CIBERSEGURIDAD

Informe de situación 2022

DISRUPTIVE

Plataforma Tecnológica Española
de Tecnologías Disruptivas

Con financiación de:

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA E INNOVACIÓN

Convocatoria 2020 Plataformas Tecnológicas
y de Innovación (PTR2020-001159)

Secretaria técnica a cargo de:

APTE
Asociación de Parques Científicos y Tecnológicos de España

INDICE

INTRODUCCIÓN

El Instituto Nacional de Ciberseguridad (INCIBE) a través de **INCIBE - CERT** gestionó **93.483 incidentes** durante 2021, casi un 30% menos que en 2020 y el **33% relativos a ataques de malware informático**. Asimismo, el **Centro Criptográfico Nacional detectó 69.202 incidentes** durante 2021, un 16% menor que en 2020, sin embargo, los incidentes críticos aumentaron un 124% con respecto an año anterior.

Según el Informe Anual de Seguridad Nacional de 2021, **el ransomware, sigue siendo la mayor amenaza** contra los sistemas y la información y durante la primera mitad de 2021 ocasionaron un importante impacto en algunos organismos públicos. En este sentido, **España participa en una iniciativa global liderada por Estados Unidos para tratar de movilizar a la comunidad internacional contra el ransomware**, que no solo constituye un problema económico si no que supone una amenaza a la soberanía de los Estados.

Gráfico 1: Informe «Panorama de amenazas» de ENISA de 2021 - Principales amenazas

Tal y como indica el Informe de Seguridad Nacional, la ciberseguridad es un aspecto y reto crucial en todas las tecnologías digitales disruptivas:

Durante los próximos años, incrementará el uso de la **IA** tanto para optimizar los ciberataques como para cometer actividades delictivas.
En cuanto al **5G**, uno de los retos fundamentales es reforzar su ciberseguridad, en particular ante la vulnerabilidad de la cadena de suministro y en lo relativo a injerencias externas.
En julio el Instituto Nacional de Estándares y Tecnología (NIST - National Institute of Standards and Technology) del Departamento de Comercio de Estados Unidos aprobó los primeros algoritmos de cifrado resistentes a la **computación cuántica**.
La ciberseguridad jugará un papel crucial de cara a garantizar un uso seguro de las aplicaciones desarrolladas bajo la tecnología **blockchain**.

Durante 2022 se han producido varios hechos importantes relacionados con la ciberseguridad:

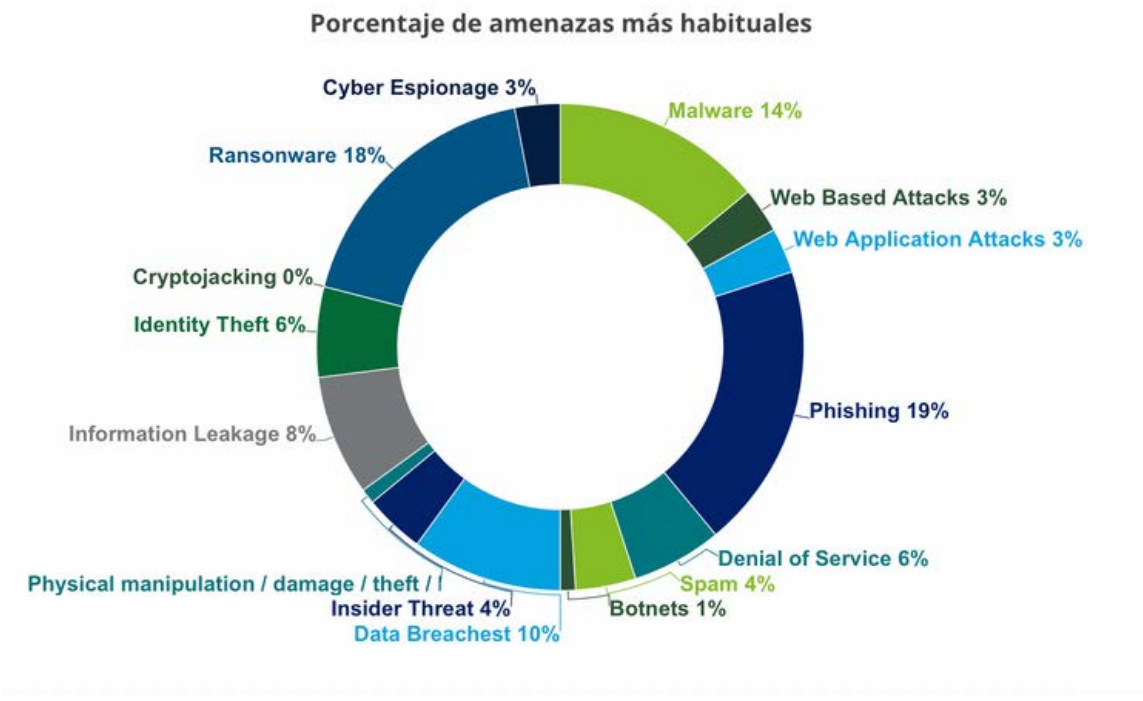
El 28 de abril de 2022 el pleno del Congreso de los Diputados convalidó la **Ley de Ciberseguridad 5G** que establece los requisitos de ciberseguridad específicos para el despliegue y la explotación de redes 5G.

En mayo, la Unión Europea aprobó la directiva NIS 2. La directiva sustituye a la directiva sobre la seguridad de las redes y sistemas de información y tiene como objetivo fortalecer los requisitos de seguridad, abordar la seguridad de las cadenas de suministro, simplificar las obligaciones de información e introducir medidas de supervisión y requisitos de ejecución más estrictos, incluidas sanciones armonizadas en toda la UE.

El pasado 28 de junio la Presidencia del Consejo y el Parlamento Europeo alcanzan un **acuerdo político sobre la Directiva relativa a la resiliencia de las entidades críticas** para aumentar la resiliencia de este tipo de entidades. El texto aprobado incluye entidades críticas en una serie de sectores como la energía, el transporte, la salud, el agua potable, las aguas residuales o el espacio.

Según datos de **Telefónica Cyber Security Tech,** el 60% de las pymes que sufren un ciberataque desaparece en menos de 6 meses tras el incidente, y cada ataque tiene un coste medio de 35.000 euros.

Según el informe elaborado por **Deloitte** sobre **el estado de la ciberseguridad en España** y publicado en 2022, las principales amenazas que sufren las empresas son las siguientes:



Fuente: Estado de la ciberseguridad en España (Deloitte)

Este informe pretende ser una foto del momento actual en el que se encuentra dicha tecnología en España y que sirva para poder comparar la situación en un futuro próximo.

TENDENCIAS

Fortune Business Insights pronostica que en el periodo del 2021 al 2028 **se registrará un crecimiento anual del mercado de la ciberseguridad del 12%**, situándose en torno de 366.000 millones de dólares.

En el último congreso **ENISE,** cita ineludible en la agenda de la ciberseguridad nacional e internacional organizado por INCIBE, las tendencias en el ámbito de la ciberseguridad más destacadas han sido las siguientes:

- **Nuevas amenazas y continuidad de negocio:** El coste de sufrir un ciberataque es cada vez mayor, por ello es necesario tomar medidas al respecto, y disponer de una estrategia de ciberseguridad clara.
- **Gestión y gobierno TI corporativo:** la digitalización lleva a que en las empresas gane más peso el área de Tecnologías de la Información (TI).
- **Protección de datos y activos de información:** La información es uno de los activos más importantes que tiene una empresa y por ello debe estar bien protegida.
- **Ciberseguridad en la nube:** las soluciones cloud ofrecen grandes ventajas pero para que sean seguras, debe adoptarse un modelo de seguridad fuerte que ayude a anticiparse a los ciberataques.
- **Inteligencia Artificial:** la aplicación de esta tecnología en el campo de la ciberseguridad contribuirá a afrontar la transformación digital con garantías.
- **Seguridad IoT:** aplicar IoT en las empresas presenta nuevos desafíos de seguridad, privacidad y cumplimiento normativo.
- **Cumplimiento normativo:** el RGPD tiene un gran impacto en los requisitos globales de protección de datos.

TENDENCIAS

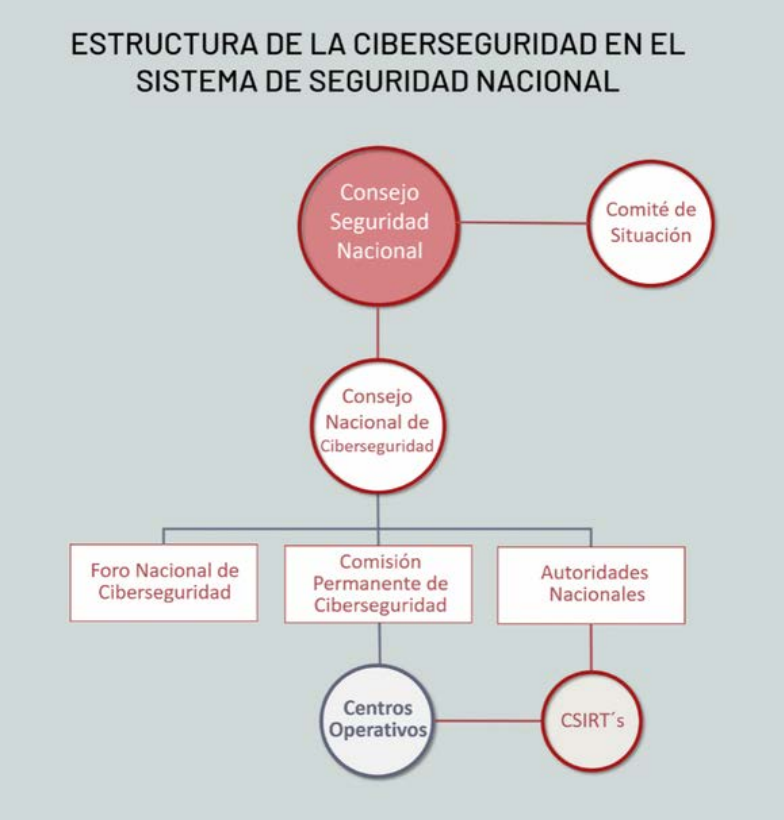
El análisis de Accenture publicado en febrero de 2022 identificaba cinco tendencias que afectan al panorama de la ciberseguridad:

1. **Los ataques de ransomware siguen siendo rentables** y la industria, la fabricación, los servicios financieros, la atención sanitaria y la tecnología siguen siendo los sectores más atacados.
2. **Las cadenas de suministro ofrecen un punto de ataque.**
3. **Los infostealers impulsan el mercado del malware.**
4. **La centralidad de la nube provoca nuevos vectores de ataque.**
5. **Se compran y venden activamente fallos de vulnerabilidad.**

Un aspecto cada vez más importante en materia de ciberseguridad es la **ciberresiliencia** y en este sentido, Accenture cuatro niveles de ciberresiliencia incluyendo un grupo élite de 'ciberdefensores': organizaciones que sobresalen en ciberresiliencia, pero que también se alinean con la estrategia empresarial para lograr mejore

Fuente: Informe Estado de resiliencia en ciberseguridad 2021 (Accenture)

ESTRATEGIA EN ESPAÑA



El febrero de 2022 el **Foro Nacional de Ciberseguridad**, un espacio de colaboración público-privada impulsado por el **Consejo de Seguridad Nacional** y creado en 2020 con el objetivo de fomentar la cultura de ciberseguridad, ofrecer apoyo a la Industria e I+D+i y promover la formación y el talento , publicó sus tres primeros informes que abordan cuestiones como la **generación de una cultura de ciberseguridad en la sociedad**, la creación de un **Esquema Nacional de Certificación de Responsables de Ciberseguridad** o las **necesidades de la industria y la investigación españolas en ciberseguridad.**
En la parte de enlaces de interés del presente informe se pueden consultar estos documentos.

En marzo, el Consejo de Ministros aprobó el **Plan Nacional de Ciberseguridad**, dando cumplimiento al mandato emitido por el Consejo de Seguridad Nacional y en desarrollo de la **Estrategia Nacional de Ciberseguridad 2019**.

ESTRATEGIA EN ESPAÑA

El **Plan Nacional de Ciberseguridad** es la articulación de la estrategia a seguir por todo el Estado para la mejora y refuerzo de la ciberseguridad de infraestructuras críticas, administraciones y organizaciones privadas. **Dotado con 1.200 millones de euros** para su financiación, el Plan **recoge 150 iniciativas**, entre actuaciones y proyectos, a desarrollar en los próximos tres años.

Entre las iniciativas destacan las siguientes:

Creación de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes y Amenazas, a través de la cual organismos públicos y privados puedan intercambiar información en tiempo real sobre ciberataques y otras ciberamenazas.

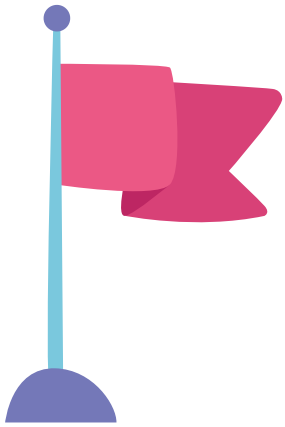
Puesta en marcha del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos (COCS). Esta actuación ya fue anunciada en 2017, pero no ha sido hasta ahora cuando finalmente ha comenzado su despliegue, con la licitación del proyecto a la alianza establecida por Indra y Telefónica.

En mayo, el **Centro Criptológico Nacional** publicó un nuevo **Esquema Nacional de Seguridad (ENS)** con el objetivo de facilitar una mejor respuesta, reducir las vulnerabilidades y promover la vigilancia continua ante los ciberataques.

Puesta en marcha de la Red Nacional de SOCs: Esta Red nace como respuesta a la Estrategia de Ciberseguridad para la Década Digital de la UE (2020), en la que se ve la necesidad de crear una red europea de SOC que, basada en IA, permita mejorar la detección de ciberamenazas. La Red Nacional de SOC, además de coordinar el intercambio de información entre los SOC nacionales, actuará como nexo de unión entre los diferentes SOC europeos.

RETOS Y OPORTUNIDADES

El informe de Seguridad Nacional de 2021 establece que los **principales retos** del ciberespacio son los siguientes:



- **Incremento y peligrosidad de los ciberataques**
- **Uso ilícito y malicioso del ciberespacio**
- **Dependencia tecnológica**
- **Tensión geopolítica**

Con respecto a las oportunidades, podemos señalar que en todos los **Proyectos estratégicos para la recuperación y transformación económica (PERTE)** se financian actividades relativas con el ámbito de la ciberseguridad.

A modo de ejemplo podemos citar los siguientes casos:

En el **PERTE de Salud de Vanguardia**, uno de sus 4 objetivos es potenciar la atención sanitaria primaria a través de la transformación digital que incluye actividades relativas a ciberseguridad para dispositivos médicos.

En el caso del **PERTE del Vehículo Electrico y Conectado**, las actividades de ciberseguridad están incluidas en el bloque complementario relativo a la conectividad del vehículo eléctrico.

RETOS Y OPORTUNIDADES

El pasado 4 de octubre el Instituto Nacional de Ciberseguridad **(INCIBE) presentó la nueva convocatoria de su iniciativa estratégica de Compra Pública Innovadora (CPI)** en el marco del Plan de Recuperación, Transformación y Resiliencia, con la financiación de los fondos Next Generation.

INCIBE canalizará al mercado un total de 137,2 millones de euros que elevan la cifra global del proyecto, tras la primera convocatoria publicada el 1 de julio de 2022, hasta los 224 millones, mediante contratos en el marco de la Compra Pública Innovadora.

la CPI se enmarca en los esfuerzos de INCIBE para el cumplimiento de su misión y tiene como objetivo general fortalecer el desarrollo industrial del sector de la ciberseguridad en todos sus ámbitos: I+D+i, emprendimiento, capacidades tecnológicas y talento.

Actuaciones susceptibles de ser ejecutadas mediante la Compra Pública Innovadora (CPI):

ECOSISTEMA

En el informe de situación de 2021 ya identificamos a los principales agentes del ecosistema, ahora resaltamos a los protagonistas de 2022

Durante 2022 algunos de los actores del sistema que más han destacado son los siguientes:

Incibe es designado en septiembre centro como Centro de Coordinación Nacional del Centro Europeo de Competencia en Ciberseguridad.
El Centro Europeo de Competencias en Ciberseguridad es una iniciativa europea que se enmarca dentro de las políticas europeas en ciberseguridad y que tiene como objetivo crear un ecosistema industrial y de investigación sobre ciberseguridad interconectado a escala de la UE, mejorando la cooperación entre las partes interesadas para hacer el mejor uso posible de los recursos y conocimientos técnicos existentes en esta materia en toda Europa. Con este fin se crea una red europea de Centros Nacionales de Coordinación (NCC) compuesta por 27 centros.

IriusRisk, startup de ciberseguridad aragonesa ubicada en el Parque Tecnológico Walqa consigue 29 millones de euros en una ronda liderada por Paladin Capital Group.
La empresa se fundó en Aragón por Stephen De Vries y Cristina Bentué.

ECOSISTEMA

RENIC: La Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC), promovida por INCIBE, es una asociación sectorial que engloba centros de investigación y otros agentes del ecosistema investigador en ciberseguridad de España. RENIC tiene como fin principal fomentar la investigación científica, el desarrollo tecnológico, la innovación, la trasferencia de conocimiento y tecnología a la industria y el desarrollo de proyectos de I+D+i en el sector de la ciberseguridad en España.

ObservaCIBER: es un nuevo espacio de encuentro especializado en ciberseguridad que, ante la creciente demanda de información sobre este ámbito por parte de la ciudadanía y las empresas, pretende por un lado, poner en valor el trabajo que vienen desarrollando los diferentes actores y por otro, conectar el conocimiento desarrollado por la administración en esta materia facilitando su comprensión. Su objetivo es aumentar la cultura de la ciberseguridad facilitando el acceso a la información y fomentando su calidad.

ECOSISTEMA

Woman4Ciber Spain: Women4Cyber Spain (W4C Spain) es una iniciativa que nace con el objetivo de convertirse en un referente en el impulso y visibilización del papel de la mujer en ciberseguridad en España, así como la diversidad de género en el sector.
La Asociación es el capítulo español de Women4Cyber.eu, fundada por la Organización Europea de Ciberseguridad (ECSO), y la primera asociación de mujeres en ciberseguridad en España que cuenta con respaldo europeo.

Málaga Hub de Ciberseguridad: Málaga se está posicionando como un gran hub de ciberseguridad. A la instalación de la Agencia Digital de Andalucía y el Centro de Ciberseguridad de Andalucía se le suma la apuesta que han hecho por la capital de la Costa del Sol empresas privadas del sector de la tecnología como Vodafone (con su centro tecnológico para toda Europa que creará 600 empleos cualificados), Google (con su centro de ciberserguridad), Telefónica (con el campus de programación que impulsa su Fundación en colaboración con la Junta), Dekra, Ericcson y o la Fundación Instituto Ricardo Valle.

Otros hub de ciberseguridad: Asimismo, destacan también otros puntos del mapa español, como por ejemplo, el País Vassco con el **Centro Vasco de Ciberseguridad**, Castilla La mancha con el **Centro Regional de Innovación Digital de Castilla La Mancha (CRID) o la Agencia de Ciberseguridad de Cataluña y la recién creada Agencia de Ciberseguridad de Madrid.**

CASOS DE USO

A continuación os mostramos algunos de los ejemplos de casos de uso que DISRUPTIVE ha ido recopilando y que puedes consultar con más detalle pinchando aquí

PROYECTO ARISTEO- CIDAUT

El proyecto ARISTEO, fruto de la colaboración entre Telefónica Tech Cyber & Cloud (C4IN, León) y Cidaut nació con la meta de hacer frente a la necesidad de fortalecer las redes de los entornos industriales (ICS) ante su apertura a un mundo con nuevas oportunidades y peligros de Ciberseguridad. Consiste en un conjunto de nodos conectados a Internet que representan infraestructuras críticas reales e ICS. Utilizando hardware real, se encarga de la extracción de inteligencia y detección proactiva de amenazas propias de los ecosistemas de Tecnologías de la Operación en entornos ICS.

ESTACIÓN ÓPTICA TERRESTRE QKD- Instituto Astrofísica de Canarias

IACTEC esta realizando el proyecto de una estación terrestre de comunicaciones ópticas clásicas y cuánticas, con apoyo financiero del Plan de Recuperación, transformación y resiliencia (Fondos Next Generation), que permite llevar a cabo comunicaciones seguras mediante el uso de tecnologías cuánticas. La comunicación cuántica es una tecnología que permite el envío de mensajes cifrados aprovechando las propiedades de los fotones (luz) para asegurar las seguridad de las comunicaciones y la protección de datos sensibles. En conclusión se trata de una red ultrasegura que será la base del internet del futuro. Los escenarios de comunicación que permite la estación desarrollada actualmente son inter-islas, interurbanos y con satélites LEO.

CASOS DE USO

AUDITORÍA HACKING ÉTICO- Cloud Levante

A Cloud Levante se le encomendó la tarea de mejorar la seguridad de la página web de un cliente.
Los portales web son el primer flanco de entrada y el lugar donde se testea la seguridad de la organización.
Durante el desarrollo del proyecto cloud fue necesario analizar el estado de la plataforma de la web. Analizar la configuración de cada componente y ofrecer una nueva arquitectura para mejorar la seguridad.
En concreto se realizó lo siguiente:

- Análisis de los componentes que conforman la Web y actualización de los mismos.
- Despliegue de nuevos servicios como CDN o Web Application Firewall.
- Desarrollo de una rearquitectura de la plataforma web.
- Pruebas de disponibilidad y seguridad.

ENLACES DE INTERÉS

Aquí os remitimos a enlaces de noticias, webs, documentos normativos o informes de interés, así como a bibliografía sobre esta tecnología.

Informe ciberamenazas y tendencias

La ciberseguridad es una cuestión de negocio

Observaciber

Cibersecurity Atlas

European Cybersecurity Challenge

European Cibersecurity Month

La startup de ciberseguridad ubicada en Parque Tecnológico Walqa levanta 29 millones

Annual Cyber threat review and predictions

La Unión Europea prevé un ahorro millonario gracias a la ley de Resiliencia Cibernética

Esquema Nacional de Seguridad

Novedades nuevo Esquema Nacional de Seguridad

Revista Tecnología y Sentido Común

Forno Nacional de Ciberseguridad

Informes del Foro Nacional de Ciberseguridad

Plan Nacional de Ciberseguridad 2022

Un ciberataque paraliza la actividad de 3 hospitales catalanes

Autores del Ransonware

El firmware será objetivo para malos actores

Retos de ciberseguridad para la digitalización industrial

Curso de formación dirigido a docentes

Iniciativa estratégica de compra pública innovadora de INCIBE

Retos de ciberseguridad CPI

Aprobación de la directiva NIS 2.0

la Presidencia del Consejo y el Parlamento Europeo alcanzan un acuerdo político para aumentar la resiliencia de las entidades críticas

Informe "Panorama de amenaza" de ENISA de 2021

Red Nacional de SOCs

Red de Excelencia Nacional de Investigación en Ciberseguridad

Transposición española directiva NIS 2

Interior y Economía firman un acuerdo de colaboración para reforzar la ciberseguridad

Estado de resiliencia en ciberseguridad 2021

Informe de inteligencia sobre ciberamenazas Volumen 2

Ley de ciberseguridad 5G

Primera Asamblea General de Women4CiberSpain

Málaga se puede convertir en un hub de relevancia mundial de tecnologías digitales y ciberseguridad

Andalucía destinará 60 millones en 3 años al plan de ciberseguridad que se pilotará desde Málaga

Centro Regional de Innovación Digital de Castilla La Mancha (CRID)

Centro Vasco de Ciberseguridad

Agencia de Ciberseguridad de Cataluña

Agencia de Ciberseguridad de Madrid

Estrategia Andaluza de Ciberseguridad

Informe realizado por la **Asociación de Parques Científicos y Tecnológicos de España (APTE),** entidad que gestiona la secretaría técnica de la **Plataforma Tecnológica Española de Tecnologías Disruptivas (DISRUPTIVE)** con la colaboración de su **grupo de trabajo de ciberseguridad** durante el último trimestre de 2022

DISRUPTIVE Plataforma Tecnológica Española de Tecnologías Disruptivas

Con financiación de:

GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN

Convocatoria 2020 Plataformas Tecnológicas y de Innovación (PTR2020-001159)

Secretaria técnica a cargo de:

APTE Asociación de Parques Científicos y Tecnológicos de España