. Imagina un atacante capaz de rastrear dispositivos móviles en zonas de conflicto, obteniendo información sensible sobre posiciones militares y movimientos de tropas. Este nivel de vigilancia tiene profundas implicaciones para la seguridad nacional y la privacidad individual.

Ciberseguridad en Tiempos de Guerra: El Conflicto Rusia-Ucrania

Vigilancia en Zonas de Conflicto

El conflicto entre Rusia y Ucrania ha demostrado ser un campo fértil para la aplicación de nuevas tecnologías de vigilancia avanzada. Utilizando las técnicas descritas en este artículo, es posible monitorizar los movimientos de tropas y la localización de sus bases militares. Para realizar este tipo de vigilancia no se requieren equipos sofisticados ni acceso directo a las infraestructuras de comunicación del enemigo, haciendo que la información obtenida sea extremadamente valiosa para la inteligencia militar.

En el contexto del conflicto, la recopilación de datos de Wi-Fi se realiza mediante dispositivos de recolección de datos desplegados en el terreno y satélites que interceptan señales Wi-Fi. Estos dispositivos capturan información sobre los puntos de acceso y la transmiten a centros de análisis donde se procesan y correlacionan con datos de inteligencia existentes. Este enfoque permite crear mapas dinámicos de las posiciones de tropas y movimientos logísticos.

Impacto en la población civil

Los civiles también se ven afectados por el uso de WPS en zonas de conflicto. El rastreo de dispositivos móviles puede revelar la ubicación de refugiados, hospitales y otros puntos críticos. La interceptación de señales Wi-Fi en áreas urbanas densamente pobladas permite a los analistas de inteligencia obtener información detallada sobre la distribución y movimiento de la población civil, lo que puede ser utilizado para planificar operaciones militares y humanitarias.

Además, el uso de técnicas de triangulación permite identificar dispositivos individuales y sus patrones de movimiento. Esto puede ser utilizado para monitorear a activistas, periodistas y otras personas de interés, exponiéndolas a riesgos adicionales en situaciones ya peligrosas. La capacidad de rastrear dispositivos móviles en tiempo real ofrece una herramienta poderosa tanto para operaciones defensivas como ofensivas.

Otros casos de estudio

Otro de los estudios más impactantes que detalla el informe es el seguimiento de dispositivos en Gaza, demostrando cómo se pueden identificar apagones y desapariciones de dispositivos. Además, se investigaron los efectos de desastres naturales como los incendios en Maui, Hawaii, mostrando el alcance y la versatilidad de esta tecnología en diversas situaciones.

La Batalla Invisible: Espionaje y Geoestrategia

Geoestrategia y Wi-Fi

El seguimiento de dispositivos móviles en áreas como Kiev, Donetsk y otras regiones conflictivas ha permitido obtener una visión detallada de los movimientos militares. Este tipo de análisis ha revelado desplazamientos estratégicos y ha ayudado a predecir acciones futuras. La recopilación de datos se realiza mediante la captura de señales Wi-Fi en puntos estratégicos y el uso de drones equipados con sensores de interceptación de señales.

La Respuesta de los Fabricantes

Ante la divulgación de estas vulnerabilidades, empresas como Apple han tomado medidas para mitigar los riesgos. Ahora, los usuarios pueden optar por no participar en el WPS de Apple, mejorando su privacidad. Sin embargo, estas medidas son solo el primer paso. Es crucial que los fabricantes continúen desarrollando soluciones más robustas para proteger la privacidad a nivel global.

Conclusiones

El futuro de la ciberseguridad en redes Wi-Fi depende de la colaboración entre usuarios, fabricantes y reguladores. Es esencial desarrollar políticas y tecnologías que protejan la privacidad sin sacrificar la funcionalidad. Por otro lado, los fabricantes deben esforzarse, en seguir mejorando sus sistemas de privacidad y seguridad, implementando características que limiten el acceso no autorizado a datos de geolocalización.

Así pues, la tecnología Wi-Fi, aunque revolucionaria, presenta desafíos significativos en términos de ciberseguridad y privacidad. La capacidad de utilizar sistemas de posicionamiento para la vigilancia masiva y el espionaje geoestratégico subraya la importancia de una ciberseguridad robusta. Los usuarios y fabricantes deben trabajar juntos para proteger la privacidad y asegurar que la conectividad no se convierta en una herramienta para la vigilancia maliciosa. En tiempos de conflicto como el de Rusia y Ucrania, la seguridad digital se convierte en una cuestión de vida o muerte, haciendo imperativo que tomemos medidas proactivas para defender nuestra privacidad y seguridad.

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



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



Security Operations Center

Introducción: El Panorama del SOC Moderno

Con un escenario donde el perímetro es totalmente difuso debido a la movilidad de los trabajadores, la migración de las aplicaciones al cloud y las consecuencias de la adopción de proyectos de transformación digital dentro de las organizaciones. Hace que la superficie de exposición, y las vulnerabilidades hayan incrementado de forma exponencial en los últimos años.

Poco a poco, las organizaciones de todos los tamaños se han dado cuenta de sus limitaciones en cuanto a personal y experiencia para abordar adecuadamente esta creciente necesidad de proteger su negocio de las constantes amenazas de los cibercriminales.

La enorme inversión que se tiene que realizar para poder disponer de un SOC (Security Operations Center), es algo que muy pocas organizaciones pueden permitirse. No sólo debemos pensar en la inversión tecnológica, sino también en la inversión de talento y capital humano necesario para abordar el conocimiento de todas las plataformas tecnológicas existentes alrededor de un SOC

Selección y Recolección de los Datos Adecuados

La selección y recolección de los datos correctos es vital para el funcionamiento eficaz de cualquier SOC. Esta estrategia implica la cuidadosa consideración del valor relativo de diferentes tipos de datos, como la información proveniente de sensores y los datos de registro recolectados por sistemas de red y del endpoint, recursos en

cloud, aplicaciones, etc. Lo primero que se suele plantear en un proyecto de SOC para recopilar toda esta información, es instalar un SIEM.

A pesar de que, por lo general, existe una clara conciencia de que las soluciones SIEM son complejas de instalar, muchas organizaciones se aventuran a la instalación de este tipo de soluciones sin definir claramente objetivos, requisitos y estimaciones de crecimiento. Incluso se aventuran a pensar que hay soluciones que "out of the box" ya pueden cumplir sus requisitos. Una mala planificación hace que, por lo general, el proyecto no se implemente de forma adecuada, obteniendo unos resultados que no son los esperados o que no cumplen las expectativas generadas

Otro de los errores que más se cometen a la hora de implantar un SIEM, es no definir claramente un alcance. Es habitual encontrarse con dos extremos, los que no definen un alcance y aquellos que su alcance es "monitorizarlo todo".

Evidentemente, ambos extremos son perjudiciales, y como se suele decir en el equilibrio está la clave. Querer abarcarlo todo desde un principio es complicado, sobre todo porque este tipo de herramientas requieren de la coordinación con muchas otras áreas de TI (sistemas, redes, etc.) y no sólo eso, sino que también hay que tener en cuenta que no basta con integrar las fuentes de información directamente en un SIEM, sino que hay que diseñar previamente qué información queremos recopilar de cada fuente, el formato y la retención que queremos tener.

Estos factores condicionaran tanto la elección de la herramienta, el hardware elegido, la arquitectura del sistema, las licencias y por supuesto tendrá un impacto en el presupuesto. Por tanto, son claves para el éxito de un proyecto de estas características. Algunos de los puntos clave a tener en cuenta para la instalación de un SIEM son, entre otros:

- Evaluar las necesidades, recursos disponibles y el nivel de madurez de la organización para determinar si una herramienta SIEM puede sernos de utilidad
- Hacer una pequeña lista de proveedores de SIEM, y estudiar con detenimiento si las propuestas se ajustan a las necesidades de tu organización
- Siempre que sea posible, es interesante hacer una prueba de concepto (PoC) para conocer el producto en detalle y saber si se ajusta a nuestras necesidades
- Definir el alcance del proyecto, si fuese necesario repartirlo en varias fases
- Conocer las dependencias tecnológicas del alcance definido
- Definir un set inicial de reglas que cubra las necesidades de detección. Este set de reglas podrá ampliarse en fases posteriores del proyecto, incluso combinarlo con trabajos de "caracterización de amenazas" para conocer qué gaps tenemos.
- Evaluar regularmente el funcionamiento del SIEM, incluir nuevas reglas de detección (casos de uso) lo cual redundará en una mejor postura de defensa de la organización



**CONTINÚA EN
PRÓXIMA PÁGINA**

Priorizar la Respuesta a Incidentes

Un aspecto esencial en la operación de un SOC es la respuesta a incidentes. Esta debe ser priorizada de forma organizada y sistemática. Para esto, el uso de **manuales de procedimientos (playbooks) es vital, pues permite estandarizar la respuesta a incidentes de forma efectiva**. Un manual de procedimientos generalmente incluye: título, intención, alcance, condiciones estimulantes (circunstancias en las que se debe usar el manual), procedimientos, pasos y expectativas a seguir, y varios metadatos (quién lo aprobó, historia de revisión). Aunque el SOC no siga con frecuencia un escenario de respuesta a incidentes, puede ser útil codificar ese tipo de incidente en un procedimiento operativo estándar (SOP) para que la próxima persona no tenga que reaprender el proceso.

El arte de escribir manuales de procedimientos efectivos reside en balancear la cantidad de detalle y especificidad, y al mismo tiempo entender que algunos detalles cambiarán con cada incidente. Es necesario capturar aquellos aspectos que son consistentes entre un tipo específico de tecnología y un incidente de alta prioridad para el constituyente. Si un manual es muy general, los respondientes cibernéticos experimentados lo complementarán con su propio conocimiento, lo que puede ser bueno, pero también puede llevar a inconsistencias y a que otros queden sin información. Igualmente, si dejan la organización, su conocimiento se irá con ellos.

Es necesario capturar suficiente detalle para que los respondientes cibernéticos menos experimentados entiendan cómo responder a un incidente y que los respondientes más experimentados sean consistentes en su enfoque.

Por otro lado, un exceso de detalle puede hacer que el manual se vuelva obsoleto rápidamente y puede sofocar la capacidad de los analistas para actuar por intuición y adaptarse al incidente. Finalmente, cuando el SOC explica un incidente a las partes interesadas y a la alta dirección, el mensaje debe ser claro y conciso. **La explicación no debe enfocarse en bits y bytes sino en la misión, los costos y a veces las vidas.** Las cuatro preguntas que se deben responder son: (1) qué (y/o quién) fue el objetivo, (2) si el adversario tuvo éxito, (3) quién es el adversario y cuál es su motivación, y (4) cómo continuar la misión.

Contratar y Desarrollar Personal de Calidad

La tecnología sin personas que la operen, no sirve de nada. Por tanto, a la hora de planificar un SOC, el personal es el aspecto más importante. Numerosas encuestas indican que la contratación de personal es la principal preocupación para aquellos que trabajan en el campo de la ciberseguridad y que la escasez de habilidades tiene un impacto significativo en sus organizaciones.

No solo se trata de contratar talento, también es necesario crear un ambiente que anime al personal a quedarse ("fidelización del talento"), mientras se planifica para la eventual rotación que, queramos o no, ocurrirá. A la hora de hacer las contrataciones ya no vale guiarse por la "titulitis" en este sector, hay aspectos que marcan mucho la diferencia entre los profesionales de ciberseguridad:

•**Pasión por la ciberseguridad:** Es quizás la principal cualidad a buscar en cualquier posible contratación al SOC, independientemente de la posición o el nivel de experiencia.

•**Entusiasmo, curiosidad y sed de conocimiento:** Un especialista en ciberseguridad debe ser entusiasta, curioso y siempre querer aprender más.

•**Habilidades blandas y trabajo en equipo:** El candidato ideal debe demostrar habilidades en el manejo de personas y debe

tener una disposición al trabajo en equipo.

•**Conocimientos técnicos:** Un candidato debe demostrar conocimientos generales de TI y ciberseguridad, así como un conocimiento profundo en al menos una o dos áreas relacionadas con las operaciones de ciberseguridad.

Ahora bien, una vez tenemos a nuestro personal, como si de un gimnasio se tratase, hay que proveerles de un entrenamiento para mejorar su capacidades y saciar su ansiedad por nuevos conocimientos.

El entrenamiento formal del personal es esencial para asegurar una base de conocimientos técnicos y la adhesión a procesos relevantes del SOC. Esto puede incluir un proceso de calificación técnica o "check-ride" que cada nueva contratación debe pasar dentro de un período de tiempo específico después de la contratación. Este tipo de procesos asegura que todos los empleados puedan operar con un nivel base de capacidades técnicas y una adhesión consistente a los procesos relevantes del SOC, dependiendo de su función laboral. El programa también debe incluir actividades de enriquecimiento, tales como asistencia a congresos de seguridad, simulacros, asistencia a foros donde se comparten procesos y procedimientos que ayudan a una mejor gestión del SOC.

Por esta razón, es necesario que tengamos en consideración la formación de los líderes que van a gestionar el SOC, prepararles para trabajar en ambientes de mucha presión, y con skills que no sólo van a ser técnicos, hay que trabajar mucho su faceta de comunicación con la alta dirección, y con actores externos, como pueda ser la prensa, por ejemplo.

Y si entramos en la formación, también debemos considerar formar a nuestra alta dirección en el entendimiento de qué es un SOC, y de cómo actuar ante un ciberincidente. Que todas las partes implicadas en un incidente de seguridad estén bien formadas, es la clave para restaurar en el menor tiempo posible la normalidad sin que para ello exista un grave impacto en la continuidad de negocio, y en la reputación e imagen de la organización.

Conclusión: El Camino hacia la Excelencia en Ciberseguridad

El establecimiento de un centro de operaciones de seguridad requiere de un entendimiento profundo de los datos, la tecnología y, sobre todo, el factor humano. La selección y la recolección de los datos correctos, el uso de herramientas, el desarrollo tanto del personal como la alta dirección, así como la priorización de la respuesta a incidentes son los pilares fundamentales de un SOC eficaz.

Para garantizar un buen funcionamiento del SOC, es crucial **mantener una comunicación clara y una colaboración fluida con todas las partes interesadas**. Esto incluye a la alta dirección, los responsables de IT y los usuarios. La capacidad de traducir jerga técnica en lenguaje de negocios, la elaboración de informes claros y concisos, y el establecimiento de métricas y KPIs relevantes son elementos clave para la eficacia del SOC.

Además, con un servicio de seguridad gestionada adecuado, las organizaciones tendrán la tranquilidad de saber que hay un equipo de expertos cualificados que supervisan constantemente su empresa, buscan amenazas, investigan actividades sospechosas y responden a posibles incidentes.

Con el panorama de amenazas a la ciberseguridad en permanente evolución, trabajar con un equipo cuyo único objetivo es la ciberseguridad aporta tranquilidad a su empresa para que pueda centrarse en su negocio.

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



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



La Guerra Electrónica y el control del espectro

En la actualidad, el espectro electromagnético se ha convertido en un recurso muy codiciado, y juega un papel fundamental en nuestro día a día, donde una gran mayoría de nuestras comunicaciones tienen lugar. Hasta tal punto que, si se provocasen interrupciones o disrupciones en los sistemas de comunicaciones inalámbricos, tendría consecuencias devastadoras para la sociedad.

Es por esta razón que, en el contexto actual geopolítico en el que vivimos, vemos constantemente como el término *Guerra Electrónica* (EW) lleva años saltando periódicamente en muchos medios de comunicación. Pero, ¿qué es la guerra electrónica?

LA LUCHA POR EL CONTROL DEL ESPACIO RADIOELÉCTRICO

El término de guerra electrónica no es algo nuevo, es más, los seres humanos llevan luchando por el control del espacio electromagnético prácticamente desde que somos conocedores de su existencia. Si nos ceñimos estrictamente a lo que podríamos denominar una definición de guerra electrónica, podemos decir que, bajo las siglas EW (Electronic Warfare), se engloba cualquier acción militar que involucre el espacio electromagnético para controlar su uso. Su objetivo principal reside en la capacidad de interferir los sistemas de detección y comunicaciones del adversario, lo que puede incluir la perturbación de radares, comunicaciones por radio, y otros dispositivos electrónicos.

Contrariamente a lo que se pueda pensar, la EW en el contexto del ejército no es algo reciente. Desde que se tiene conocimiento de propagación de las ondas de radio, se intuyó que, si servía para enviar mensajes, también podría servir para sintonizar las radios del bando enemigo e interceptar sus mensajes, lo que llevó al desarrollo de dispositivos capaces de interceptar las señales y, con ello, el desarrollo de técnicas de cifrado para evitar la interceptación de información.

A día de hoy, tanta es su importancia, que ya se considera un dominio o ámbito de interés en el que se desarrollan las operaciones militares, al igual que el espacio cibernético. Y es que, no cabe duda que ante la imparable digitalización de los sistemas de información que estamos viviendo en los últimos tiempos, junto con la proliferación de sistemas y redes de comunicaciones inalámbricos que permiten acceder a sistemas que hace años se encontraban offline, está proporcionando la inevitable convergencia y la interoperabilidad de múltiples tecnologías, plataformas, sensores, sistemas de mando y control, así como, sistemas de armas.



CONTINÚA EN
PRÓXIMA PÁGINA



SIEMENS
MANN



Sin ánimo de ser exhaustivos, y con una finalidad meramente divulgativa y no técnica, se van a exponer conceptos y elementos que configuran la Guerra Electrónica (EW). Históricamente se ha dividido en diferentes segmentos, según hablemos de:

- ESM** (Medidas de apoyo electromagnético): comprende las acciones adoptadas para buscar, interceptar, identificar o localizar fuentes de energía electromagnética radiada, intencionalmente o no, con el propósito de reconocer inmediatamente cualquier indicio de amenaza.

- ECM** (Contramedidas electromagnéticas): comprende las medidas adoptadas para impedir o reducir la utilización del espectro electromagnético por parte del adversario. Estas medidas incluyen, entre otras, la perturbación, el uso de chaffs o bengalas y las técnicas de engaño.

- EPM** (Medidas de protección electromagnéticas): son aquellas medidas tomadas para la protección de los sistemas electrónicos para contrarrestar los efectos de las contramedidas del adversario.

NUEVOS ESCENARIOS DE LA GUERRA ELECTRÓNICA

En el actual conflicto entre **Ucrania y Rusia** se está llevando a cabo un juego del gato y el ratón para interferir mutuamente en sus sistemas hasta un nivel nunca visto y poniendo de manifiesto la importancia de la EW. Tanto es así, que está teniendo afectación sobre la sociedad civil, en forma de denegación de los sistemas GNSS en algunas zonas, supuestos cortes en los cables submarinos que dan servicio de internet.

De hecho, comienza una confluencia del dominio del espectro electromagnético y el dominio ciber. A día de hoy, la gran mayoría de nuestros sistemas de comunicación emplean el protocolo IP, lo cual lo hace más susceptible de recibir ataques. Y aunque pueda parecer descabellado, todo el conocimiento que se está

adquiriendo derivado del conflicto de Ucrania y Rusia puede tener consecuencias en otras partes y por otros actores maliciosos.

Con esto, vuelve a tener una relevancia muy importante lo que en esta sección llevamos comentando desde hace muchos artículos; cuando hablamos de ciberseguridad también tenemos que pensar en los sistemas de comunicaciones inalámbricos, a los cuales se le pueden aplicar medidas de Guerra Electrónica. Tanto es así, que por ejemplo, recientemente salió a la luz, un ataque muy simple que conseguía denegar el servicio de carga de los vehículos EV, inhabilitando el canal de comunicación entre el cargador y el vehículo aplicando técnicas de jamming haciendo que el cable por el que se comunican ambos dispositivos se "llenase" de "ruido" y fuese imposible la comunicación.

Y no solo es aplicable al caso de uso de los vehículos, también se utilizan técnicas de jamming para los sistemas de alarmas o, como ya vimos en un artículo de esta sección, para la escucha de los micrófonos inalámbricos de la alta dirección de una gran empresa. Eso, combinado con drones, tal y como se pudo ver en el ejemplo que contamos en un artículo en el 2024, es posible acceder a las redes wireless de una organización.

CONCLUSIONES

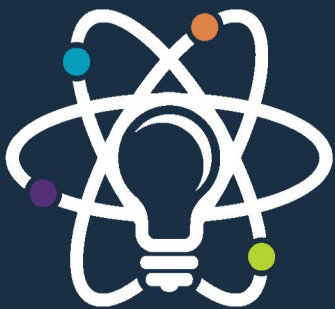
En definitiva, sólo decir que estamos ante el principio de una evolución tecnológica donde los sistemas inalámbricos de comunicaciones juegan un papel fundamental. Y que en nuestros planes de protección, planes directores de seguridad, y mapas de riesgos debemos contemplar los sistemas de comunicaciones inalámbricos como un riesgo más y darles todo el cariño necesario para implementar los controles de seguridad que nos permitan disminuir el riesgo de ataque.

Gov Book

Governance

Body of Knowledge

P4MGO!®



P4MGO!
PORTFOLIO, PROGRAMME
PROJECT & PRODUCT
MANAGEMENT & GOVERNANCE

Amenazas no convencionales en el mundo del IoTM

A medida que las nuevas tecnologías se expanden, también lo hacen los desafíos de seguridad asociados. Es normal ver como muchas organizaciones disponen de controles de seguridad basados en red, como el control de acceso (NAC), Firewalls, IDS, IPS, EDR, XDR, registros de todos los movimientos de los usuarios, etc.

Estas soluciones de seguridad cubren una gran parte de las amenazas a las que se enfrentan las organizaciones, pero existen entornos críticos que, con el aumento de las tecnologías de comunicaciones inalámbricas y la rápida adopción de estas, se hace necesario implantar nuevos controles de seguridad que tengan en consideración también el espacio radioeléctrico: es el claro ejemplo del mundo del IoTM (Internet de las cosas médicas).

El IoTM es la aplicación de la tecnología de internet de las cosas en el sector sanitario, siendo una de las áreas donde sus beneficios son más importantes y evidentes.

¿POR QUÉ ES IMPORTANTE PROTEGER EL MUNDO DEL IOTM?

Las empresas de tecnología médica fabrican una amplia variedad de dispositivos médicos (se cifra en más de medio millón), una cantidad nada despreciable, que puede ser considerada una superficie de exposición notable.

Entre estos dispositivos se incluyen marcapasos, monitores de glucosa en sangre, bombas de insulina, dispositivos de imagenología portátiles, wearables para el seguimiento de signos vitales, y equipos de telemedicina, entre muchos otros.

La adopción del IoTM conlleva beneficios significativos, como la mejora en la atención al paciente, mayor eficiencia de los profesionales sanitarios, diagnósticos más precisos y una mejor prevención de enfermedades. Sin embargo, también presenta desafíos, como garantizar la seguridad y privacidad de los datos.



CONTINÚA EN
PRÓXIMA PÁGINA



A 1.25

En definitiva, la capacidad de estos dispositivos médicos de conectarse a internet, en muchos casos, de forma inalámbrica, para transmitir información en tiempo real está revolucionando la medicina, pero también estamos abriendo la puerta a ataques y amenazas más complejas que pueden explotar estos protocolos de comunicación inalámbricos.

LA NECESIDAD DE IMPLANTAR SISTEMAS DE DEFENSA DEL ESPACIO RADIOELÉCTRICO

Un ataque mediante RF es un tipo de ataque que no requiere encontrarse próximo al dispositivo objetivo, lo cual lo hace más difícil de detectar y proteger. Estos ataques, como el lector ya podrá imaginar, pueden llegar a tener consecuencias desastrosas, ya que pueden causar que estos dispositivos interrumpan sus funciones, o puedan acabar dañados por el atacante, poniendo en peligro la salud del usuario.

En muchas ocasiones, los fabricantes, en la fase de diseño, no consideraron una amenaza que estos dispositivos fuesen atacados usando comunicaciones inalámbricas, por lo que durante su concepción no aplicaron controles de seguridad. Pero hoy en día, con el abaratamiento de los sistemas SDR (radios definidas por software) y la gran cantidad de información accesible en internet, hace que sea más factible que un atacante quiera usar las comunicaciones inalámbricas como vector de ataque.

Sin embargo, y ante la gravedad del problema, hemos de afirmar que abordar el problema no es sencillo; si bien existen soluciones de seguridad muy enfocadas al mundo del IoT, estas no contemplan las amenazas que tienen como vector de ataque los sistemas de radiofrecuencia, y en otras ocasiones, los protocolos de comunicaciones usados no son seguros desde su concepción.

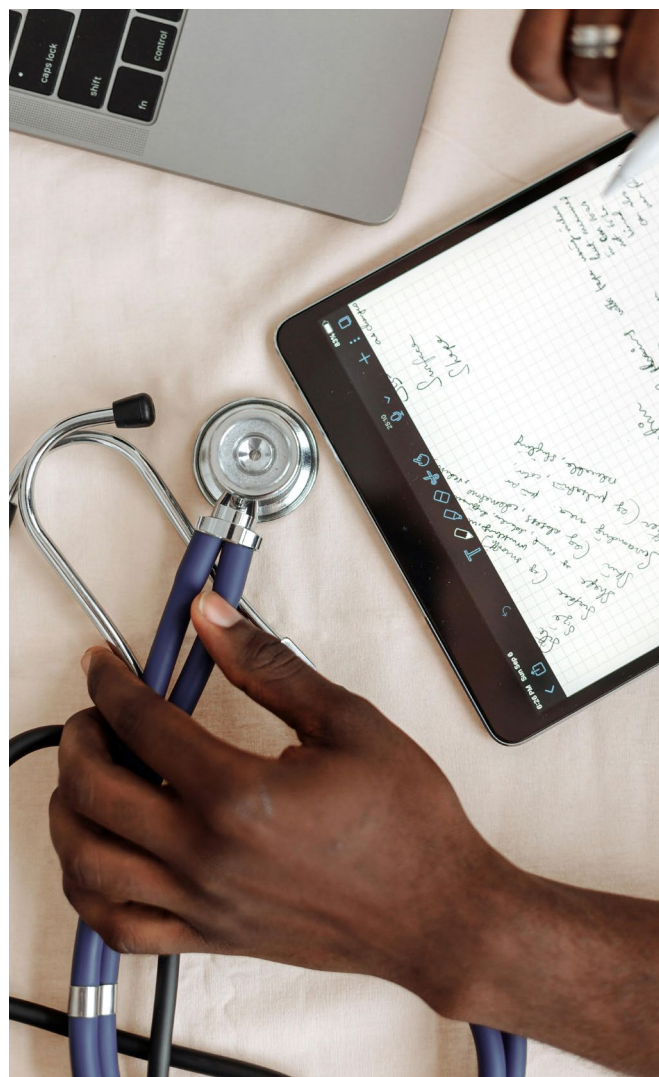
Para poder abordar este tipo de amenazas, es necesario un enfoque totalmente distinto al que venimos acostumbrados en la protección de otros activos. Evidentemente, hay que seguir prestando atención a los ataques que vienen a través de la red, pero también hay que buscar otro enfoque, que contemple el análisis del espectro radioeléctrico, analizando las señales electromagnéticas emitidas por los diversos dispositivos IoT para poder determinar anomalías y desviaciones del comportamiento normal del dispositivo, lo que ayudaría a identificar actividades maliciosas, acceso no autorizados y filtraciones de datos, entre otros ataques.

Para resolver el problema mencionado, existen diversos grupos de investigadores y empresas privadas que buscan, mediante el análisis de las señales radio, distinguir entre transmisiones legítimas y no autorizadas, para poder detectar estos tipos de ataques. Para ello, utilizan técnicas de sensado de espectro radioeléctrico, usando para ello equipos de radio definida por software (SDR).

Son técnicas que ahora nos parecen excesivamente complicadas pero ya existen empresas y entornos donde estas medidas forman parte ya de su plan de seguridad. Y es que, la tecnología avanza hacia un mundo sin cables.

¿POR QUÉ ES ESENCIAL PROTEGER LOS DISPOSITIVOS DE LAS AMENAS DE RF?

Para comprender más en detalle a qué riesgos nos enfrentamos, veamos a modo resumen algunas razones por las que es importante protegernos de las amenazas de RF:



•**Superficie de ataque en expansión:** a medida que más dispositivos dependen de la conectividad inalámbrica, el nivel de riesgo aumenta en proporción. Y, aunque no es muy popular, existen grupos especializados en atacar sistemas usando como vector de ataque los sistemas RF.

•**Detección de ataques “invisibles”:** los atacantes suelen explotar vulnerabilidades en protocolos de comunicaciones que, normalmente, las organizaciones no tienen en cuenta. Convirtiéndose en puertas de entrada silenciosas donde no se han implementado controles de seguridad.

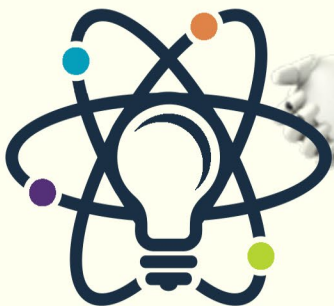
•**Monitorización y sensado del espectro:** los dispositivos IoT e IoTm usan distintas frecuencias y protocolos para sus comunicaciones, por lo tanto es importante disponer de sistemas de sensado de RF y detección de actividad no convencional en una gran variedad de frecuencias

Conclusión

Dado que los sistemas de comunicaciones inalámbricos cada vez son más comunes en estos entornos, debemos incorporar en nuestros planes de protección, planes directores de seguridad, y mapas de riesgos que incluyan los sistemas de comunicaciones inalámbricos como un riesgo más y darles todo el cariño necesario para implementar los controles de seguridad que nos permitan disminuir la probabilidad de que estos ataques puedan materializarse.

CoE Book

Centres of Excellence Body of Knowledge P4MGO!®



P4MGO!

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



Desentrañando la Ciberseguridad en Redes Tácticas 6G: Amenazas, Arquitectura e Inteligencia Artificial

La evolución de las comunicaciones móviles hacia la sexta generación (6G) ha abierto un abanico de posibilidades en entornos críticos y tácticos, donde la seguridad y la disponibilidad se convierten en pilares fundamentales para la operatividad. En un contexto donde las redes deben ser resilientes y seguras en situaciones de emergencia, el desarrollo de infraestructuras tácticas se convierte en una necesidad imperiosa para organismos de seguridad pública, defensa y emergencias. Esta transformación no solo implica una mejora en las capacidades de transmisión y procesamiento de datos, sino también la integración de tecnologías emergentes que permitan una respuesta ágil y adaptativa ante amenazas cibernéticas. La integración de redes terrestres y no terrestres, la computación en el borde (edge computing) y la inteligencia artificial (IA) son algunos de los conceptos revolucionarios que configuran el nuevo ecosistema de las comunicaciones 6G.

Estas tecnologías permiten la creación de **“burbujas tácticas”**, redes privadas de despliegue rápido que garantizan conectividad en zonas de desastre, áreas remotas o escenarios de alta incertidumbre. La combinación de estas soluciones tecnológicas posibilita la entrega de servicios críticos como videoconferencias de alta definición, supervisión en tiempo real y control remoto de dispositivos, pero sin olvidar una parte muy importante la seguridad de la información.

Evolución y Relevancia de las Redes Tácticas en 6G

La transición de las tecnologías de comunicación tradicionales a soluciones basadas en 6G se fundamenta en la necesidad de satisfacer exigencias cada vez más complejas en entornos críticos. Durante décadas, las comunicaciones de seguridad pública se han apoyado en infraestructuras específicas, como la TETRA, pero el avance hacia redes basadas en estándares 3GPP ha permitido la convergencia de servicios y la optimización de recursos. Esta evolución no solo mejora la eficiencia operativa, sino que también reduce los costes al aprovechar infraestructuras comerciales que se extienden con soluciones privadas y de despliegue rápido.

El concepto de **"burbuja táctica"** surge como respuesta a escenarios en los que la infraestructura convencional no está disponible o ha sido comprometida, como en catástrofes naturales o ciberataques a gran escala. Estas burbujas permiten la implementación inmediata de una red autónoma, capaz de operar de forma aislada y de gestionar aplicaciones críticas como la comunicación en grupo, la vigilancia en tiempo real y el control remoto de vehículos y robots. La integración de capacidades de IA y análisis de datos en el borde (edge computing) de la red añade una capa adicional de inteligencia, permitiendo una orquestación rápida y flexible de los recursos disponibles.

Arquitectura de Seguridad para Redes Tácticas

El diseño de una arquitectura de seguridad para redes tácticas 6G requiere un enfoque que abarque desde la protección del acceso a la red hasta la seguridad de las aplicaciones y servicios desplegados. Los estándares 3GPP han establecido una base sólida en cuanto a procedimientos de autenticación, autorización y encriptación, los cuales se extienden a la integración de redes no terrestres mediante protocolos específicos para garantizar la protección de los enlaces de backhaul.



CONTINÚA EN
PRÓXIMA PÁGINA

El diseño de la arquitectura de seguridad se fundamenta en principios como la exposición controlada de capacidades, la automatización a través de inteligencia artificial y la escalabilidad para adaptarse a distintas topologías y volúmenes de tráfico. En las **burbujas tácticas**, es fundamental que los dispositivos y sistemas se autenticuen mutuamente antes de intercambiar información, lo que se logra mediante el uso de certificados digitales, credenciales específicas y protocolos de seguridad reforzados. La separación de funciones y la segmentación de la red permiten limitar el alcance de un posible compromiso, reduciendo el riesgo de que un ataque se propague de manera incontrolada.

La arquitectura también incorpora mecanismos para la gestión dinámica y la orquestación de servicios de seguridad, apoyados en tecnologías de virtualización y en redes definidas por software (SDN). Estas soluciones posibilitan la implementación de políticas de seguridad que se adaptan en tiempo real a los cambios en el entorno operativo. La integración de sistemas de detección de intrusiones y de respuesta automática a incidentes permite no solo identificar amenazas en etapas tempranas, sino también activar medidas de mitigación que protejan la continuidad del servicio. La resiliencia operativa se refuerza mediante el uso de redundancia y la capacidad de aislamiento de segmentos comprometidos, garantizando que incluso en el peor de los escenarios, la red pueda seguir funcionando en la medida de lo posible.

Desafíos y Perspectivas Futuras en la Ciberseguridad Táctica 6G

A pesar de los avances tecnológicos, la implementación de soluciones de ciberseguridad en entornos tácticos 6G enfrenta desafíos significativos que requieren una atención continua por parte de investigadores y profesionales. Uno de los principales retos reside en la interoperabilidad de sistemas heterogéneos, donde dispositivos de distintos fabricantes y protocolos diversos deben operar de manera coordinada. Esta diversidad complica la integración de mecanismos de seguridad unificados y obliga a diseñar soluciones que sean lo suficientemente flexibles para adaptarse a distintos escenarios operativos sin sacrificar la robustez de las medidas de protección.

Otro desafío relevante es el equilibrio entre el rendimiento y la seguridad. Las aplicaciones de misión crítica, que requieren latencias extremadamente bajas y un alto ancho de banda, imponen restricciones que pueden entrar en conflicto con la implementación de capas adicionales de encriptación y autenticación.

Este escenario demanda innovaciones en algoritmos de seguridad que sean eficientes y que, al mismo tiempo, ofrezcan un nivel de protección acorde a los estándares

de resiliencia necesarios para la operatividad en situaciones de alta tensión. La investigación en criptografía post-cuántica y en técnicas de encriptación es fundamental para superar estas barreras y asegurar que las redes 6G puedan mantener la integridad y confidencialidad de los datos sin comprometer la velocidad de procesamiento.

La colaboración entre organismos de investigación, industrias y entidades gubernamentales se vislumbra como una necesidad imperiosa para avanzar en este campo. La estandarización de protocolos y la elaboración de marcos regulatorios adaptados a las nuevas realidades tecnológicas permitirán crear un ecosistema de seguridad robusto y adaptable. En este sentido, en España hemos avanzado algunos pasos, ya que disponemos del ENS5G (Esquema Nacional de Seguridad 5G), lo que permite regular y definir una línea base para la seguridad de las redes 5G.

Conclusiones

La transformación digital en el ámbito de las **comunicaciones tácticas** ha alcanzado un punto de inflexión crucial con la llegada del 6G. Las nuevas capacidades tecnológicas, la integración de redes terrestres y no terrestres y el uso intensivo de inteligencia artificial están redefiniendo la forma en que se protege la información y se aseguran los servicios críticos en entornos operativos.

La arquitectura de seguridad propuesta para redes tácticas 6G se fundamenta en principios sólidos que abarcan desde la autenticación y la autorización hasta la encriptación y la gestión dinámica de recursos. La implementación de soluciones basadas en SDN, NFV y otras tecnologías de virtualización garantiza la flexibilidad necesaria para operar en entornos heterogéneos y en condiciones adversas.

En conclusión, la ciberseguridad en redes tácticas 6G representa un desafío de gran envergadura, pero también una oportunidad única para transformar el paradigma de la protección en entornos críticos.

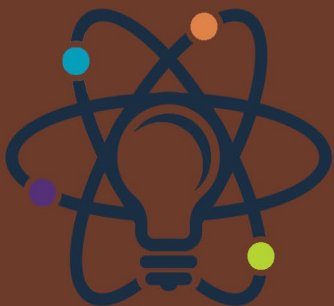
El camino hacia un ecosistema seguro exige la convergencia de tecnologías de vanguardia, la colaboración estrecha entre sectores y el compromiso continuo con la innovación. Solo a través de una estrategia integral y adaptativa será posible garantizar que, en el futuro, las comunicaciones en situaciones de emergencia sean no solo eficientes, sino también inviolables.

PMO Book

Management Offices

Body of Knowledge

P4MGO!®



P4MGO!

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





Así se protege una infraestructura 5G frente a ciberataques

La quinta generación de redes de comunicaciones móviles (5G) ya es una realidad en muchos países, y millones de usuarios hacen uso diario de esta tecnología. Por sus características técnicas, 5G permite conexiones permanentes, ubicuas, de gran capacidad y, sobre todo, de muy alta velocidad.

Con la llegada de esta tecnología, se abre un enorme potencial de transformación, con un impacto multiplicador en la productividad empresarial, la automatización industrial, los servicios críticos y la conectividad de dispositivos, etc. Sin embargo, como toda innovación disruptiva, su adopción conlleva nuevos retos y ciberriesgos que deben ser cuidadosamente analizados y gestionados. La tecnología 5G no solo representa un salto cuantitativo en velocidad y capacidad de conexión, sino también un cambio cualitativo en la forma en que se diseñan y operan las redes móviles. Este nuevo paradigma trae consigo oportunidades sin precedentes, pero también introduce desafíos significativos en materia de ciberseguridad. En este artículo, profundizaremos en los elementos arquitectónicos clave de 5G, las amenazas emergentes y las estrategias para mitigar los riesgos asociados.

ARQUITECTURA DE 5G: UN ECOSISTEMA COMPLEJO Y DINÁMICO

La arquitectura de las redes 5G representa una evolución significativa respecto a las generaciones anteriores, caracterizándose por su flexibilidad, escalabilidad y capacidad

para adaptarse a una amplia variedad de casos de uso. Esta transformación es posible gracias a la integración de tecnologías avanzadas que permiten una gestión más eficiente y dinámica de los recursos de red.

En particular, las redes 5G adoptan un enfoque basado en servicios (Service-Based Architecture, SBA), donde las funciones de red se implementan como componentes modulares y virtualizados, usando muchas de las tecnologías que conocemos en el ámbito del mundo IT.

Esta modularidad facilita la implementación de servicios personalizados y la adaptación rápida ante las demandas cambiantes del mercado. Además, la separación entre el plano de control y el plano de usuario permite una gestión más granular y eficiente del tráfico de red.

Como comentábamos, muchas de las tecnologías son conocidas y vienen del mundo IT, a continuación nombramos algunas detallando sus funciones dentro del ecosistema del 5G:



CONTINÚA EN
PRÓXIMA PÁGINA

•**Virtualización de Funciones de Red (NFV):** NFV transforma funciones de red que tradicionalmente requerían hardware especializado en aplicaciones que se ejecutan sobre infraestructura de propósito general. Esto reduce la dependencia de hardware propietario y permite una implementación más ágil de nuevos servicios. No obstante, la virtualización también amplía la superficie de ataque, ya que las funciones virtualizadas pueden ser susceptibles a vulnerabilidades del sistema operativo o del hipervisor.

•**Computación en el Borde (Edge Computing):** La computación en el borde acerca el procesamiento de datos al usuario final, reduciendo la latencia y mejorando la eficiencia en aplicaciones sensibles al tiempo, como vehículos autónomos o realidad aumentada. Esta proximidad también plantea retos de seguridad, ya que los nodos de borde pueden ser más vulnerables a ataques físicos o cibernéticos.

•**Segmentación de Red (Network Slicing):** La segmentación de red permite crear múltiples redes virtuales independientes sobre una misma infraestructura física, cada una optimizada para diferentes casos de uso y con políticas de seguridad específicas.

Esta capacidad es esencial para atender las diversas necesidades de aplicaciones como IoT, comunicaciones críticas o servicios de alta velocidad. Sin embargo, la gestión de múltiples segmentos introduce complejidad adicional en términos de orquestación y aislamiento de seguridad.

AMENAZAS EMERGENTES EN 5G

Tal y como comentábamos en la sección anterior, la adopción de tecnologías como la virtualización de funciones de red (NFV), las redes definidas por software (SDN) y la computación en el borde (edge computing) ha introducido vulnerabilidades que los atacantes pueden explotar. Además, la implementación de la segmentación de red (network slicing) y la proliferación de dispositivos IoT han multiplicado los vectores de ataque, requiriendo una revisión exhaustiva de las estrategias de seguridad existentes.

En este contexto, es fundamental identificar y comprender las amenazas emergentes que afectan a las redes 5G. Estas amenazas no solo comprometen la integridad y disponibilidad de los servicios, sino que también ponen en riesgo la privacidad de los usuarios y la confidencialidad de los datos transmitidos. La creciente dependencia de proveedores externos y la complejidad de las cadenas de suministro tecnológicas añaden capas adicionales de riesgo que deben ser gestionadas de manera proactiva.

A continuación, se detallan algunas de las principales amenazas que enfrentan las redes 5G:

•**Ataques a la Identidad y Privacidad del Usuario:** Aunque 5G implementa mecanismos como el SUCI para proteger la identidad del usuario, estudios han revelado que el protocolo

de 5G-AKA aún presenta vulnerabilidades. Estas incluyen ataques de vinculación que permiten rastrear a un usuario a lo largo del tiempo y capturas de IMSI (International Mobile Subscriber Identity), especialmente cuando se emplean esquemas de cifrado nulos o configuraciones inseguras por parte de los operadores.

•**Vulnerabilidades en APIs y Gestión de IoT:** El uso intensivo de APIs para la gestión de dispositivos IoT en redes 5G ha introducido nuevos vectores de ataque. Investigaciones han identificado fallos en la autenticación y control de acceso en estas interfaces, permitiendo potencialmente el acceso no autorizado a datos y funciones críticas.

•**Ataques de Denegación de Servicio (DoS) y Desincronización:** El protocolo 5G-AKA también ha mostrado vulnerabilidades ante ataques de denegación de servicio y desincronización. Estos ataques pueden explotar la gestión de números de secuencia o mensajes de error para causar fallos persistentes en la autenticación del usuario.

REFLEXIÓN FINAL

Para garantizar la seguridad y resiliencia de las redes 5G frente a las amenazas emergentes, es esencial que los operadores de redes móviles, proveedores de servicios y organismos reguladores colaboren estrechamente en el desarrollo e implementación de medidas de seguridad integrales. En España, este compromiso se ha materializado con la aprobación del Esquema Nacional de Seguridad de redes y servicios 5G (ENS 5G), mediante el Real Decreto 443/2024, de 30 de abril.

El ENS 5G establece un marco normativo específico para abordar los riesgos asociados a la tecnología 5G, considerando las aportaciones de cada agente de la cadena de valor. Sus objetivos incluyen reforzar la protección de la seguridad nacional, garantizar un funcionamiento continuado y seguro de las redes y servicios 5G, y promover un mercado de suministradores diversificado para evitar la dependencia de proveedores de alto riesgo.

Además, el esquema contempla la creación de un Centro de Operaciones de Seguridad 5G de referencia, dependiente del Ministerio para la Transformación Digital y de la Función Pública, encargado de apoyar en la prevención, protección, detección y respuesta frente a amenazas, incidentes y ciberataques en las redes y servicios 5G. Este centro contribuirá a la certificación y normalización de los sistemas, fortaleciendo así la ciberseguridad en el ecosistema 5G nacional.

Asegurar las redes 5G implica ir más allá de las medidas tradicionales: exige el diseño de arquitecturas seguras por defecto, la actualización continua de los protocolos, la cooperación y la capacidad de respuesta ante ciberamenazas complejas y persistentes.

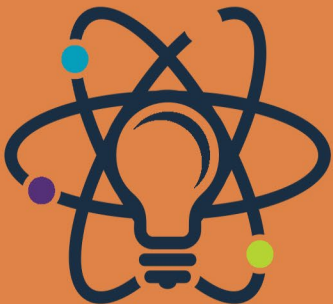
PgM Book

Programme

Management

Body of Knowledge

P4MGO!®



P4MGO!

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



Rediseñando los SOC para una detección más efectiva

La evolución de los Centros de Operaciones de Seguridad (SOC) ha estado marcada por la necesidad de adaptarse a entornos tecnológicos cada vez más complejos y heterogéneos. En este proceso, los equipos de detección y respuesta han centrado gran parte de sus esfuerzos en garantizar que todos los activos, servicios y aplicaciones estén adecuadamente monitorizados. La introducción de soluciones SIEM (Security Information and Event Management) ha permitido, sin duda, escalar la capacidad de ingestión, correlación y almacenamiento de eventos, pero también ha traído consigo un nuevo conjunto de desafíos técnicos que requieren una revisión crítica de la arquitectura operativa tradicional.

Con la incorporación masiva de nuevas fuentes de datos —sistemas cloud, endpoints móviles, redes industriales, aplicaciones SaaS, infraestructuras híbridas—, el volumen de alertas generadas ha crecido de forma exponencial. La capacidad de los SIEM para consolidar esta información en tiempo real es indiscutible, pero los analistas enfrentan ahora una carga cognitiva sin precedentes al tener que revisar, clasificar y responder a alertas en un flujo continuo e implacable.

Este fenómeno, conocido como “alert fatigue” o fatiga por alertas, no es simplemente una cuestión de volumen, sino de calidad. La integración descontrolada de fuentes sin una estrategia de priorización y filtrado provoca que muchas de las alertas generadas carezcan de fidelidad o relevancia. En consecuencia, los analistas se ven obligados a invertir su tiempo en investigar eventos que no representan una amenaza real, lo que no solo retrasa la detección de incidentes

genuinos, sino que además erosiona la moral del equipo y su eficacia operativa. Los SOC más maduros abordan esta situación adoptando un enfoque iterativo y disciplinado: desarrollan un ciclo de vida de la detección de amenazas que incluye la revisión periódica de reglas de correlación, el ajuste fino de umbrales de alerta y la desactivación de aquellas fuentes que aportan más ruido que valor. Sin embargo, en muchas organizaciones, este proceso de afinado se realiza de forma reactiva —y no proactiva—, una práctica que no escala y que limita severamente la capacidad de respuesta del centro.

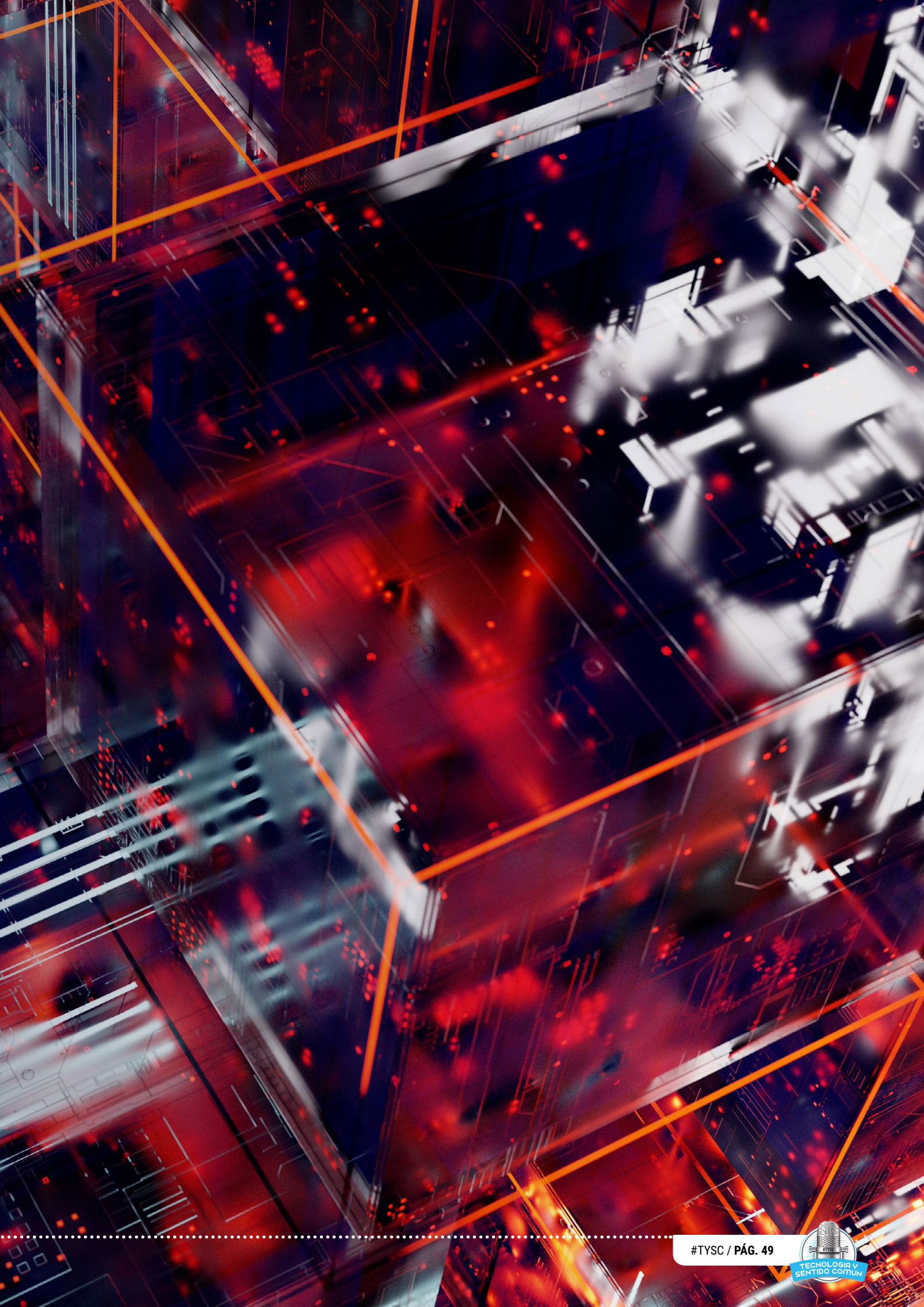
AUTOMATIZACIÓN: EL FALSO SALVAVIDAS DE LA CIBERSEGURIDAD MODERNA

En los últimos años, la automatización ha sido promovida como la solución definitiva a los problemas de eficiencia y escalabilidad de los SOC. Herramientas de orquestación y respuesta automática (SOAR) permiten crear flujos de trabajo predefinidos que replican decisiones y acciones habituales en la investigación de incidentes. Sin embargo, aunque estos sistemas pueden reducir drásticamente los tiempos de respuesta en determinadas tareas repetitivas, su implementación no está exenta de limitaciones operativas y riesgos estratégicos.

Una de las principales falacias alrededor de la automatización es asumir que cualquier proceso puede ser automatizado con el mismo grado de fiabilidad.



**CONTINÚA EN
PRÓXIMA PÁGINA**





En la práctica, la investigación de una alerta requiere del acceso a información contextual rica y actualizada. Sin un motor que proporcione este contexto en tiempo real —incluyendo relaciones entre usuarios, dispositivos, ubicaciones, horarios, hábitos de uso, cambios recientes en la infraestructura—, el valor de la automatización se diluye y puede incluso introducir errores en el análisis.

En muchas ocasiones, los playbooks automatizados únicamente replican la lógica de decisión de una persona, pero carecen de la flexibilidad para adaptarse a casos no previstos o a desviaciones sutiles en los patrones de comportamiento.

Además, la implementación de sistemas SOAR requiere de una inversión significativa en tiempo y recursos para diseñar, probar y mantener los flujos de trabajo. A esto se suma la necesidad de disponer de APIs funcionales y bien documentadas en los sistemas de origen y destino. La ausencia de estándares abiertos o la escasa integración entre plataformas puede frenar el despliegue de automatizaciones eficaces y generar cuellos de botella en el SOC.

Por tanto, aunque la automatización puede reducir tiempos de triaje y mitigar la fatiga de alertas, no puede considerarse una solución completa si no se articula sobre una base sólida de gestión, donde existan procesos y procedimientos bien definidos.

EL CONTEXTO COMO VARIABLE CRÍTICA

Supongamos que un analista recibe una alerta que indica que el usuario user@dominio.tld ha iniciado sesión desde una IP inusual, geolocalizada en un país sin relación aparente con la actividad del usuario. En este escenario, el primer impulso puede ser considerar la alerta como sospechosa, pero sin información contextual suficiente, la investigación no podrá avanzar con solidez.

El analista necesitará responder a una serie de preguntas antes de escalar el incidente o descartarlo. ¿Ha iniciado sesión ese usuario desde otras ubicaciones previamente no habituales? ¿Qué dispositivos tiene asignados? ¿Ha habido cambios recientes en la red corporativa? ¿Existen registros de tickets de soporte relacionados con ese usuario en los últimos días? ¿Hay registros de actividad en otras herramientas corporativas que puedan correlacionar esa IP con un uso legítimo?

Estas preguntas, lejos de ser retóricas, configuran el núcleo de cualquier análisis efectivo. La calidad de las decisiones que tome el analista dependerá directamente de la capacidad del SOC para proporcionar respuestas rápidas y precisas a estas preguntas. En ausencia de esta información, cualquier decisión —ya sea una escalada, una cuarentena o una desestimación— estará basada en intuiciones o suposiciones, lo cual introduce un riesgo inaceptable en operaciones críticas.

Aquí es donde muchos SOCs fracasan: disponen de herramientas potentes de ingesta de datos, pero no cuentan con una arquitectura de datos que permita modelar relaciones, generar grafos de actividad o visualizar patrones históricos. El concepto de “data fabric” aún no está

maduro en muchos entornos de seguridad, y sin esa capa de abstracción semántica es prácticamente imposible contextualizar los eventos en tiempo real.

REDISEÑANDO LA ARQUITECTURA DEL SOC CON UN ENFOQUE CENTRADO EN DATOS

El primer paso para construir un SOC eficiente no es automatizar, sino definir una arquitectura centrada en el dato. Esta arquitectura debe permitir el acceso en tiempo real a información contextual rica, normalizada y modelada. Para ello, es necesario establecer una capa intermedia que actúe como broker semántico entre las distintas fuentes de datos y los consumidores de información (analistas, SIEM, SOAR, herramientas de threat hunting).

Esta capa debe incorporar capacidades de correlación avanzada, modelos de scoring adaptativos y visualizaciones interactivas. Ya no se trata únicamente de almacenar logs, sino de dotarlos de significado. En este contexto, el uso de motores de grafos (como Neo4j o TigerGraph) permite construir relaciones explícitas entre usuarios, dispositivos, ubicaciones y eventos. Esto facilita el análisis de amenazas complejas y reduce drásticamente el tiempo necesario para identificar movimientos laterales o ataques persistentes.

HAY QUE EVOLUCIONAR, PASAMOS DE SOCS REACTIVOS A CENTROS DE INTELIGENCIA

El camino hacia un SOC verdaderamente eficaz no está en acumular más herramientas ni en disparar respuestas automáticas ante cada evento sospechoso. Está en transformar el modelo operativo para que cada alerta, cada evento y cada dato contribuya a construir una imagen clara y coherente del entorno. Para ello, necesitamos integrar el contexto como variable operativa, rediseñar las arquitecturas de datos, fomentar la automatización basada en conocimiento y empoderar a los analistas con herramientas que les liberen del ruido y les conecten con la inteligencia. Ni siquiera la IA a corto plazo, será capaz de sustituir a nuestros mejores analistas.

El futuro del SOC no es reactivo, es proactivo. Un SOC que detecta, sí, pero que sobre todo comprende, predice y decide. Y para lograrlo, no basta con tecnología: hace falta un nuevo modelo mental.

Y hasta aquí llegamos por esta temporada. Gracias por haber estado al otro lado, leyendo, compartiendo y formando parte de este viaje. En septiembre volvemos con las pilas cargadas, más contenidos sobre tecnología, radiocomunicaciones y alguna que otra sorpresa que estamos preparando para seguir mejorando. Así que no te despistes mucho este verano... ¡nos vemos a la vuelta!

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



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



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

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

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

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



CONTINÚA EN
PRÓXIMA PÁGINA

Suscríbete gratis

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

Stakeholders .news

PORTFOLIO, PROGRAMAS Y PROYECTOS MANAGEMENT

NÚMERO 11 DICIEMBRE 2022

PROTAGONISTA DEL MES

MARC
HUGHMANS

FONDOS, ESTOS LÓBOS

PRENDIDAS

REGULARES

U

VER EN CUENTA

NO

V DIGITAL

ACIÓN

PRECIO PARA

USD 11.000

PROYECTOS . GESTIÓN . EXCELENCIA . CALIDAD . PROFESIONALES

Even
CIER
Revista
y "Stak

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

Stakeholder

PORTFOLIO, PROGRAMMA

NÚMERO #011

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

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

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



CONTINÚA EN
PRÓXIMA PÁGINA

CIÓN DE PORFOLIOS, PROGRAMAS Y PROYECTOS

holders

.news

AGEMENT

CONISTA DEL MES

MARC
BERGHMANS

NDOS, ESTOS LODOS

APRENDIDAS

INGULARES
ega

NER EN CUENTA

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

años, de 1470 a 1484

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

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

de ago

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



CONTINÚA EN
PRÓXIMA PÁGINA

STA

logía & Común



REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

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

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

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

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



CONTINÚA EN
PRÓXIMA PÁGINA



TECNOLOGÍA Y SENTIDO COMÚN

12:15 a 13:00

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

Susíbete gratis

REVISTA

Tecnología & Sentido Común

2022

PREMIOS SAPIENS



REVISTA

Tecnología & Sentido Común

<https://tecnologiaysentidocomun.com>

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

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

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

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



CONTINÚA EN
PRÓXIMA PÁGINA



MESA REDONDA
moderada por Javier Pérez



LUIS
MORÁN

Sección:
Personas Y
Procesos



#TYSC / PÁG. 60

Sharing

13:00 a 13:30

DA "STAKEHOLDERS.NEWS"

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



Suscríbete gratis

REVISTA

Tecnología & Sentido Común

#10

2022 PREMIOS SAPIENS

Llanos Cuenca
NUESTRA INVESTIGACIÓN A FUTURO

Talento y Liderazgo
FERNANDO RIOSA

Es tend...

Alejandro Blasco
CONEXIÓN

La nueva Administración
VÍCTOR ALBARRACÍN

Por Procesos
MADELINE CASTRO

Consejo de amigo
JOSÉ LUIS PUENTES

72+

CONSEJO DE AMIGO

REVISTA

TECNOLOGÍA & SENTIDO COMÚN

REVISTA

Tecnología & Sentido Común

<https://tecnologiaysentidocomun.com>



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

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

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



CONTINÚA EN
PRÓXIMA PÁGINA

Suscríbete gratis

DIRECCIÓN Y GESTIÓN DE PORFOLIOS, PROGRAMAS Y PROYECTOS

Stakeholders .news

PROGRAMME & PROJECT MANAGEMENT

NOVIEMBRE #011 - NOVIEMBRE 2022

STAKEHOLDERS.NEWS

PROTAGONISTA DEL MES

MARC BERGHMANS

DE AQUELLOS FONDOS, ESTOS LOGROS
en EDITORIAL
con Javier Paris

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

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

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

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

LAS PMOS EN EL METAVERSO
en SUPER PMOS
con Ricardo Sastre

CONTRATOS ÁGILES
en TRANSFORMACIÓN ÁGIL
con Ángela Plaza

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

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

ENFOCARSE EN EL BIEN SER DE LA
PERSONA: UNA DIMENSIÓN MÁS
HUMANA DENTRO DE LA DIRECCIÓN
de PROYECTOS
en CENTROAMÉRICA
con Estuardo Castañeda



#TYSC / PÁG. 62

13:30 a 13:45

NUEVOS COLABORADORES



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



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



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



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





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

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

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



**CONTINÚA EN
PRÓXIMA PÁGINA**

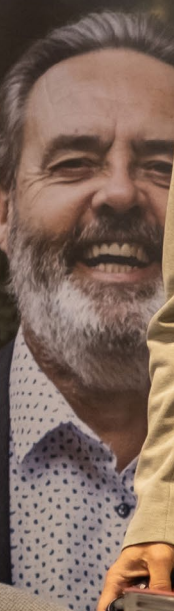
Suscríbete gratis

REVISTA MENSUAL DE DIRECCIÓN Y GESTIÓN DE PORTFOLIOS
Stakeholders

PORTFOLIO, PROGRAMME & PROJECT

NÚMERO #011 - NOVIEMBRE

PROYECTOS · GESTIÓN · EXCELENCIA · CALIDAD · PROFESIONALES



ENTREGA DE PREMIOS

PREMIO REVISTA

**Tecnología &
Sentido Común**
20

REVISTA
**Tecnología &
Sentido Común**

<https://tecnologiaysentidocomun.com>

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

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

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

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



**Curso de
Certificación en:**

Gobierno Corporativo

**ISO 37000
Corporate
Governance
Leader**

Dirección Académica:
Javier Peris

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

MidMgmt®

MPPM®

MGEIT®

eGob®

Tutorías en Directo

Solicita tu admisión en:



+ 34 96 109 44 44

admisiones@escueladegobierno.es

<https://escueladegobierno.es>

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

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

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

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

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

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

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

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

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



CONTINÚA EN
PRÓXIMA PÁGINA

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

Los tres objetivos estratégicos son:

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

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

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

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

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

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

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



**Hace mucho
tiempo que
hablas.**

**¿Pero hace
cuánto no
dialogas?**



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

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

NUEVOS MASTERS



TITULACIÓN MasterGEIT®

CONTENIDO DEL MASTER

Módulo 01: Gestión del Tiempo
Curso de Doble Certificación TSG4® Yellow Belt + TSG4® Green Belt

Módulo 02: Gestión de Procesos de Negocio
Curso de Doble Certificación BPM Executive + ISO 19510 Leader

Módulo 03: Dirección y Gestión de Proyectos
Curso de Doble Certificación OpenPM® (PgM) Executive + ISO 21502 Leader

Módulo 04: Dirección y Gestión de Programas
Curso de Doble Certificación OpenPM® (PgM) Executive + ISO 21503 Leader

Módulo 05: Gestión de Servicios de Tecnología
Curso de Doble Certificación FITSM Executive + ISO 2000 Leader

Módulo 06: Gestión de Seguridad de la Información
Curso de Doble Certificación CSX Executive + ISO 27000 Leader

Módulo 07: Gestión de la Continuidad del Negocio
Curso de Doble Certificación CBC Executive + ISO 22301 Leader

Módulo 08: Gobierno de Información y Tecnología
Curso de Doble Certificación COBIT 2019 Executive + ISO 38500 Leader

Módulo 09: Gobierno del Dato
Curso de Doble Certificación DANA Executive + ISO 38505 Leader

Módulo 10: Gobierno Corporativo
Curso de Doble Certificación COSO Executive + ISO 37000 Leader

Los cursos de Doble Certificación se basan en los Programas de la Escuela de Gobierno eGob® y cuentan con la acreditación de la ISO 9001:2015. Los cursos de Doble Certificación se basan en los Programas de la Escuela de Gobierno eGob® y cuentan con la acreditación de la ISO 9001:2015.

MISIÓN

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- ✓ Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- ✓ Cursos de cuatro sesiones en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- ✓ Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- ✓ Cursos de Doble Certificación convalidables por asignaturas del Master en Gobierno, Dirección, Gestión y Ejecución de Portfolios, Programas y Proyectos MasterPPM®.



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

MISIÓN

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- ✓ Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- ✓ Cursos de cuatro sesiones en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- ✓ Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- ✓ Cursos de Doble Certificación convalidables por asignaturas del Master en Gobierno, Dirección, Gestión y Ejecución de Portfolios, Programas y Proyectos MasterPPM®.



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

eGob®

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