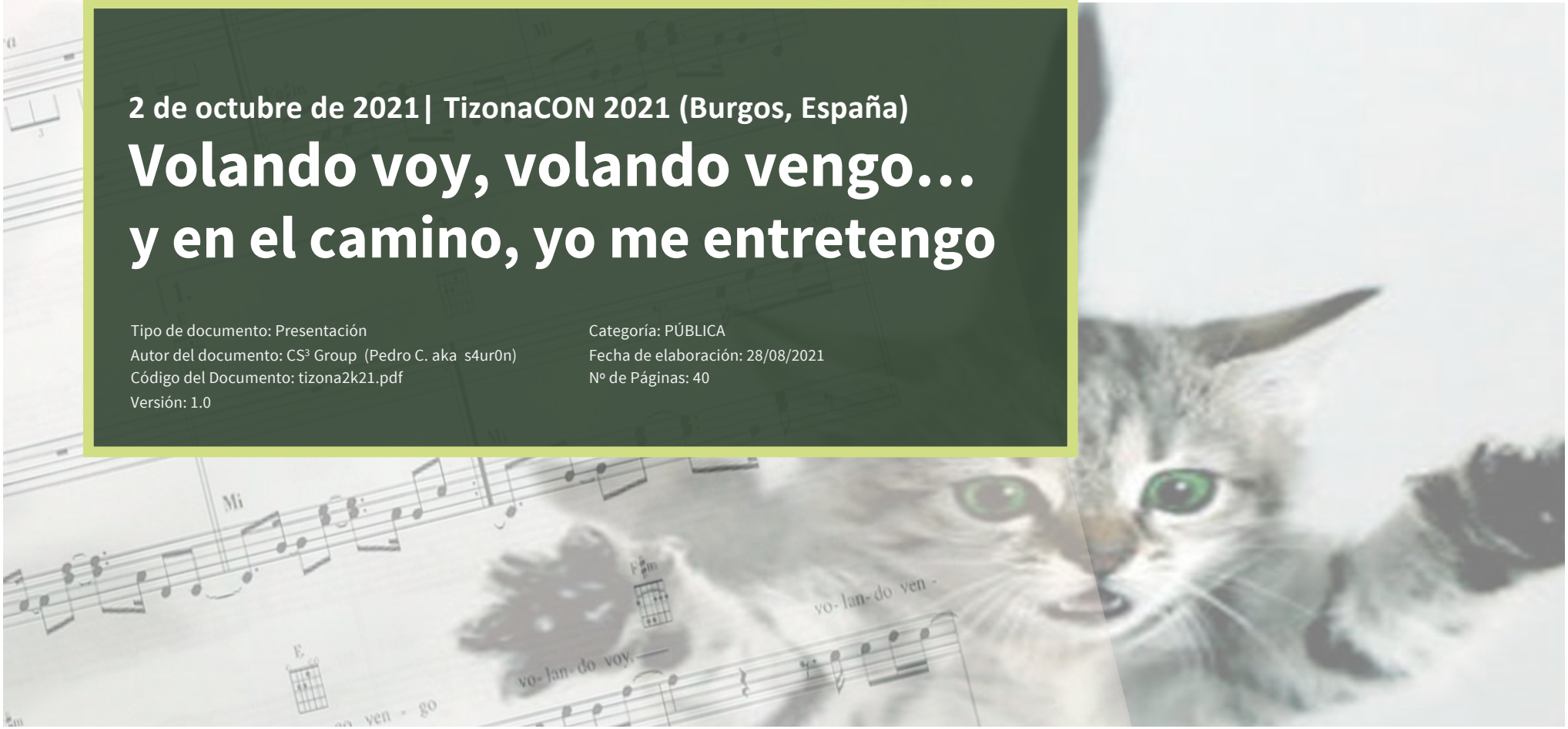
© 2021 CS³ Group – Todos los derechos reservados

2 de octubre de 2021| TizonaCON 2021 (Burgos, España)

Volando voy, volando vengo…
y en el camino, yo me entretengo

Tipo de documento: Presentación
Autor del documento: CS³ Group (Pedro C. aka s4ur0n)
Código del Documento: tizona2k21.pdf
Versión: 1.0

Categoría: PÚBLICA
Fecha de elaboración: 28/08/2021
Nº de Páginas: 40

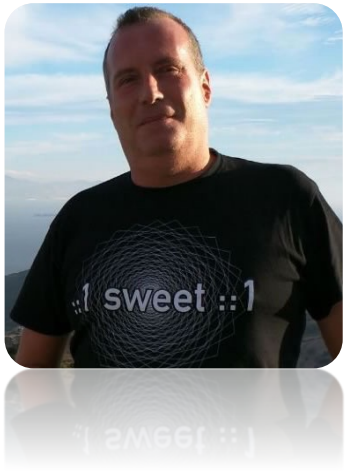


0. Presentación

Para l@s que no me conozcan…

© 2021 CS³ Group – Todos los derechos reservados

whoami




```
class PedroC:
    def __init__(self):
        self.name =      'Pedro Candel'
        self.email =     's4ur0n@s4ur0n.com'
        self.web =       'https://www.s4ur0n.com'
        self.nick =      '@NN2ed_s4ur0n'
        self.company =   'CS³ Group'
        self.role =      'Security Researcher'
        self.work =      [ 'Reversing', 'Malware', 'Offensive
                           Security', '…' ]
        self.groups =    [ 'mlw.re', 'OWASP', 'NetXploit', '...' ]
```

© 2021 CS³ Group – Todos los derechos reservados

¿Qué hacemos y a qué nos dedicamos?

Formación en Seguridad
Cursos presenciales a medida impartidos en las instalaciones del cliente o las concertadas con prácticas reales desde el primer momento

Hacking Ético
Auditorías de caja negra, gris o blanca para aplicaciones web, sistemas y redes de comunicaciones

Análisis de Malware
Análisis de Malware automatizados y manuales con completos informes de comportamiento e indicadores de compromiso (IOC)

Ingeniería Inversa
Ingeniería Inversa para binarios de sistemas Windows de 32/64 bits, GNU/Linux de 32/64 bits, OSX Mach-O de 64 bits, ARM y firmwares

Exploiting
Desarrollo y adaptación de exploits para sistemas Windows de 32/64 bits, GNU/Linux de 32/64 bits, OSX Mach-O de 64 bits y Android

Desarrollo Seguro
Auditoría SAST, DAST, IAST y RASP para análisis de vulnerabilidades en el código de proyectos en Java, .Net, PHP, C/C++ y Cobol

Hardware Hacking
Análisis de vulnerabilidades en dispositivos hardware, sistemas embebidos y firmware con técnicas de ingeniería inversa

Seguridad en dispositivos móviles
Análisis estático, dinámico e instrumentación dinámica de aplicaciones Android (APK), iOS (IPA) y Windows Mobile (APPX)

Respuesta ante incidentes
Investigación remota de incidentes de seguridad, análisis de las situaciones y respuesta inmediata ante las amenazas

Forense
Adquisición y elaboración de informes periciales con garantía de imparcialidad y objetividad para todo tipo de sistemas de información

DevSecOps
Desarrollo, Seguridad y Operaciones en CSI (Continuous Security Integration) con pruebas automatizadas de seguridad para CI/CD

Intelligence
Recopilación, análisis y explotación de datos a gran escala con fuentes OSINT, SIGINT, HUMINT, Deep Web, redes P2P, etc.

SIGINT
Inteligencia de comunicaciones, análisis y auditoría de seguridad en señales y protocolos de radiofrecuencia (RF)

T.S.C.M.
Technical Surveillance Counter-Measures: Contramedidas electrónicas para detección y localización de dispositivos de escucha

Telecom
Análisis y auditoría GSM/3G/4G, implementación de servicios de operadores móviles virtuales (HLR, VLR, GGSN, Roaming voz y datos)

ATM
Análisis de vulnerabilidades, auditoría, forense, skimming, shimming y pruebas de blackbox para NCR, Hyosung, WRG, Diebold Nixdorf e Hitachi

PoS/TPV
Auditoría y cumplimiento de controles en terminales Verifone e Ingenico. Monitorización y transaccionabilidad completa según ISO 8583

LOPD/GPDR/Cumplimiento
LOPD, adaptación GPDR, ISO 27000, SGSI, análisis y gestión de riesgos, Políticas de seguridad, continuidad de negocio, ITIL, PCI DSS

© 2021 CS³ Group – Todos los derechos reservados

¿Y en el tiempo libre?





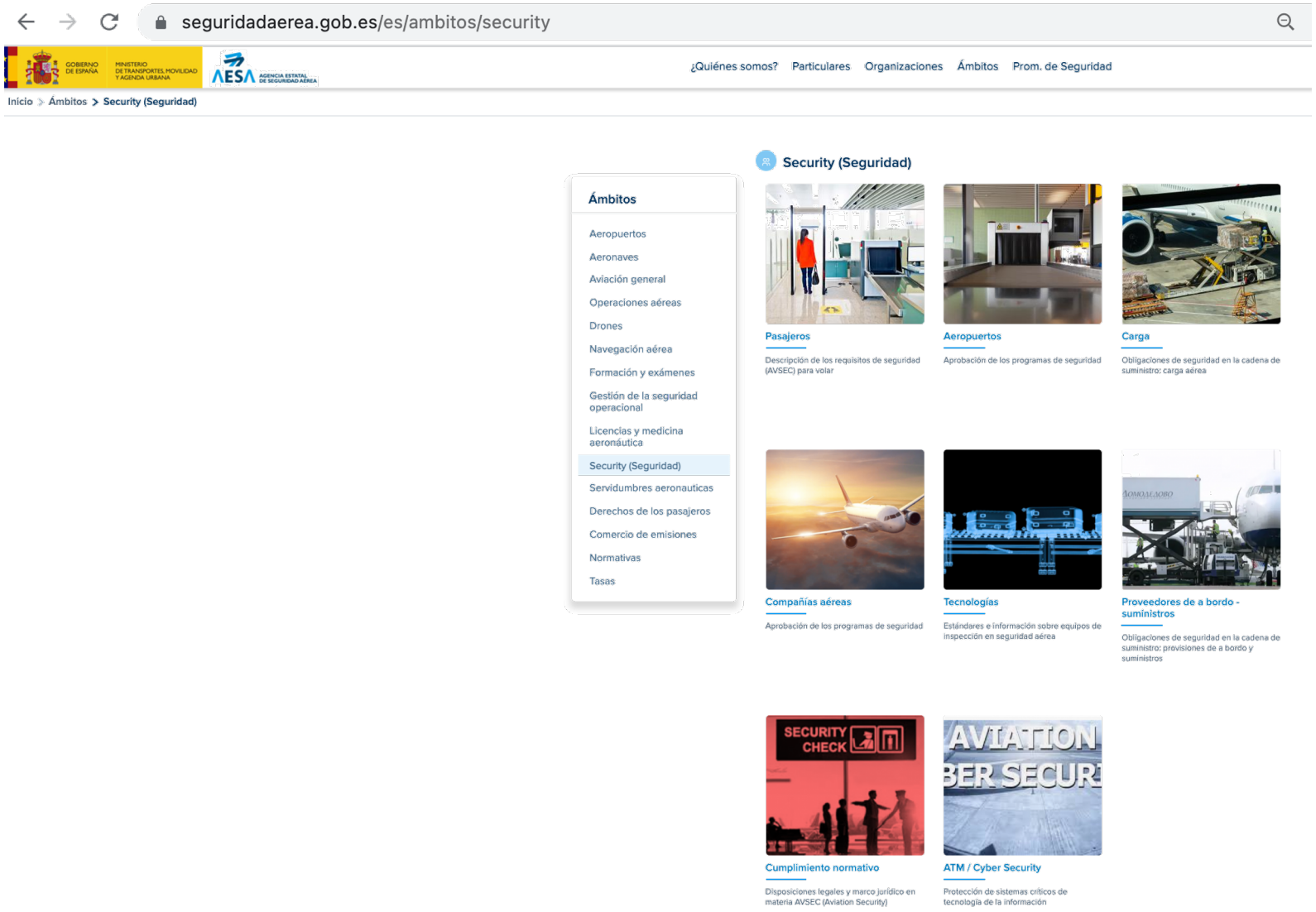
© 2021 CS³ Group – Todos los derechos reservados

1. General

El 101 de los “reguladores”

© 2021 CS³ Group – Todos los derechos reservados

AESA



© 2021 CS³ Group – Todos los derechos reservados

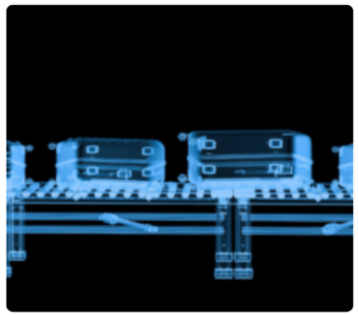
AESA

- Licencias y medicina aeronáutica
- Security (Seguridad)
- Servidumbres aeronauticas
- Derechos de los pasajeros
- Comercio de emisiones
- Normativas
- Tasas



Compañías aéreas

Aprobación de los programas de seguridad



Tecnologías

Estándares e información sobre equipos de inspección en seguridad aérea



Proveedores de a bordo - suministros

Obligaciones de seguridad en la cadena de suministro: provisiones de a bordo y suministros



Cumplimiento normativo

Disposiciones legales y marco jurídico en materia AVSEC (Aviation Security)



ATM / Cyber Security

Protección de sistemas críticos de tecnología de la información

© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



20 JUL
2021

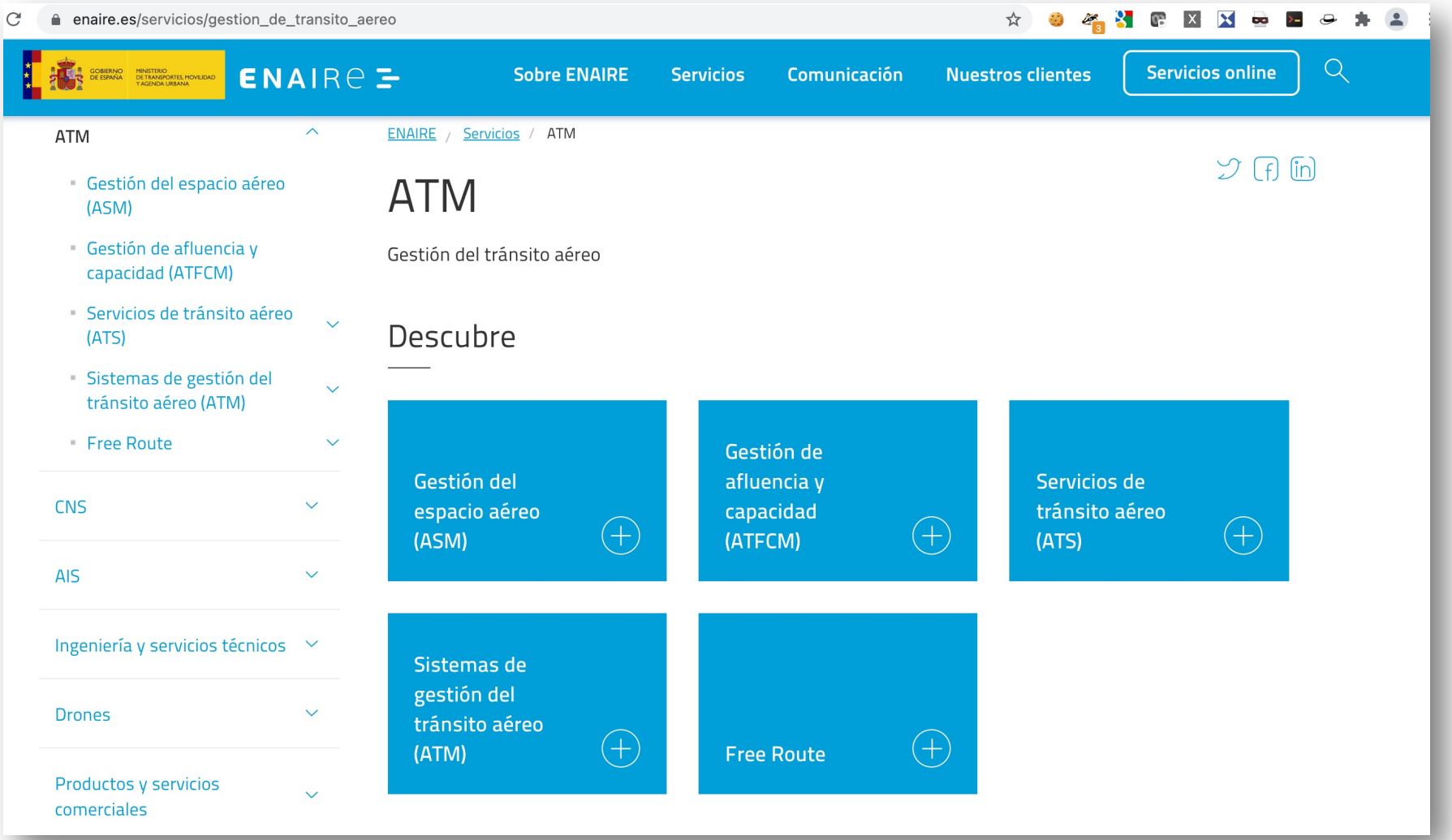
ENAIRE y EASA se reúnen para compartir los proyectos tecnológicos de ENAIRE y potenciar la cooperación entre ambas Organizaciones

ENAIRE y la Agencia Europea de Seguridad Aérea, EASA, han celebrado hoy una reunión bilateral estratégica para compartir los proyectos tecnológicos y de innovación de ENAIRE, como es el desarrollo e implementacion en España del U-space, el concepto europeo para la gestión automatizada de operaciones de drones basado en un conjunto de servicios digitalizados; la iniciativa de la entidad recien constituida por ENAIRE e INDRA, Startical, para la prestación de servicos satelitales de vigilancia ADS-B y comunicaciones VHF y de datos que permitirá niveles de prestación de servicios en las áreas oceanicas y remotas similares al continental basados en el concepto de "nuevo espacio"; la recategorización de la separación por estelas turbulentas (RECAT), entre otros, y potenciar la cooperación entre las dos entidades.

El director ejecutivo de EASA, Patrick Ky, la responsable del programa de drones, María Algar y

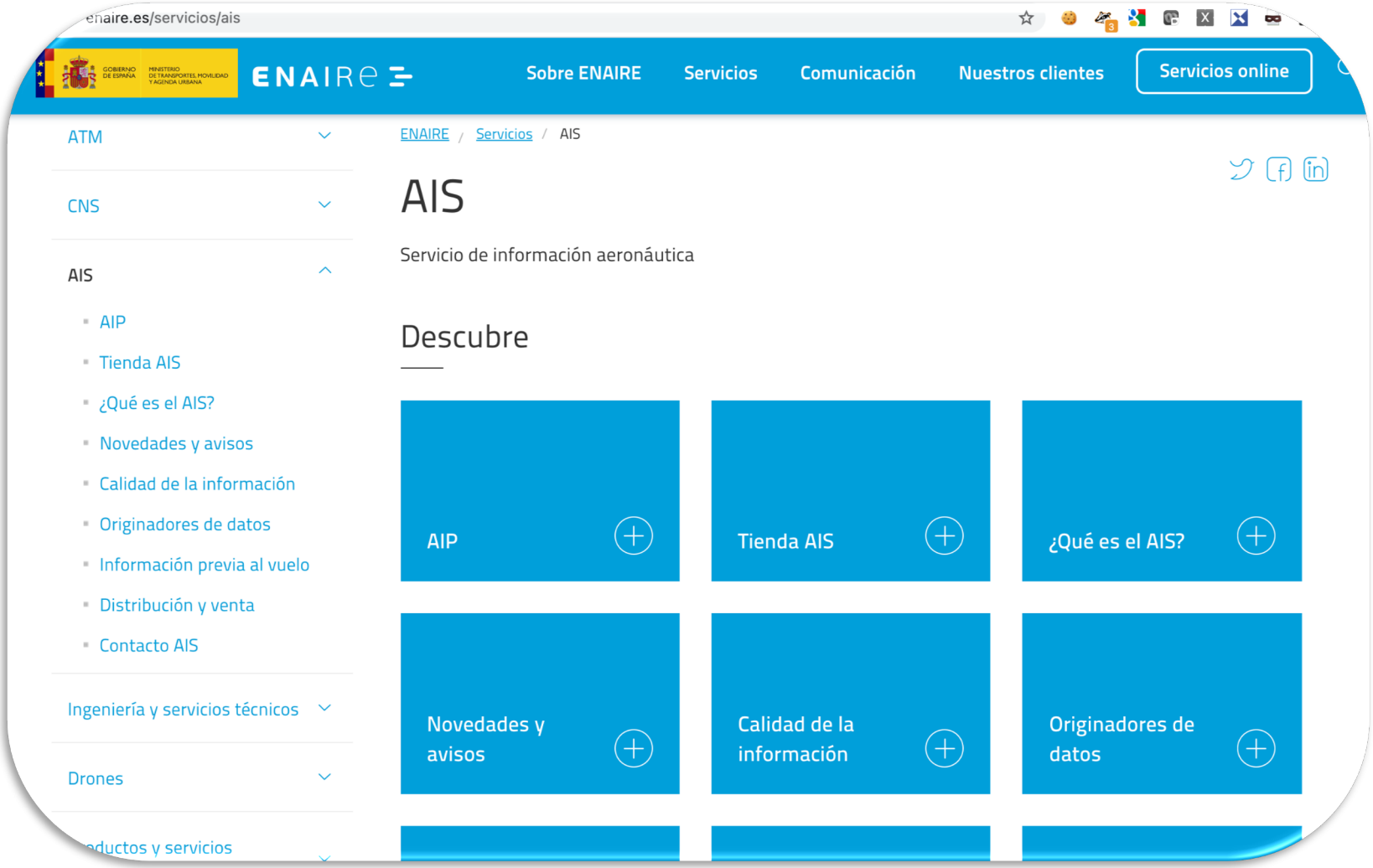
© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



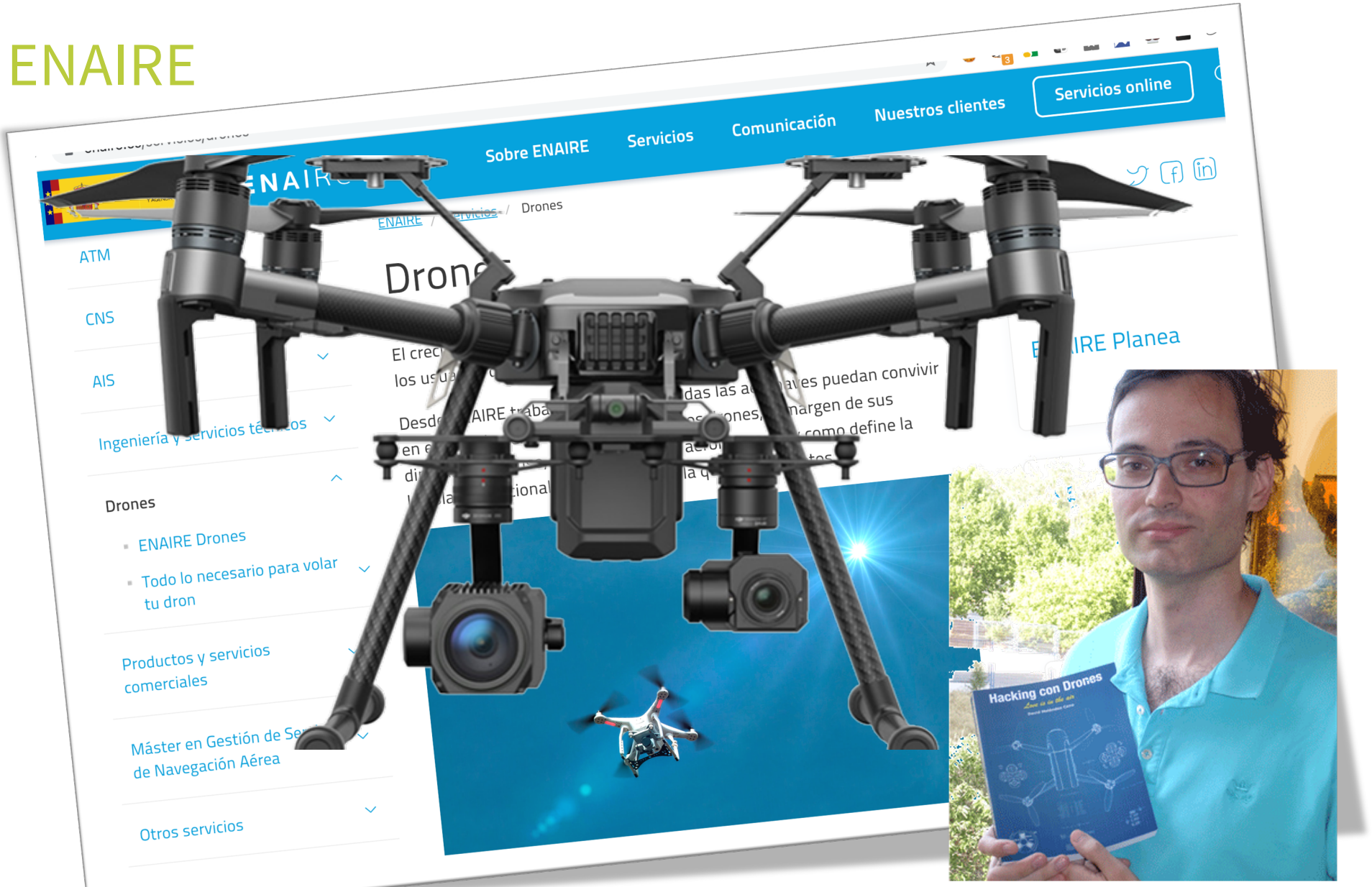
© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



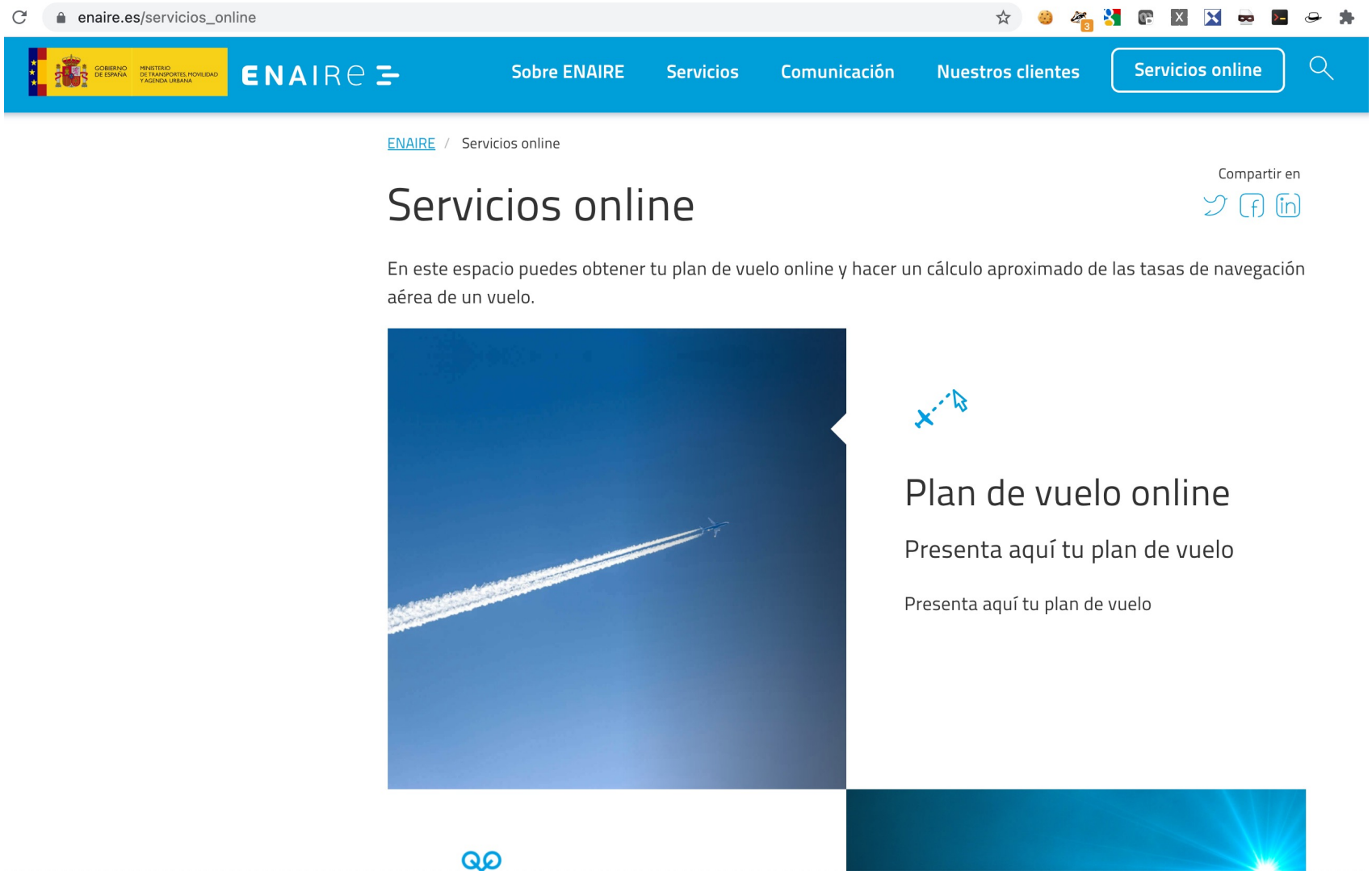
© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



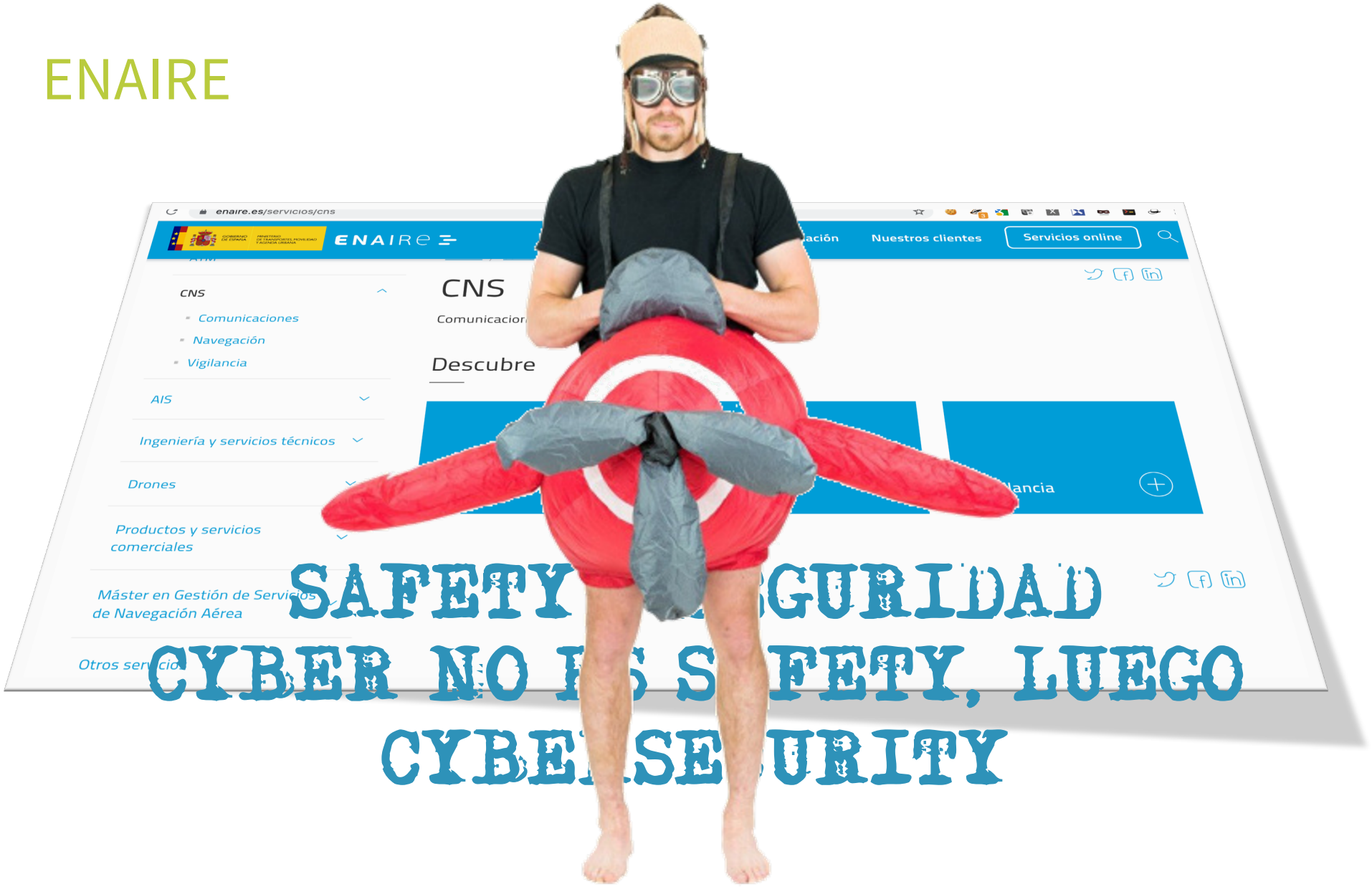
© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



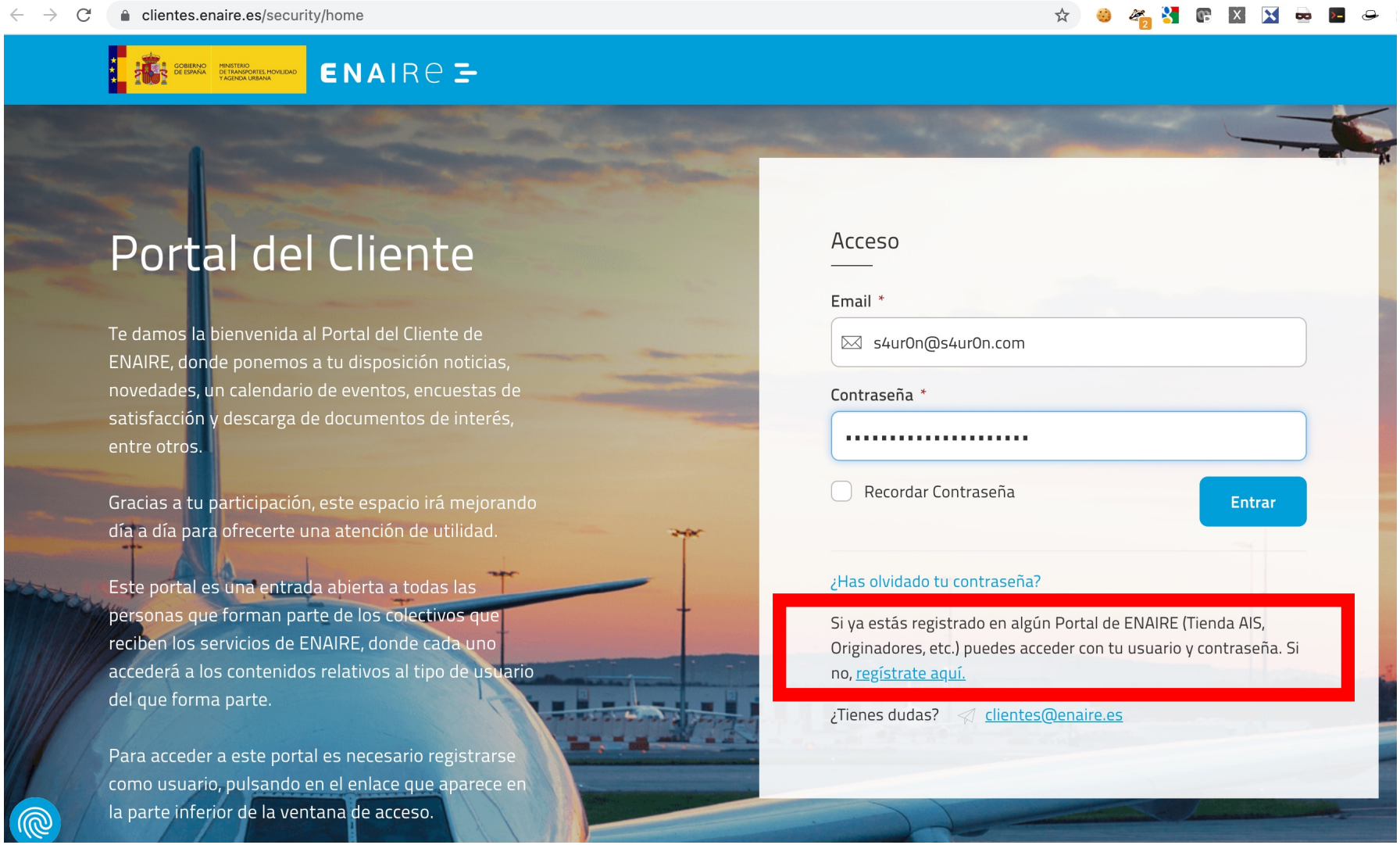
© 2021 CS³ Group – Todos los derechos reservados

2. ¿Volamos o qué?

Si… pero se me olvidó algo…

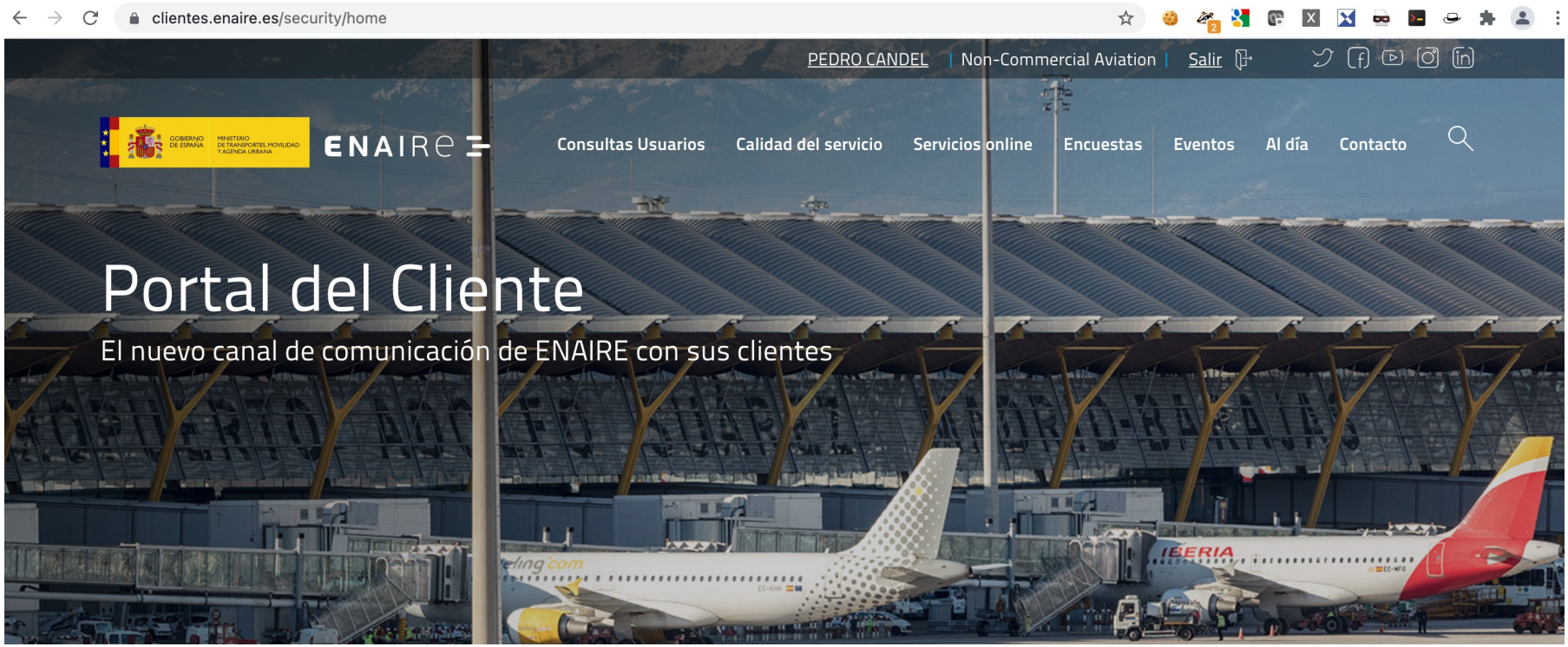
© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



Bienvenido al Portal del Cliente de ENAIRE, que nace con el propósito de facilitar y optimizar la comunicación de ENAIRE con sus clientes.

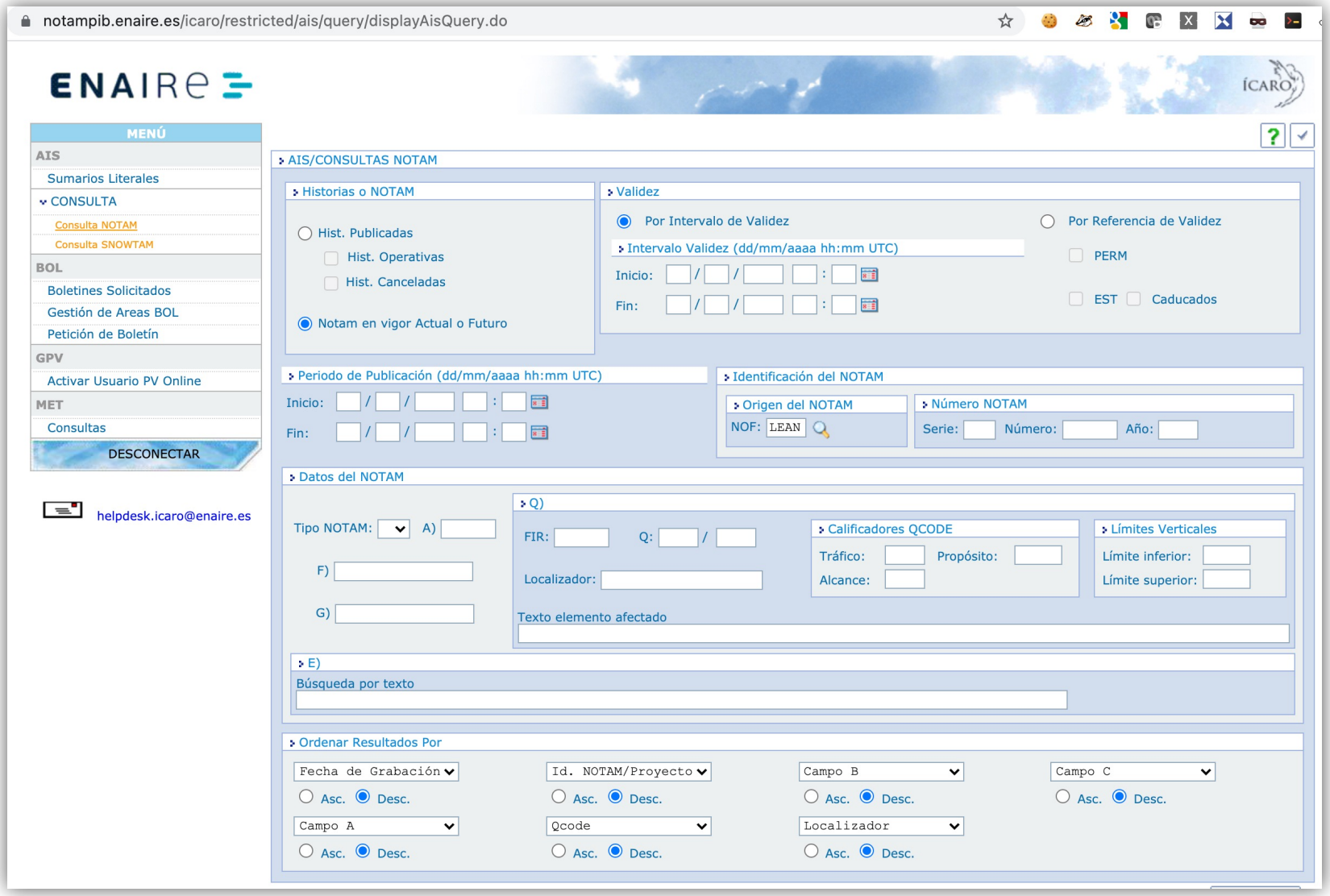
Este portal se ha concebido como un punto de encuentro, de participación, de consulta y de información actualizada y de utilidad para todos los clientes de ENAIRE.

Este portal es una entrada abierta a todas las personas que forman parte de los colectivos que reciben los



© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



© 2021 CS³ Group – Todos los derechos reservados

ENAIRE

GOBIERNO DE ESPAÑA · MINISTERIO DE TRANSPORTES, MOVILIDAD Y AGENDA URBANA · AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

¿Quiénes somos? Particulares Organizaciones Ámbitos Prom. de Seguridad

Inicio > Ámbitos > Aviación general > NOTAM de Aviación General para operar en Espacio Aéreo controlado

Aviación general

- Operaciones no comerciales con aeronaves distintas de las propulsadas complejas NCO
- Aeronaves de estructura ultraligera ULM
- Globos
- Planeadores
- Aeronaves de construcción por aficionados
- Demostraciones aéreas civiles
- Suspensión de limitaciones operacionales
- NOTAM de Aviación General para operar en Espacio Aéreo controlado

NOTAM de Aviación General para operar en Espacio Aéreo controlado

¿Cuándo es necesario solicitar un NOTAM?

Para realización de actividades de Aviación General en espacio aéreo controlado, siempre que:

- Exista información que se tenga que distribuir, de carácter temporal y de corta duración (por ejemplo una vuelta aérea), o
- Se introduzcan con poco tiempo de preaviso cambios permanentes, o temporales de larga duración, que sean de importancia para las operaciones (por ejemplo modificaciones del espacio aéreo), o
- Ante la presencia de peligros para la navegación aérea (comprendidos los obstáculos, maniobras militares, exhibiciones y competiciones, actividades importantes de paracaidismo fuera de emplazamientos promulgados).

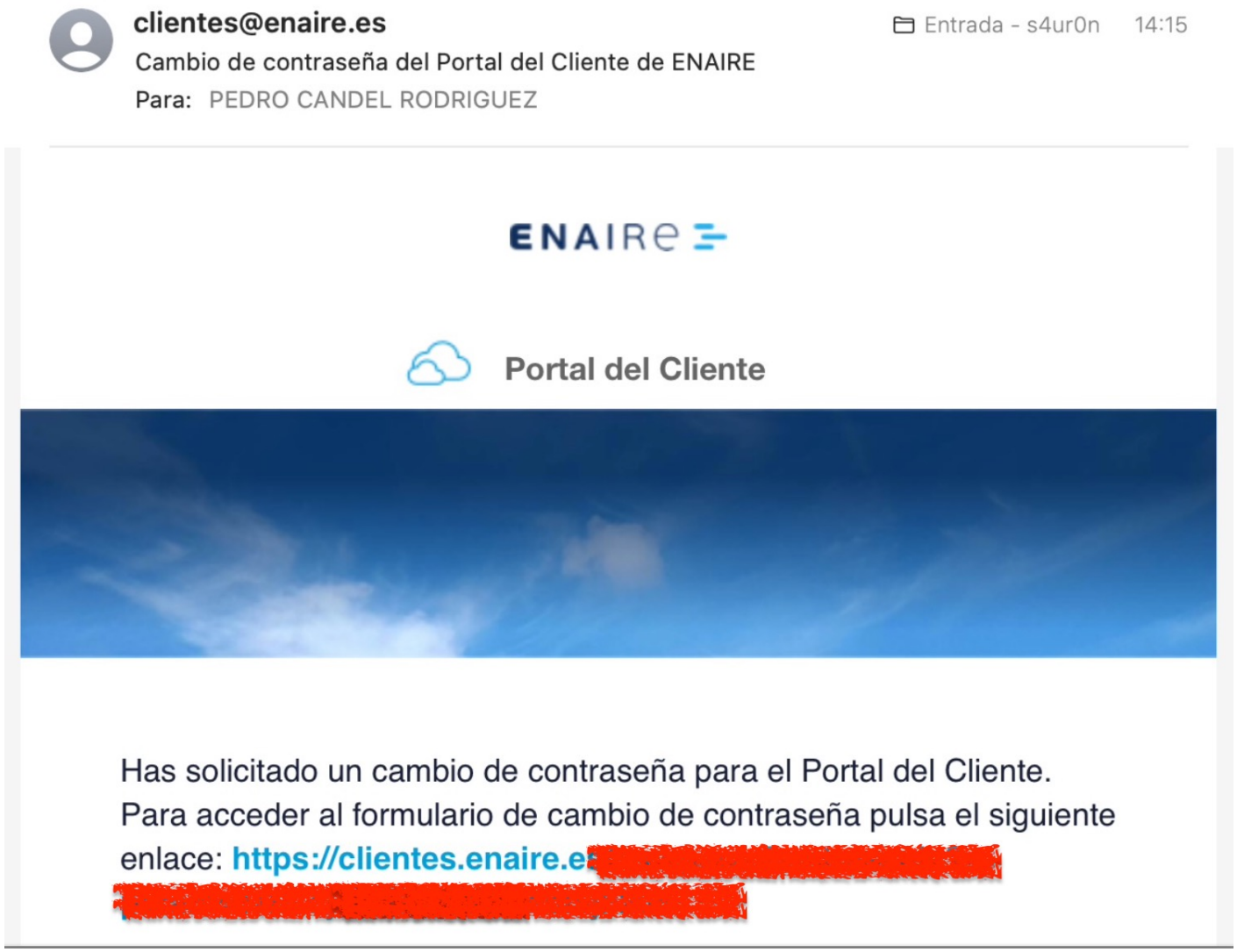
¿Qué actividades de Aviación General deben solicitar un NOTAM?

- Lanzamiento de paracaidistas.*
- Exhibiciones aéreas.
- Vueltas aéreas.
- Competiciones aéreas.

(*) La realización de forma frecuente de actividades de paracaidismo en un mismo emplazamiento requiere el establecimiento de una zona promulgada que se publicará en el apartado ENR 5.5 de la Publicación de información aeronáutica (AIP). Las solicitudes de publicación de NOTAM desde el 1

© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



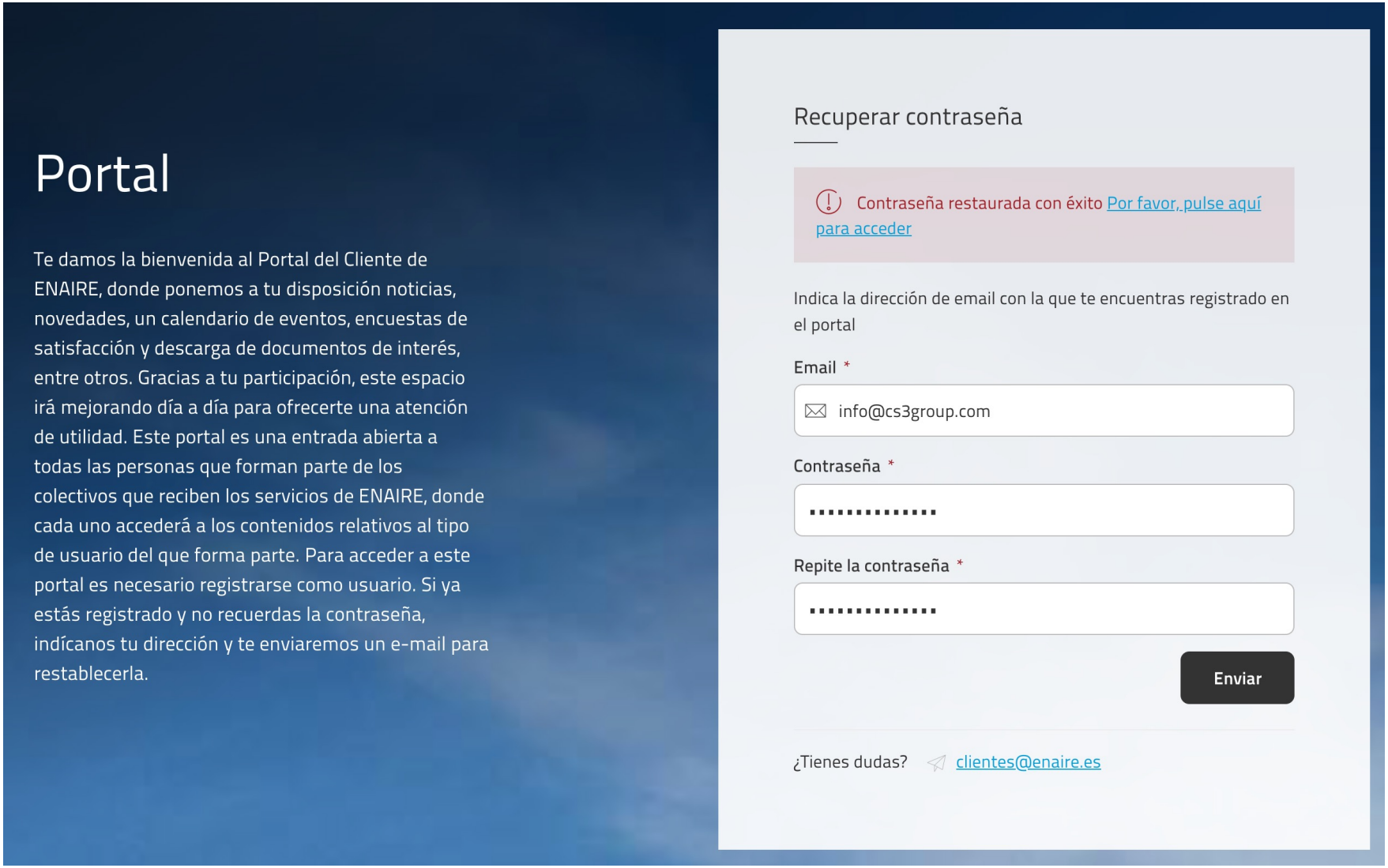
© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



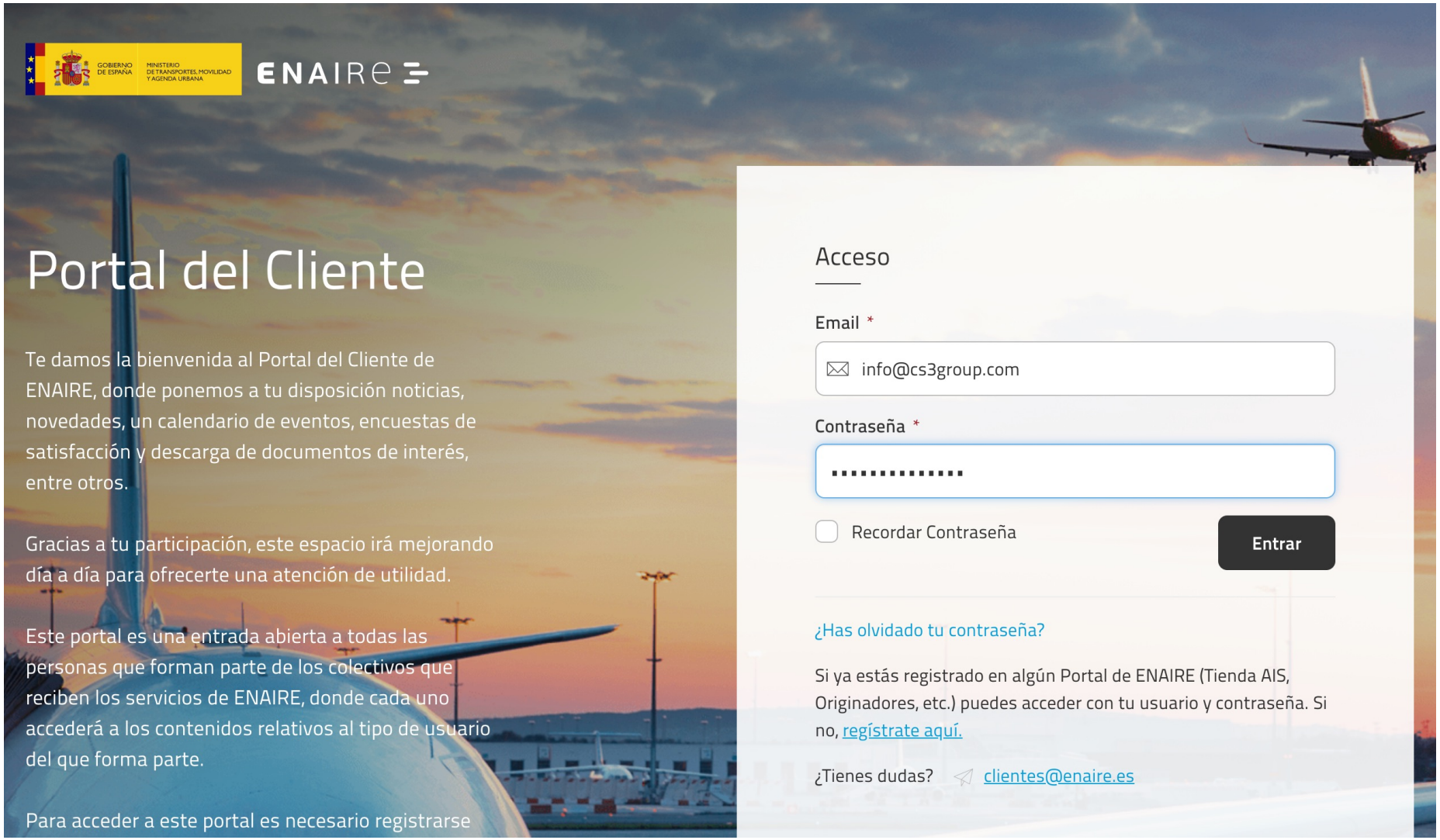
© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



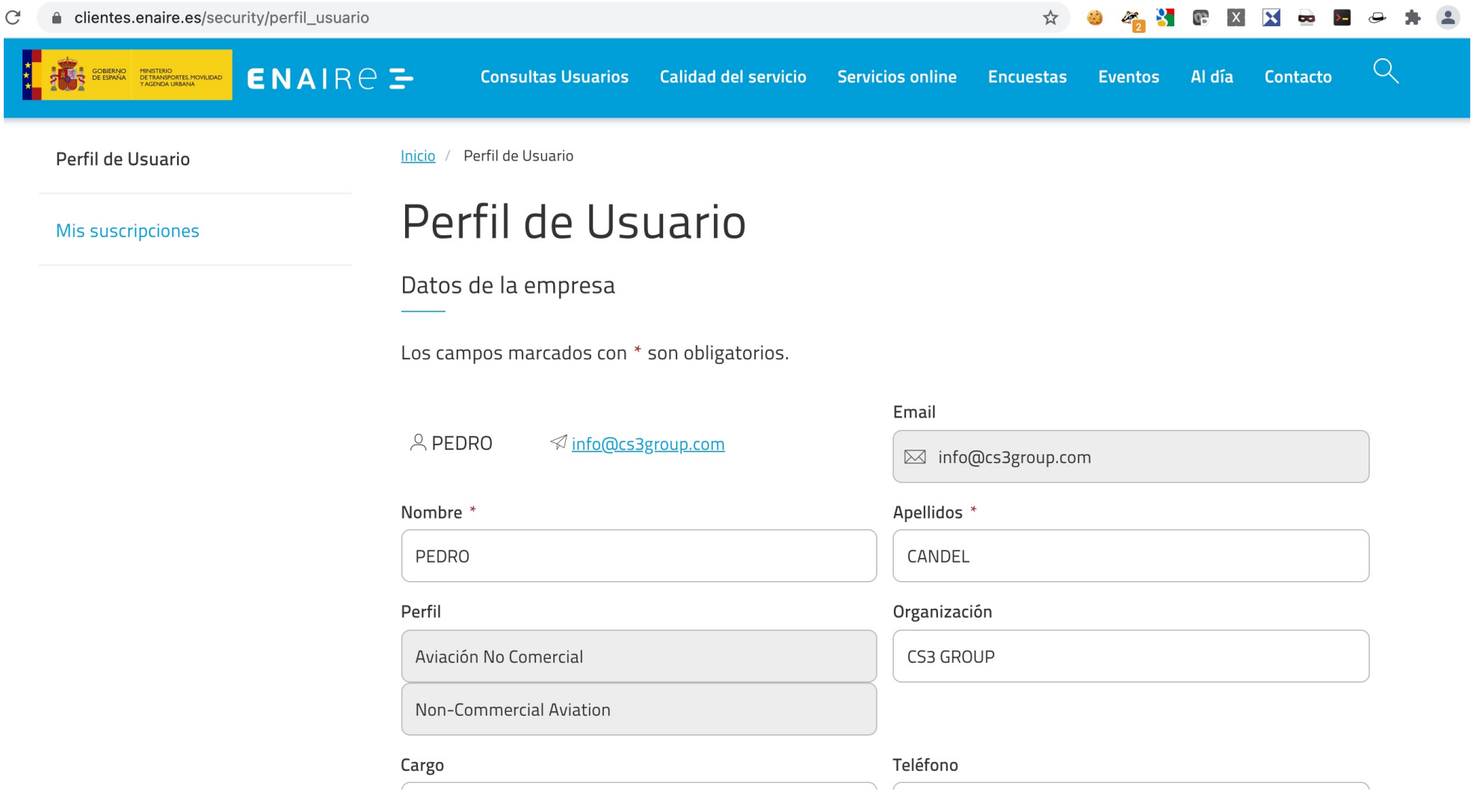
© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



© 2021 CS³ Group – Todos los derechos reservados

ENAIRE







© 2021 CS³ Group – Todos los derechos reservados

3. Vamos a ello…

¿Entramos a las aplicaciones o cambio de password?

© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



© 2021 CS³ Group – Todos los derechos reservados

4. Bonus track

Arreglado… ahora hemos mejorado todo…

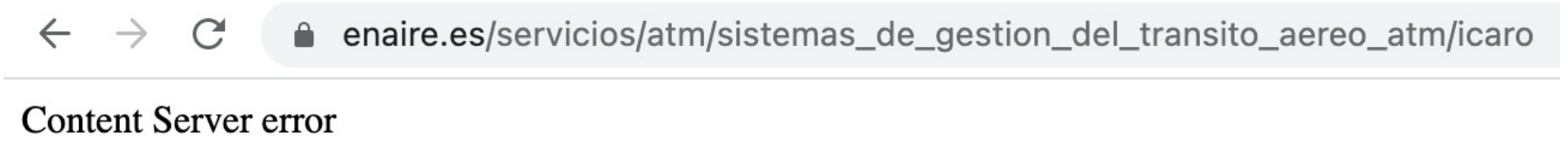
© 2021 CS³ Group – Todos los derechos reservados

ENAIRE

- Muchos portales **con las mismas credenciales** “unificadas”… (todo interconectado y es el **eslabón más débil** de todos).
- Acceso directo **SIN TOKEN** sólo conociendo el email… y el “**parámetro cifrado**” para **restablecer las contraseñas** directamente…
- Simplemente un “**cifrado**” en **Base64** para… ¿Tener acceso a todo?
- Sin recuperación de ninguna pregunta o algo que pueda asegurar si es el interesado el que responde… Al menos que **compruebe que se ha solicitado un reseteo de la contraseña**… entendiendo que ha sido si o si solicitado su cambio.
- ¿Un simple “**error**” del “becario” o una “**feature**”?
- ¿Hay datos personales, PVs, NOTAMs, Tasas, etc…? ¿Afecta a RGPD?
- ¿Se podría modificar el email asociado una vez dentro y que el **piloto o su compañía** no fueran conscientes de algún cambio?
- Algunas dudas me generan…

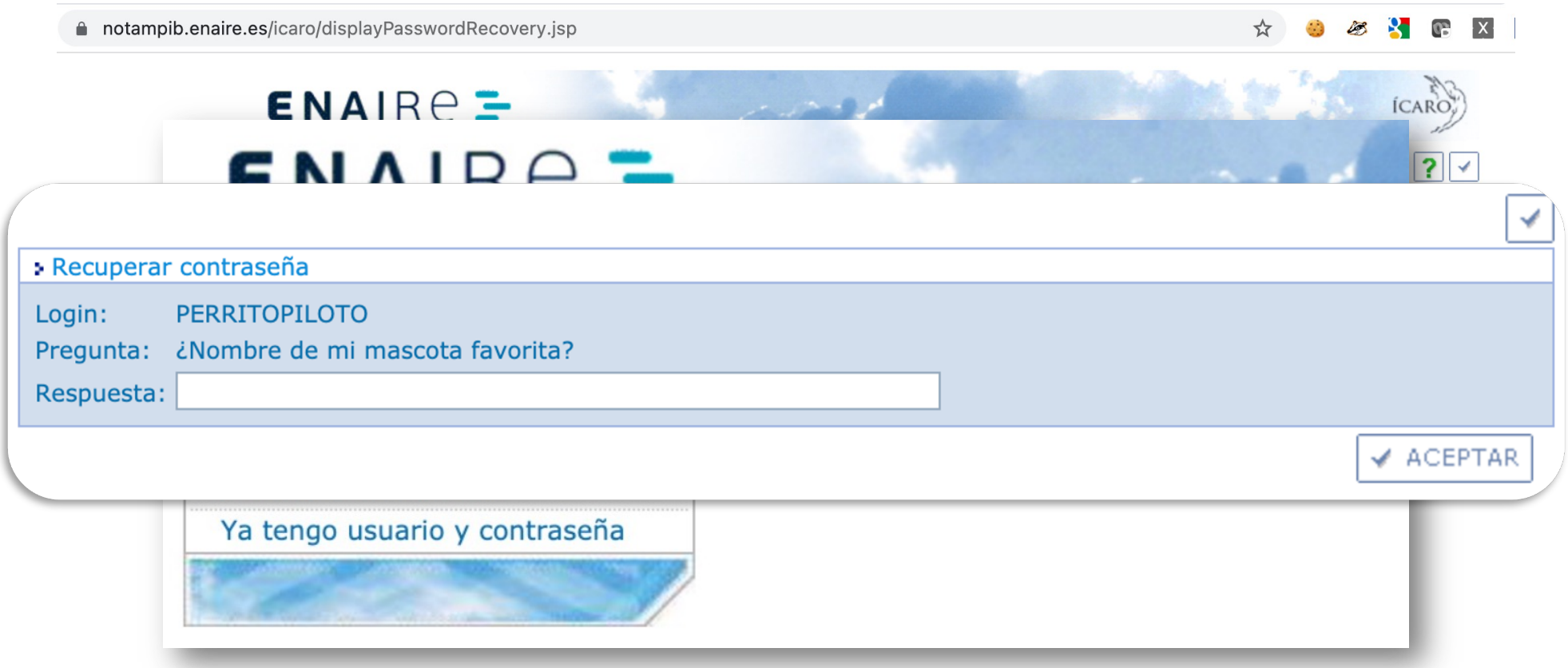
© 2021 CS³ Group – Todos los derechos reservados

Bonus Track



© 2021 CS³ Group – Todos los derechos reservados

Bonus Track



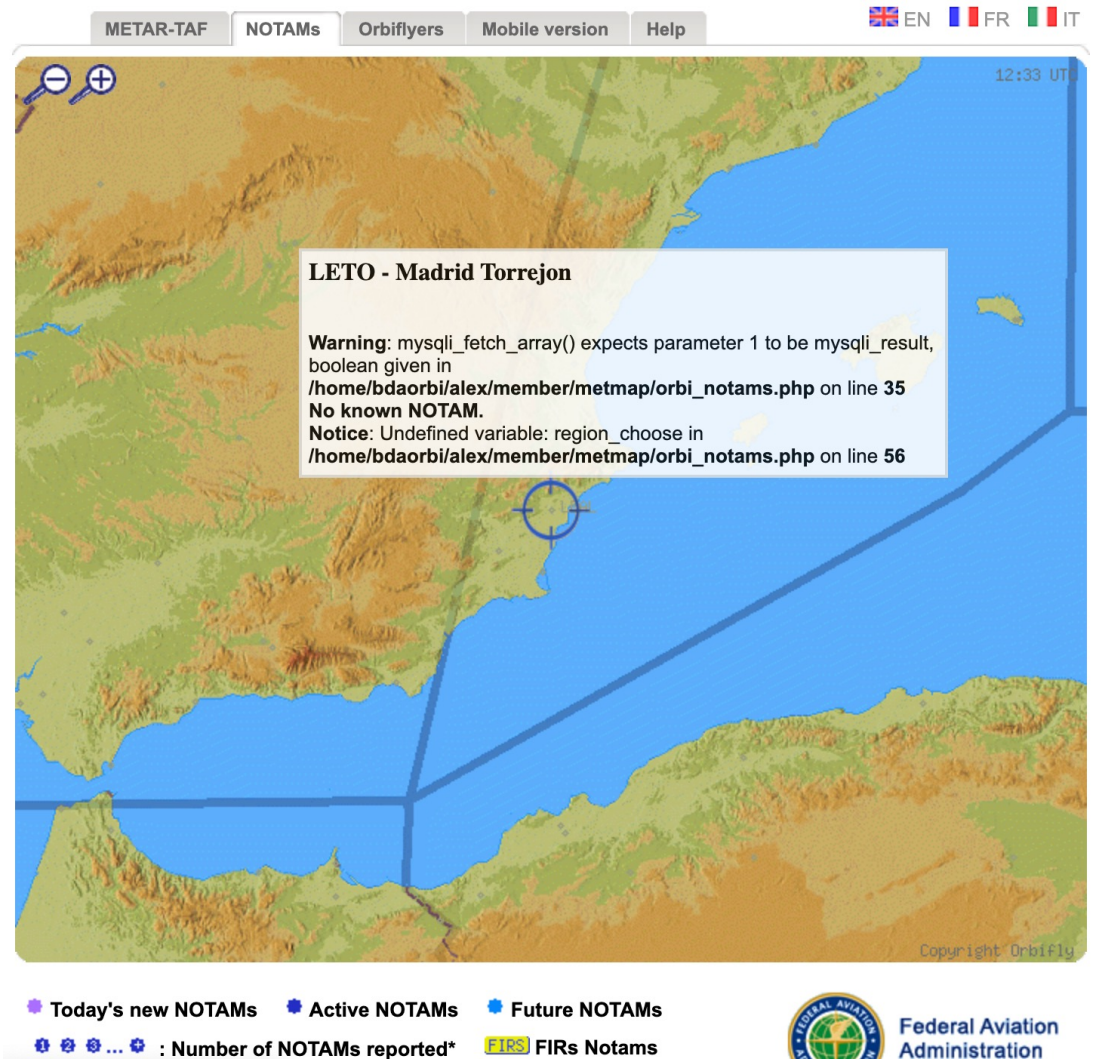
© 2021 CS³ Group – Todos los derechos reservados

ENAIRE



© 2021 CS³ Group – Todos los derechos reservados

Bonus Track (otros están peor)

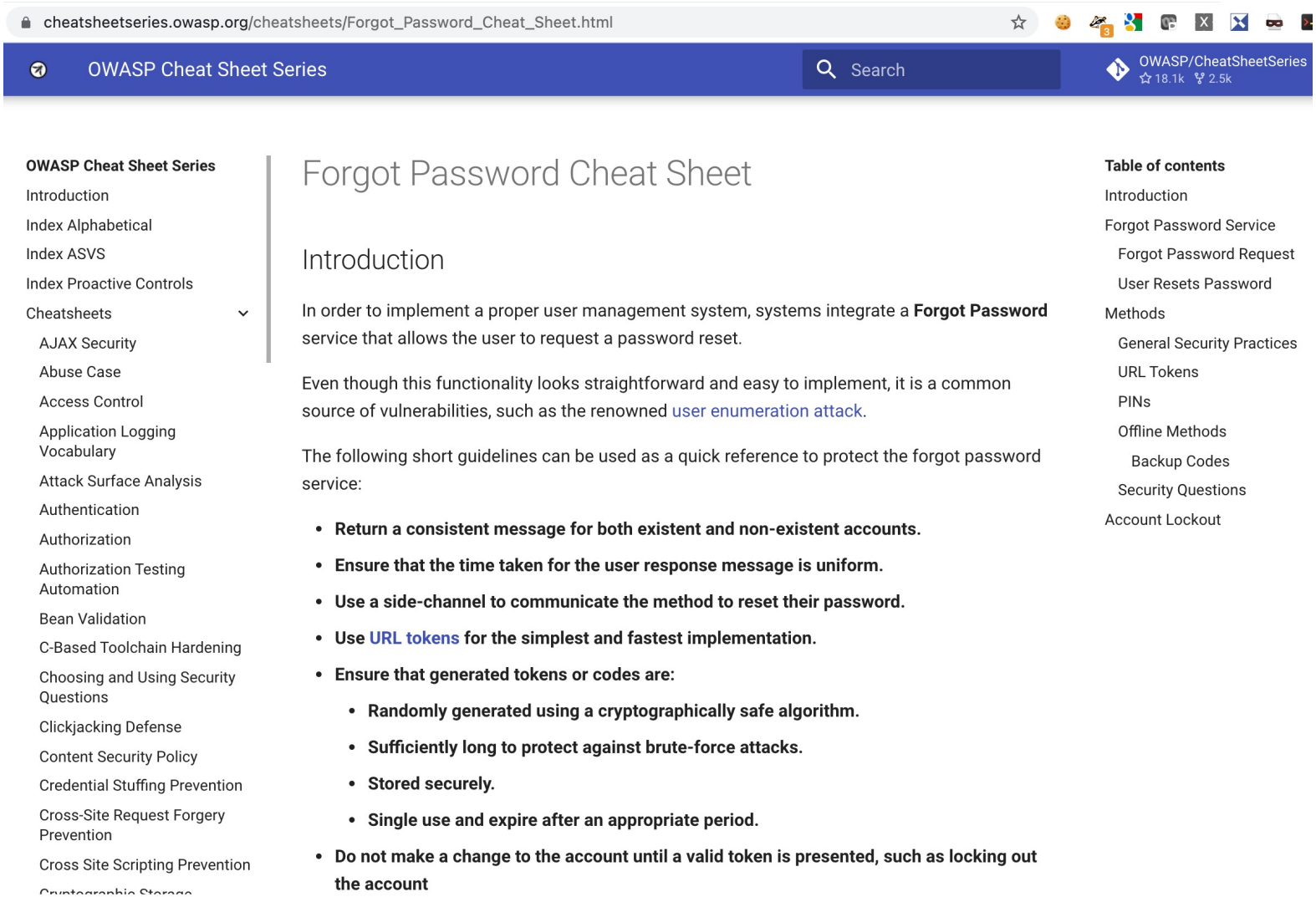


© 2021 CS³ Group – Todos los derechos reservados

5. Soluciones

El único animal que tropieza dos veces en la misma piedra es el ser humano...

© 2021 CS³ Group – Todos los derechos reservados



© 2021 CS³ Group – Todos los derechos reservados

Disclaimer

- Estamos en la **mejores manos y con los/as que nunca salen en las charlas** que nos garantizan ir a donde se quiera y agradecerles el esfuerzo para actualizar todo **con las máximas garantías de SEGURIDAD**. Un aplauso para todos ellos/as y darles las gracias por estar siempre con nosotros!!!



© 2021 CS³ Group – Todos los derechos reservados

¡Muchas gracias!

TIZONA CONF
CONGRESO DE CIBERSEGURIDAD
2021
ONLINE

CS³ SECURITY SERVICES
https://cs3group.com



© 2021 CS³ GROUP. Todos los derechos reservados.

Todas las demás marcas comerciales, productos, servicios, logotipos, imágenes, etc. referenciados aquí son propiedad de sus respectivos dueños. La información presentada es exclusivamente con propósitos informativos y únicamente expresa la opinión del autor en el momento de su publicación. CS³ GROUP no puede garantizar la veracidad y licitud del contenido o información aquí presentada. CS³ GROUP ofrece TODO EL MATERIAL Y EL CONTENIDO DE ESTA PRESENTACION "COMO ESTÁ", SIN NINGUNA GARANTÍA EXPRESA O TÁCITA DE NINGÚN TIPO, INCLUYÉNDOSE SIN LIMITACIÓN LAS GARANTÍAS DE QUE EL PRODUCTO O SERVICIO SEA COMERCIALIZABLE, NO INFRACTORA DE LA PROPIEDAD INTELECTUAL DE NADIE, O IDÓNEA PARA UN DETERMINADO PROPÓSITO. CS³ GROUP NO TIENE NINGUNA OBLIGACIÓN DE PAGAR INDEMNIZACIÓN POR DAÑOS Y PERJUICIOS DE NINGÚN TIPO (INCLUYENDO, ENTRE OTRAS, LA PÉRDIDA DE GANANCIAS, PÉRDIDA DE EXPLOTACIÓN, PÉRDIDA DE INFORMACIONES) PRODUCIDOS POR EL USO O POR LA INCAPACIDAD DE USAR EL MATERIAL Y/O INFORMACION AQUÍ PRESENTADA.