VENTAJAS PARA *START-UPS* LATINOAMERICANAS EN ESPAÑA. TRÁMITES Y PASOS PARA ESTABLECERSE

ESTUDIO

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. Propuesta de contenido 5

1.1. Introducción 5
1.2. El consumo y madurez en ciberseguridad de Europa y España 5

1.2.1. ¿Por qué Europa? 5

1.2.2. ¿Por qué España dentro de Europa? Análisis del gasto español en ciberseguridad 9

1.2.3. ¿Por qué España dentro de Europa? Análisis del índice de madurez en ciberseguridad español 12

1.3. El consumo y madurez en ciberseguridad en Latinoamérica 15

1.3.1. Consumo en ciberseguridad en diferentes países latinoamericanos 15

1.3.2. Ámbito regulatorio, legislativo, administrativo y de oferta y demanda en diferentes países latinoamericanos 19

1.4. Estudio de casos de éxito: Argentina y México 40

1.4.1. México 41

1.4.2. Argentina 46

1.5. Procedimiento para la creación de una empresa como extranjero residente fuera de la comunidad europea 49

1.5.1. ¿Y si tengo la doble nacionalidad? 50

1.5.2. El DUE (Documento Único Electrónico) como medio para facilitar los trámites de creación de una sociedad limitada 51

1.5.3. Documentación previa necesaria para la obtención del DUE 53

1.5.4. Información previa necesaria para la obtención del DUE 55

1.5.5. Trámites previos a la solicitud del DUE 56

1.5.6. Pasos que realiza el sistema telemático de creación de empresas, sin intervención del emprendedor, una vez cumplimentado el DUE 59

1.5.7. Trámites complementarios a la solicitud del DUE 60

1.5.8. Trámites no incluidos en el sistema 61

1.6. Ayudas y reglamentación para la creación de *start-up* en 2023 en España 61

1.6.1. Creación de la *start-up* 61

1.6.2. Crecimiento de la *start-up* 62

1.6.3. Cese de actividad 63

1.7. Conclusiones 63

2. Referencias 65

ÍNDICE DE FIGURAS

Figura 1. Proyección (P) del mercado mundial de ciberseguridad hasta 2027, contrastado con el consumo real (R) en 2021 y 2022. Datos: [1]. Análisis: INCIBE 6
Figura 2. Tasa de Crecimiento Promedio (CAGR) 6
Figura 3. Proyección de la cuota de mercado mundial en ciberseguridad en 2027. Datos: [1]. Análisis: INCIBE 7
Figura 4. Impacto directo en términos de empleo de la ciberseguridad en Europa. Fuente: [2] 8
Figura 5. Gap entre demanda y oferta de empleo en mercados digitales. Fuente: [2] 8
Figura 6. Consumo de soluciones de seguridad por sector en Europa. Fuente: [2] 9
Figura 7. Países con una cuota de gasto mayor al 1% en ciberseguridad (TOTAL: 168.338,69M $). Datos: [1]. Análisis: INCIBE 10
Figura 8. Nodos del programa RETECH español. Fuente: [2] 12
Figura 9. Ranking ITU GCI 2020. Fuente: [3] 13
Figura 10. Dominios del ranking ITU [3] 14
Figura 11. Desglose de la puntuación de España en el GCI 2020 15
Figura 12. Gasto proyectado por países destacados de la región de Latinoamérica en 2027. Datos: [1]. Análisis: INCIBE 18
Figura 13. Desglose de la puntuación de Argentina en el ranking ITU GCI 2020 20
Figura 14. Desglose de la puntuación de México en el ranking ITU GCI 2020 21
Figura 15. Desglose de la puntuación de Brasil en el ranking ITU GCI 2020 22
Figura 16. Desglose de la puntuación de Colombia en el ranking ITU GCI 2020 23
Figura 17. Desglose de la puntuación de Chile en el ranking ITU GCI 2020 24
Figura 18. Desglose de la puntuación de Perú en el ranking ITU GCI 2020 25
Figura 19. Desglose de la puntuación de Uruguay en el ranking ITU GCI 2020 26
Figura 20. Ranking por países en la región de América según el ranking ITU GCI 2020 26
Figura 21. Países Latinoamericanos con una Estrategia Nacional de Ciberseguridad según el ranking ITU GCI 2020 27
Figura 22. Gráfico comparativo entre países Latinoamericanos del dominio D1 del estudio de la OEA. Datos: [15]. Análisis: INCIBE 31
Figura 23. Gráfico comparativo entre países Latinoamericanos del dominio D2 del estudio de la OEA. Datos: [15]. Análisis: INCIBE 33
Figura 24. Gráfico comparativo entre países Latinoamericanos del dominio D3 del estudio de la OEA. Datos: [15]. Análisis: INCIBE 34
Figura 25. Gráfico comparativo entre países Latinoamericanos del dominio D4 del estudio de la OEA. Datos: [15]. Análisis: INCIBE 36
Figura 26. Gráfico comparativo entre países Latinoamericanos del dominio D5 del estudio de la OEA. Datos: [15]. Análisis: INCIBE 37
Figura 27.Localización geográfica de start-up en Argentina en el primer semestre de 2022 (% del total de start-up). Fuente: [22] 46
Figura 28. Funciones principales de un PAE [41] 52
Figura 29. El DUE [35] 53

ÍNDICE DE TABLAS

Tabla 1. Gasto en ciberseguridad en la zona Europa oeste. Datos: [1]. Análisis: INCIBE 10
Tabla 2. Gasto en ciberseguridad en España por tipo de solución. Datos: [1]. Análisis: INCIBE 11
Tabla 3. Mercado mundial de Ciberseguridad por regiones. Datos: [1]. Análisis: INCIBE 15
Tabla 4. Países latinoamericanos mejor posicionados en el ranking de 50 países con más gasto en ciberseguridad. Datos: [1]. Análisis: INCIBE 16
Tabla 5. Gasto de países destacados en la región de Latinoamérica. Datos: [1]. Análisis: INCIBE 17

Tabla 6. Gasto en ciberseguridad en países latinoamericanos por tipo de solución Datos: [1]. Análisis: INCIBE 18
Tabla 7. Resumen de los aspectos Latinoamericanos analizados vs España. Datos: [3]. Análisis: INCIBE 28
Tabla 8. Análisis del dominio D1 de los países latinoamericanos estudiados según la OEA. Datos: [15]. Análisis: INCIBE 30
Tabla 9. Análisis del dominio D2 de los países latinoamericanos estudiados según la OEA. Datos: [15]. Análisis: INCIBE 32
Tabla 10. Análisis del dominio D3 de los países latinoamericanos estudiados según la OEA. Datos: [15]. Análisis: INCIBE 34
Tabla 11. Análisis del dominio D4 de los países latinoamericanos estudiados según la OEA. Datos: [15]. Análisis: INCIBE 35
Tabla 12. Análisis del dominio D5 de los países latinoamericanos estudiados según la OEA. Datos: [15]. Análisis: INCIBE 36
Tabla 13. Resumen global de puntuación de los 5 dominios de los países latinoamericanos estudiados según la OEA. Datos: [15]. Análisis: INCIBE 38
Tabla 14. Start-up "unicornio" destacables en México 42
Tabla 15. Principales empresas de ciberseguridad en México 43
Tabla 16. Listado de empresas "unicornio" en Argentina. Valoración en MUSD en abril de 2022. Fuente: [22] 47
Tabla 17. Principales empresas de ciberseguridad en Argentina 47

1. PROPUESTA DE CONTENIDO

1.1. Introducción

En este informe estudiaremos de manera general el **panorama de ciberseguridad en Latinoamérica**, y los diferentes motivos por los cuales España puede ser **un destino atractivo** para la inversión y crecimiento en ciberseguridad para empresas latinoamericanas que quieran incorporarse al mercado europeo.

Para ello se destacarán, entre otros, el **atractivo de España** para las empresas latinoamericanas para entrar en el mercado europeo. Posteriormente se hará un estudio del **estado de la ciberseguridad** en Latinoamérica en lo relativo a consumo y madurez del mercado en el país y empresas que ofertan servicios en el mismo. Finalmente, se destacarán las diferentes **iniciativas y apoyos legislativos** que se han creado para ello en España durante los últimos años.

Este informe prestará **especial atención a las necesidades y ventajas de las empresas latinoamericanas que quieran establecerse en España**: la inexistencia de una barrera de idioma, ventajas fiscales, entorno o marco legislativo (ley de *start-up*, ley "Crea y Crece"), aspectos administrativos, etc.,

Con todo ello, el objetivo de este informe es **facilitar la incorporación de las empresas latinoamericanas** que estén buscando "dar el salto" y **expandir su mercado al mercado de ciberseguridad floreciente español**, como mejor vía para la entrada posterior en el mercado europeo.

1.2. El consumo y madurez en ciberseguridad de Europa y España

1.2.1. ¿Por qué Europa?

Como mencionamos en la introducción, una de las principales razones de la creación de este informe es exponer claramente **las ventajas de España** como país atractivo para que las empresas de ciberseguridad latinoamericanas expandan sus actividades. Además, podrán usar esta expansión **como puerta de entrada al mercado europeo**. Ahora bien, **¿por qué es atractivo el mercado europeo precisamente?** Un análisis a los datos proporcionados por Gartner [1] nos ofrece razones muy sólidas para ello.

Los países que conforman la región denominada "**Europa Oeste**" son en conjunto la **segunda región del mundo** en el mercado mundial de ciberseguridad. Como se puede ver en la Figura *1*, durante en el año 2023 se prevé un mercado de unos **44.000 millones de dólares**, mientras que la proyección del mercado hasta el 2027 ofrece un incremento muy sustancial de esta cifra, hasta **casi los 71.000 millones** (+61%). Esto sitúa a esta región solo por detrás de Norte América en el mercado de ciberseguridad.

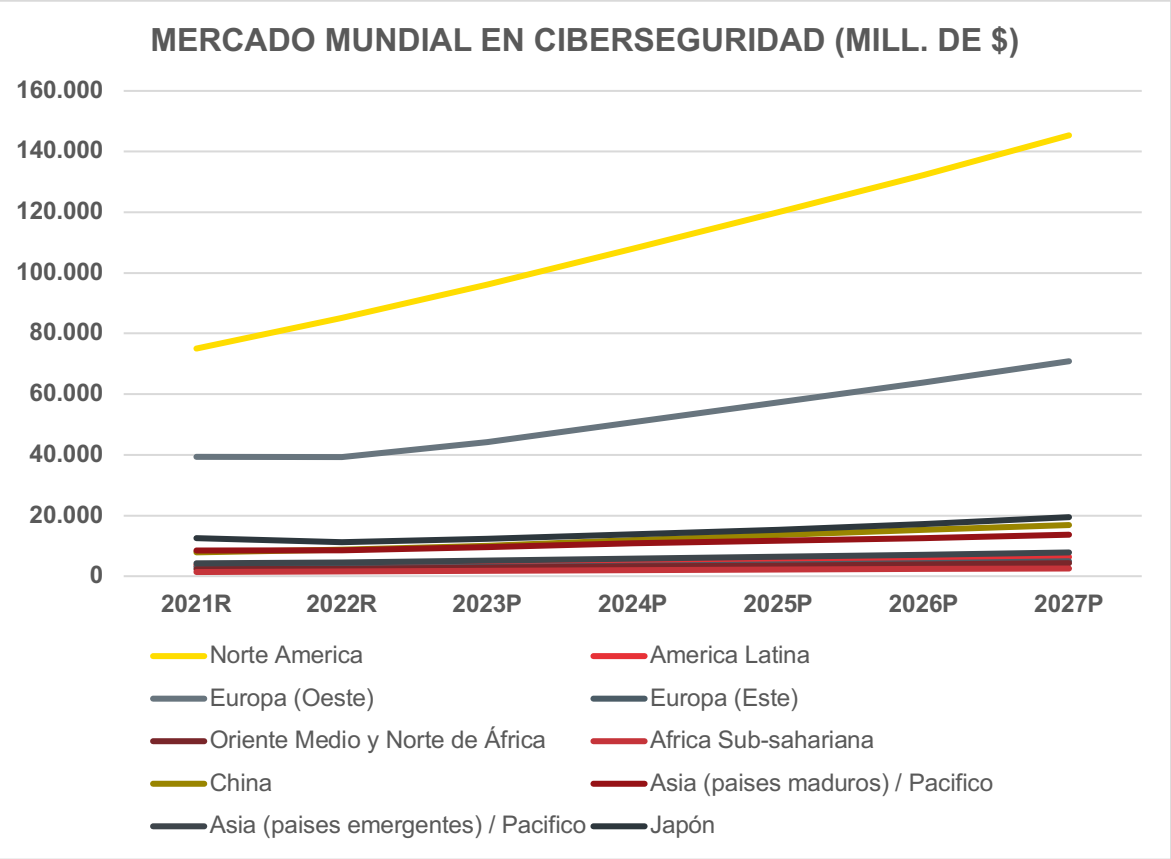


Figura 1. Proyección (P) del mercado mundial de ciberseguridad hasta 2027, contrastado con el consumo real (R) en 2021 y 2022. Datos: [1]. Análisis: INCIBE

Una de las cosas que se observa en los datos del mercado **proyectado** (P) hasta el 2027 es que, a pesar de que en el gasto esta región sigue estando en segunda posición tras Norte América, su **tasa de crecimiento promedio** o CAGR (calculada como se indica en la Figura 2) es **mayor que la de EEUU** (11,3% frente a 12,5% de Europa Oeste) y se sitúa como **segunda tasa de crecimiento más grande**, solo por detrás de China (con un 14,1%).

$$CAGR = \left(\frac{\text{Ending Value}}{\text{Beginning Value}}\right)^{\left(\frac{1}{\#\text{ of years}}\right)} - 1$$

Figura 2. Tasa de Crecimiento Promedio (CAGR)

Por tanto, Europa Oeste es la **segunda región, tanto en mercado de ciberseguridad** (solo por detrás de Norte América) **como en tasa de crecimiento** proyectada hasta el 2027 (solo por detrás de China), siendo una región con gran volumen de mercado y una **brillante proyección de futuro**, lo que la hace muy atractiva como objetivo de inversión.

Detallando algo más las proyecciones de futuro, como se ve en la Figura 3, Europa Oeste tendrá **una cuota del 24,26%** del mercado de ciberseguridad en 2027, un **0,92% más que en 2022**. Se da también la circunstancia que es **la región que más aumenta su cuota de mercado** en las proyecciones, solo por detrás de China (0,60%), y en detrimento de otras regiones (como Norte América, que pierde un 0,85% del 2022 al 2027).

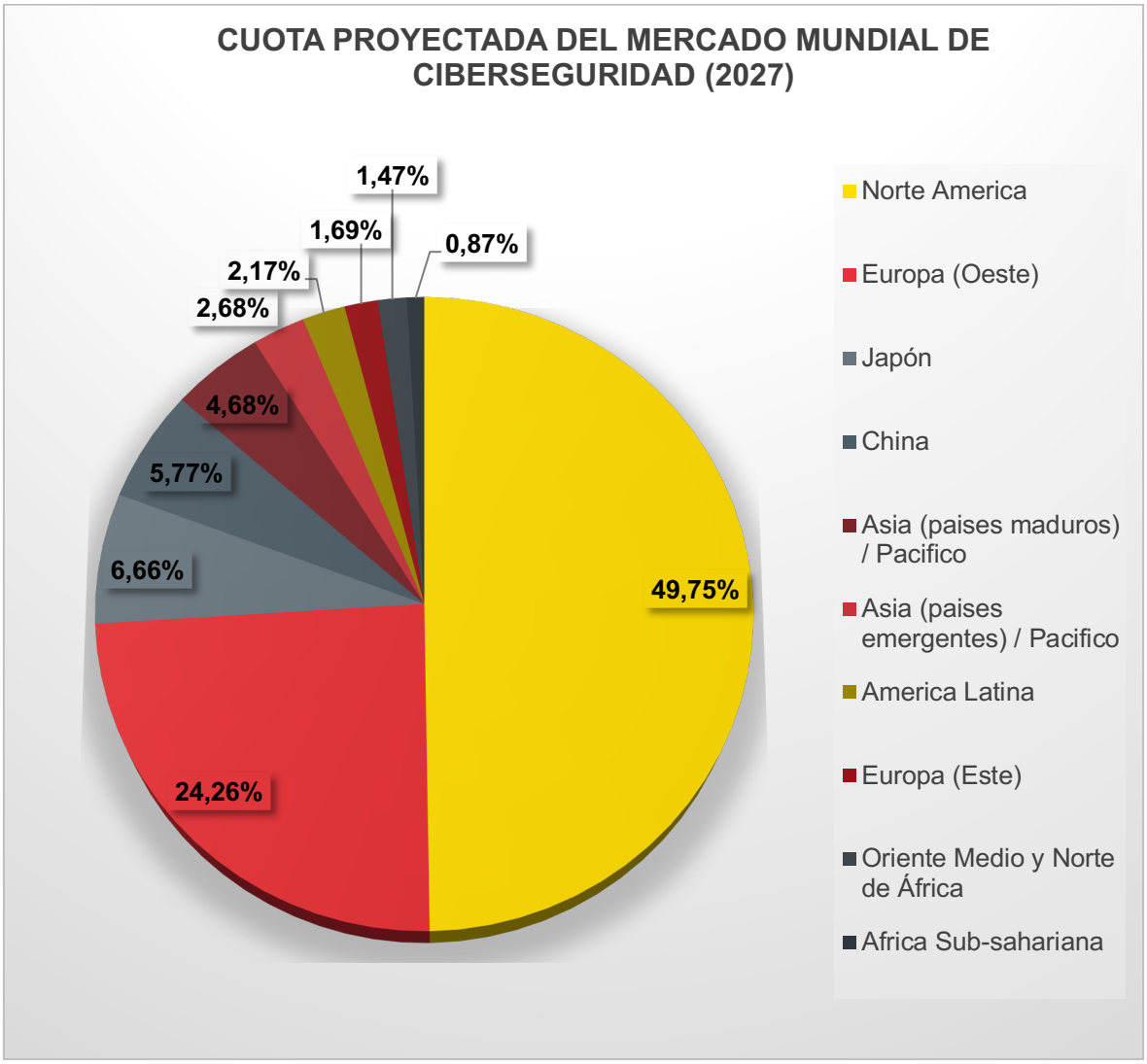


Figura 3. Proyección de la cuota de mercado mundial en ciberseguridad en 2027. Datos: [1]. Análisis: INCIBE

Una de las razones por las que la región de Europa Oeste es un destino ideal para la inversión en ciberseguridad para empresas latinoamericanas es que **es uno de los mercados laborales más atractivos del mundo** en este aspecto [2]. La Figura 4 muestra el **impacto directo en términos de empleo** de la ciberseguridad en Europa Oeste, dividida por países. En ella podemos ver claramente como Alemania se encuentra a la cabeza, siendo España el país que se encuentra en quinto lugar.

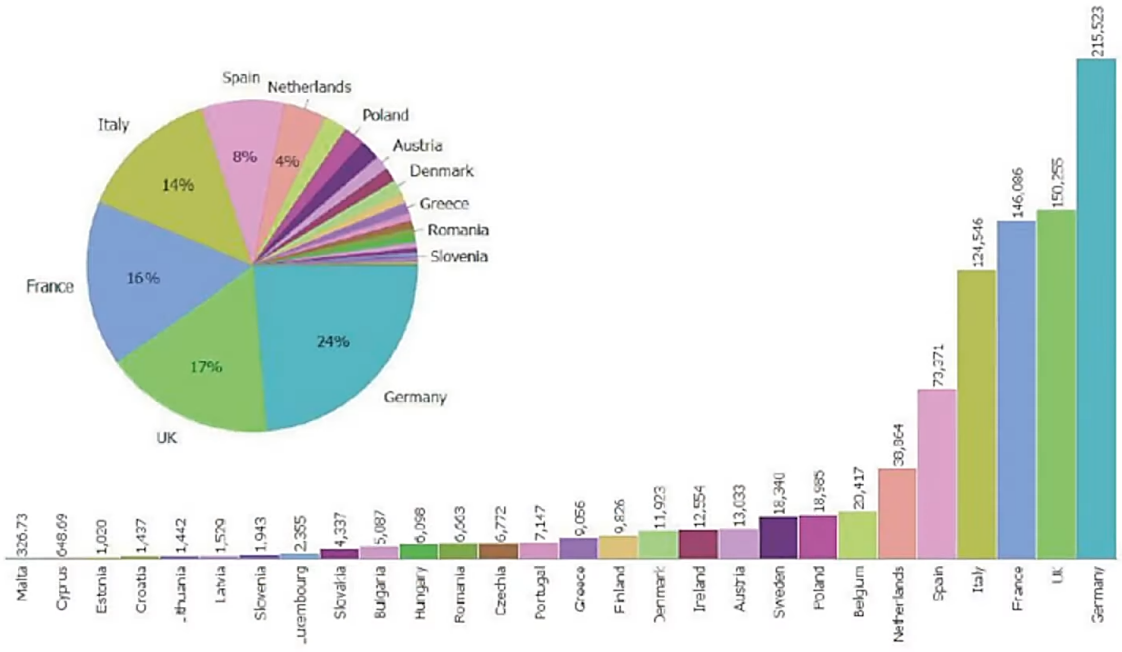


Figura 4. Impacto directo en términos de empleo de la ciberseguridad en Europa. Fuente: [2]

La región de Europa Oeste tiene un mercado **mucho más competitivo que EEUU** en la formación de profesionales y atracción de talento en ciberseguridad [2]. Si bien es cierto que existe un gap de talento en esta área (Figura 5), con **40.000 nuevos profesionales** necesarios en un futuro próximo, Europa está tomando medidas firmes para reducir este gap en los próximos 3 años y que las empresas que quieran establecerse en esta región **puedan encontrar el talento necesario** para desarrollar sus vías de negocio.

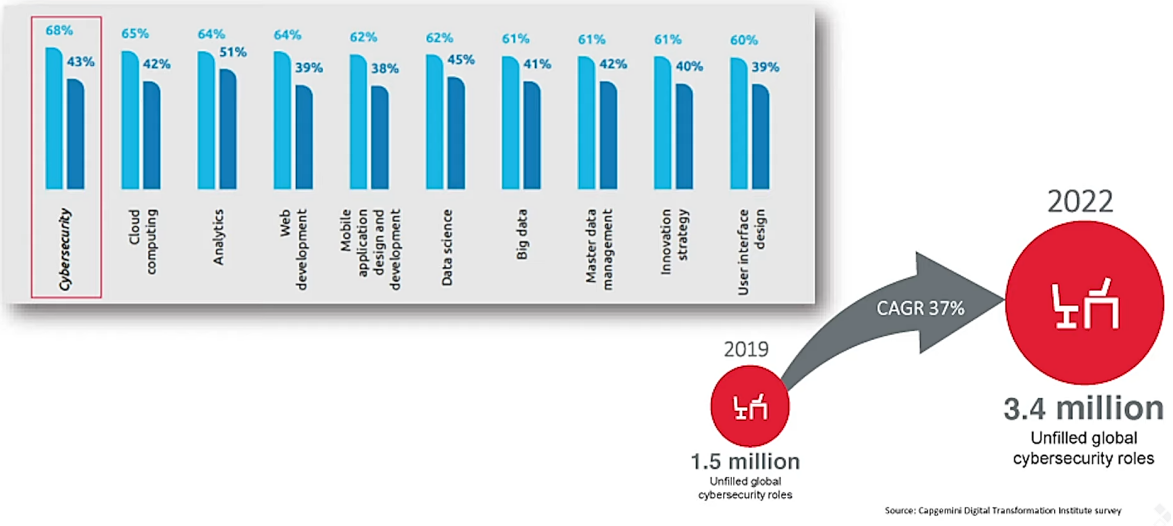


Figura 5. Gap entre demanda y oferta de empleo en mercados digitales. Fuente: [2]

La gran demanda de profesionales de seguridad se debe en parte a que se ha incrementado **la demanda de soluciones de ciberseguridad por sector en la región de Europa Oeste**. Esto quiere decir que no solo sectores más tradicionales, como el militar, demandan estas soluciones, sino que otros sectores (ver Figura 6) tienen un consumo

interior de soluciones tecnológicas en ciberseguridad que hay que desarrollar, lo que supone otra importante fuente de inversión e innovación.

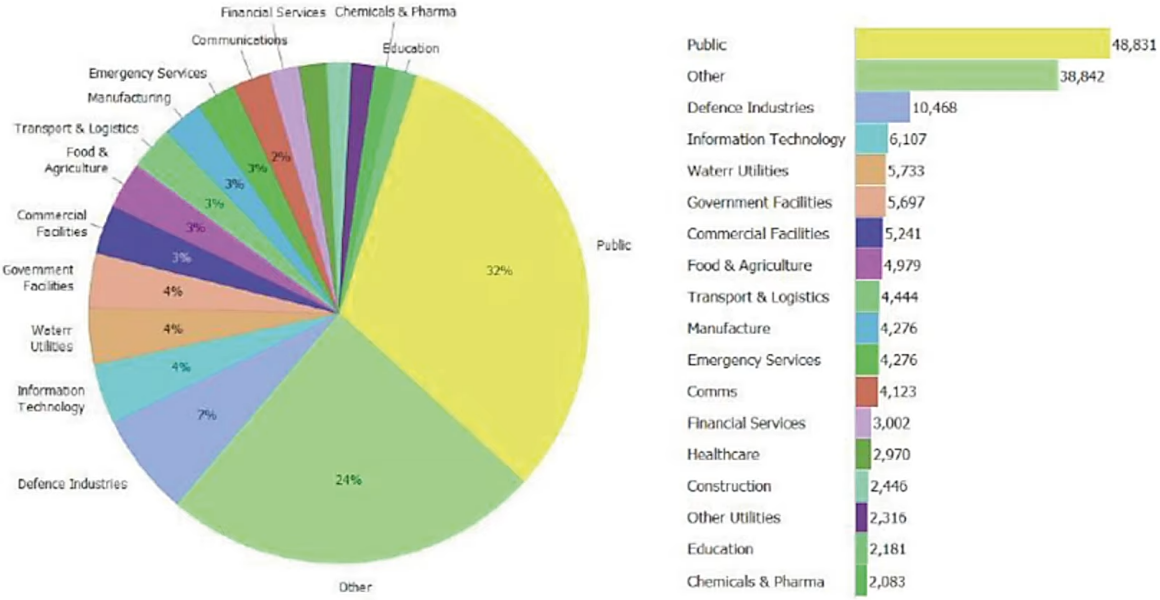


Figura 6. Consumo de soluciones de seguridad por sector en Europa. Fuente: [2]

1.2.2. ¿Por qué España dentro de Europa? Análisis del gasto español en ciberseguridad

Una vez vista la creciente importancia y proyección de futuro en el mercado de ciberseguridad de la región Europa Oeste, la siguiente cuestión ¿**por qué elegir España como puerta de entrada a este mercado?** Esto vamos a justificarlo por dos vías.

1. **La importancia de España en el mercado de ciberseguridad a nivel mundial**, que pasaremos a analizar en esta sección.
2. **Que no existe la barrera del idioma** entre Latinoamérica y España, lo que facilita la expansión del negocio tanto a nivel logístico como administrativo.

En el año 2022, de nuevo de acuerdo con los últimos datos disponibles de **Gartner** en la fecha en la que se redactó este informe [1], el gasto total en ciberseguridad de España fue de **2.047,97 millones de dólares**, un **1,22%** del gasto total mundial. Esto hace que España ocupe el **puesto 13** en el *ranking* de países que más gastan en este concepto. Como se ve en la Figura 7, **solo 14 países superan la cuota del 1% en gasto en ciberseguridad,** y España es uno de ellos.

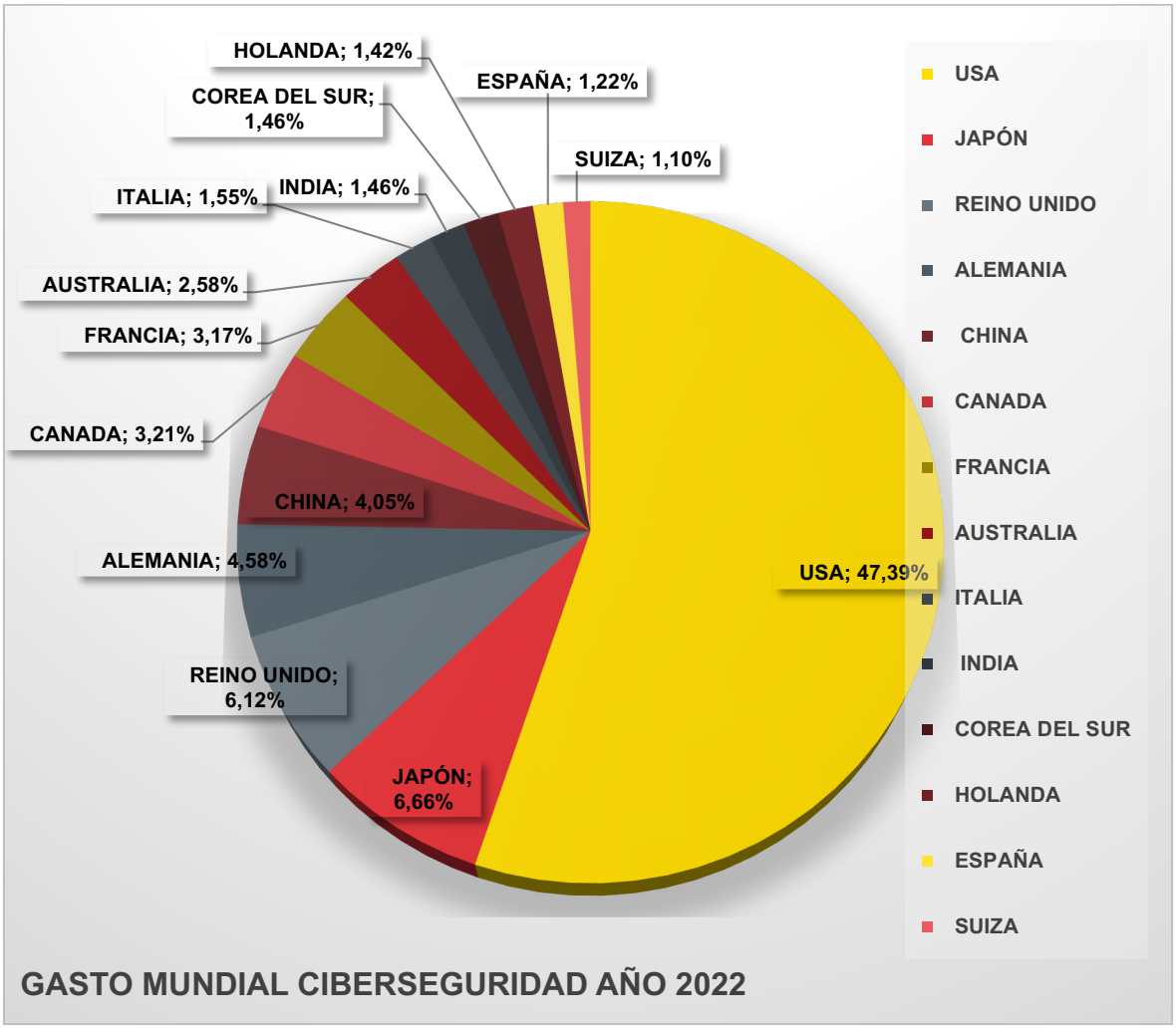


Figura 7. Países con una cuota de gasto mayor al 1% en ciberseguridad (TOTAL: 168.338,69M $). Datos: [1]. Análisis: INCIBE

Si nos restringimos solo a **países que conforman la región Europa Oeste**, España se sitúa en el **puesto 6 del *ranking* de gasto,** como se aprecia en la Tabla 1, con un **5,23%** de la cuota de gasto total de estos países y a una relativa corta distancia de Holanda e Italia, los dos países siguientes.

Tabla 1. Gasto en ciberseguridad en la zona Europa oeste. Datos: [1]. Análisis: INCIBE

PAISES EUROPA OESTE GASTO MILLONES $	2022R	CUOTA	*RANKING*
REINO UNIDO	10.307,22	26,33%	1
ALEMANIA	7.702,31	19,68%	2
FRANCIA	5.335,85	13,63%	3
ITALIA	2.603,08	6,65%	4
HOLANDA	2.384,39	6,09%	5
ESPAÑA	**2.047,97**	**5,23%**	**6**
SUIZA	1.857,79	4,75%	7
SUECIA	1.371,21	3,50%	8

BÉLIGA	973,20	2,49%	9
DINAMARCA	895,11	2,29%	10
AUSTRIA	809,37	2,07%	11
NORUEGA	786,66	2,01%	12
FINLANDIA	749,39	1,91%	13
IRLANDA	554,78	1,42%	14
PORTUGAL	368,00	0,94%	15
GRECIA	242,85	0,62%	16
HUNGRÍA	152,39	0,39%	17
TOTAL	**39.141,58**	**100,00%**	

Estos 2.047 millones de gasto en ciberseguridad de España se pueden **desglosar en sectores**. Esto permite conocer cuáles adquieren más importancia frente a otros dentro de la multitud de posibilidades de inversión que ofrece la ciberseguridad. Siguiendo la **clasificación de áreas** y los datos de Gartner, la Tabla 2 desglosa este gasto en 2022 y el proyectado en 2027.

Tabla 2. Gasto en ciberseguridad en España por tipo de solución. Datos: [1]. Análisis: INCIBE

ESPAÑA GASTO MILLONES DE $	2022R	CUOTA	2027P	CUOTA
Servicios de seguridad	1.159,94	56,64%	1.966,85	54,55%
Protección de infraestructura	228,74	11,17%	419,74	11,64%
Equipamiento de seguridad en red	227,32	11,10%	393,90	10,92%
Gestión de identidades	128,90	6,29%	208,86	5,79%
Software de Seguridad para el consumidor	102,52	5,01%	148,73	4,13%
Seguridad en nube	49,01	2,39%	138,54	3,84%
Seguridad de Aplicaciones	39,94	1,95%	129,49	3,59%
Manejo integrado de riesgos	51,19	2,50%	76,15	2,11%
Privacidad de datos	21,31	1,04%	54,25	1,50%
Seguridad de datos	26,10	1,27%	50,22	1,39%
Otro software de seguridad de la información	12,98	0,63%	18,76	0,52%
TOTAL	**2.047,97**	**100,00%**	**3.605,51**	**100,00%**

Vemos por tanto que los **servicios de seguridad** se llevan más de la mitad del gasto realizado en ciberseguridad en España, seguidos de lejos por el **equipamiento en seguridad de red** y la **protección de infraestructuras**.

Por otro lado, la proyección del incremento de gasto total en ciberseguridad en España hasta el 2027 es de un **76,05%**, poniéndolo muy por encima de los niveles actuales de Italia y Holanda señalados en la Tabla 1.

Este desglose también puede usarse como un indicador de las **áreas donde puede resultar más interesante desarrollar negocio** por parte de *start-up* latinoamericanas en el futuro, ya que estas proyecciones indican aquellas en las que hay un mayor interés en su desarrollo.

Otra razón de peso para elegir España como destino de inversión innovadora y expansión de mercado es que **tiene la investigación especializada en ciberseguridad más competitiva de la región Europa Oeste**. España **lidera el retorno de inversiones** de proyectos de ciberseguridad en la unión europea [2], por encima del Reino Unido, a pesar de que este es el país de la región que figura como primer clasificado en Europa dentro del ranking ITU que veremos después (Figura 9). Esto es gracias a los **45 equipos de investigación** de excelencia en universidades.

España también es un lugar de gran proyección en el fomento de *start-ups* que desarrollen iniciativas en ciberseguridad. En la actualidad, España ha respondido a la llamada de la OTAN para **desarrollar una aceleradora de empresas en el sur de Europa** gracias a los fondos del plan de recuperación otorgados al país [2].

Otra iniciativa muy interesante es el **programa RETECH** (Figura 8), por el cual las comunidades autónomas van a desplegar **estrategias regionales de innovación** para desarrollar las capacidades de ciberseguridad. Se trata del programa más ambicioso de Europa para desarrollar nodos tecnológicos de ciberseguridad e incorporar la ciberseguridad como eje central de las actividades la cada comunidad, fomentando así la demanda y la atracción de nuevas oportunidades de inversión para dar respuesta a sus necesidades.

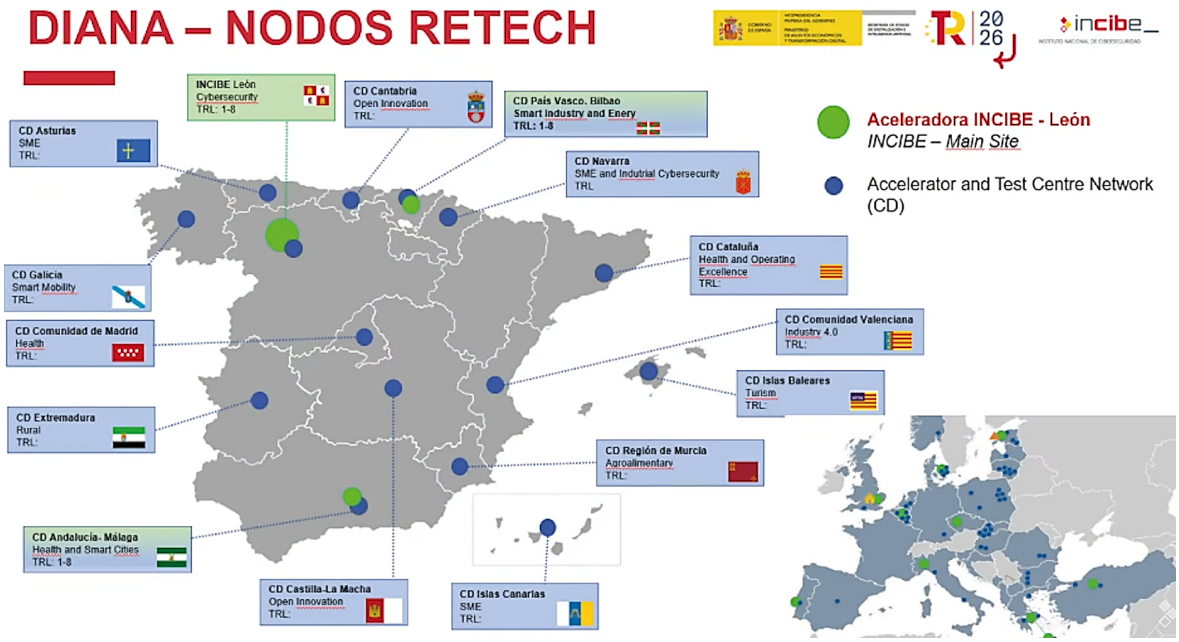


Figura 8. Nodos del programa RETECH español. Fuente: [2]

1.2.3. ¿Por qué España dentro de Europa? Análisis del índice de madurez en ciberseguridad español

Por tanto, desde la perspectiva de la región **Europa Oeste,** acabamos de ver **que España es un país muy bien posicionado** en cuanto a gasto en ciberseguridad y perspectivas de desarrollo futuro de este mercado. No obstante, el otro dato que posiciona a España en un lugar **privilegiado** respecto a otros países de su misma región **es su muy alto grado de madurez en aspectos de ciberseguridad**.

Según el ***Global Security Index*** (GCI) 2020, un ***ranking*** **internacional** creado por la ITU (*International Telecommunication Union*) [3], **España es el 4º país más ciberseguro del mundo** (ver Figura 9) entre los 194 que este *ranking* analiza. Además, se sitúa **segundo** (solo por detrás del Reino Unido) en la región de Europa Oeste que estamos analizando.

.

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10

Figura 9. Ranking ITU GCI 2020. Fuente: [3]

La importancia de este *ranking* es muy alta, no solo por ser un estudio extensivo de una gran cantidad de países, sino por la **exhaustividad** de este. El estudio divide los aspectos de ciberseguridad estudiados en **cinco dominios.**

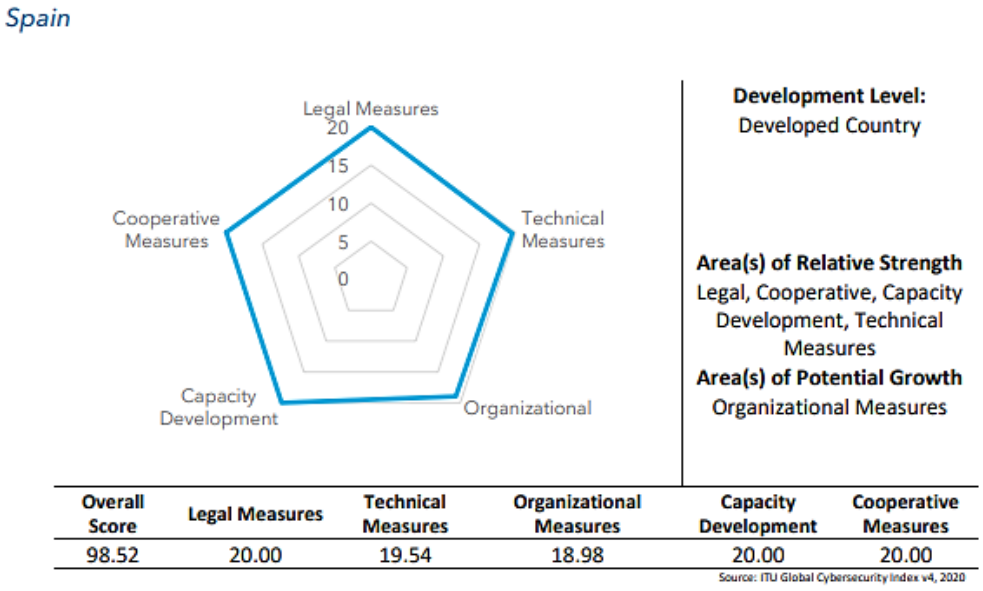
1. **Legal**: Se evalúa las leyes y regulaciones del cibercrimen y la ciberseguridad.
2. **Técnico**: Se evalúa la existencia de CSIRTs, y mecanismos de reporte de protección online de niños.
3. **Organizacional**: se valora la existencia de estrategias nacional de ciberseguridad, Agencias de ciberseguridad, etc.
4. **Desarrollo de capacidades** de ciberseguridad.
5. **Cooperación**: se valora la existencia de acuerdos y colaboraciones entre países.

La Figura 10 muestra un desglose más detallado de dichos dominios, para entender mejor qué aspectos concretos se analizan dentro de los mismos.

Figura 10. Dominios del ranking ITU [3]

Este *ranking* **no analiza el grado de madurez de las empresas**, aunque si se quieren tener datos sobre este aspecto en España se puede consultar el siguiente estudio del observatorio de ciberseguridad de ISMS Forum [4].

En el análisis realizado a España se han otorgado **puntuaciones de 0 a 20 en los cinco aspectos mencionados**. España ha obtenido **la máxima puntuación** en todos salvo en técnico y organizativo, que aún tienen cierto margen de mejora (Figura 11 [3]).



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
98.52	20.00	19.54	18.98	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2020

Figura 11. Desglose de la puntuación de España en el GCI 2020

Este resultado extraordinario de España en este *ranking* no es tampoco fruto de un solo año, sino de **un trabajo continuo y un esfuerzo global de todo el país.** España ha pasado del 9º puesto en el mismo *ranking* en su edición del 2015 al 4º en solo 5 año**s.**

Con toda la información extraída en este análisis podemos concluir que **España es un país destacado en cuanto a gasto** de ciberseguridad, sobre todo si se le compara con países de su misma región, y que **es puntero a nivel mundial en lo referente a la madurez en ciberseguridad**, a la luz de lo que arroja el *ranking* GCI mencionado. Además, tanto el gasto como el incremento de la madurez son compromisos que parece que claramente se quieren **mantener y mejorar en el tiempo** [4], haciendo a España un **lugar muy atractivo para invertir**.

Precisamente para perfilar dichas inversiones y poder discutir más en profundidad sobre ellas, en la siguiente sección vamos a hacer un análisis del consumo y madurez de la ciberseguridad en Latinoamérica, que luego podremos poner en consideración con el que acabamos de hacer de España para encontrar potenciales sinergias.

1.3. El consumo y madurez en ciberseguridad en Latinoamérica

1.3.1. Consumo en ciberseguridad en diferentes países latinoamericanos

A nivel **mundial**, la región correspondiente a **América Latina** se sitúa actualmente como **séptima** dentro de 10 áreas geográficas identificadas por los datos de Gartner [1] en cuanto a mercado de ciberseguridad. Se sitúa además muy cerca de la región Asia (Países Emergentes) / Pacífico, como se puede ver en la Tabla 3.

Tabla 3. Mercado mundial de Ciberseguridad por regiones. Datos: [1]. Análisis: INCIBE

MERCADO MUNDIAL MILLONES $	2022R	CUOTA	*Ranking*
NORTE AMERICA	85174,08	50,60%	1

EUROPA (OESTE)	39274,93	23,33%	2
JAPÓN	11213,44	6,66%	3
CHINA	8713,743	5,18%	4
ASIA (PAISES MADUROS) / PACIFICO	8529,038	5,07%	5
ASIA (PAISES EMERGENTES) / PACIFICO	4605,337	2,74%	6
AMERICA LATINA	**4080,024**	**2,42%**	**7**
EUROPA (ESTE)	2752,803	1,64%	8
ORIENTE MEDIO Y NORTE DE ÁFRICA	2509,323	1,49%	9
AFRICA SUB-SAHARIANA	1485,975	0,88%	10
TOTAL	**168338,7**	**100,00%**	

Aunque en estos momentos es una región que está por debajo de la media en este *ranking*, también es cierto que tiene una **brillante proyección de futuro** y un crecimiento proyectado hasta el 2027 que la hace una región muy activa en ciberseguridad, abierta a la hora de **hacer nuevas inversiones y expansión del mercado**. Los países mejor posicionados en el *ranking* de 50 países con más consumo de ciberseguridad (representado parcialmente antes en la Figura 7), se pueden ver en la Tabla 4.

Tabla 4. Países latinoamericanos mejor posicionados en el ranking de 50 países con más gasto en ciberseguridad. Datos: [1]. Análisis: INCIBE

PAISES. GASTO MILLONES $.	2022R	CUOTA	*RANKING*
USA	79.773,22	47,39%	1
JAPÓN	11.213,44	6,66%	2
REINO UNIDO	10.307,22	6,12%	3
ALEMANIA	7.702,31	4,58%	4
CHINA	6.824,90	4,05%	5
CANADA	5.400,86	3,21%	6
FRANCIA	5.335,85	3,17%	7
AUSTRALIA	4.345,25	2,58%	8
ITALIA	2.603,08	1,55%	9
INDIA	2.461,89	1,46%	10
COREA DEL SUR	2.450,64	1,46%	11
HOLANDA	2.384,39	1,42%	12
ESPAÑA	**2.047,97**	**1,22%**	**13**
SUIZA	1.857,79	1,10%	14
RESTO DE EUROPA DEL ESTE	1.528,93	0,91%	15
BRASIL	**1.425,44**	**0,85%**	**16**
SUECIA	1.371,21	0,81%	17
MÉXICO	**1.305,00**	**0,78%**	**18**
SINGAPUR	1.187,77	0,71%	19
…			
RESTO LATINOAMÉRICA	**847,20**	**0,50%**	**24**
AUSTRIA	809,37	0,48%	25
…			
CHILE	**207,74**	**0,12%**	**44**

COLOMBIA	**196,44**	**0,12%**	**45**
HUNGRÍA	152,39	0,09%	46
TURQUÍA	142,94	0,08%	47
ARGENTINA	**98,21**	**0,06%**	**48**

Aunque todos los países latinoamericanos dentro de este *ranking* tienen un gasto inferior al 1% mundial, se puede comprobar que **Brasil** y **México** (los mejor posicionados) se encuentran relativamente cerca de esta cota. Además, el consumo de ciberseguridad agregado del resto de países latinoamericanos (excepto **Chile**, **Colombia** y **Argentina**), como por ejemplo Perú y Uruguay, aparece en la zona media del *ranking*.

Si, como en la sección anterior, seleccionamos ahora **solo los países de esta región** dentro del *ranking*, y los ordenamos por gasto (Tabla 5), podemos comprobar que **Brasil y México tienen más de la mitad del gasto de la región total**, lo que los convierte en dos de los países más avanzados y por tanto más proclives a expandirse y crecer en otras regiones, como la de Europa Oeste que describimos antes.

Tabla 5. Gasto de países destacados en la región de Latinoamérica. Datos: [1]. Análisis: INCIBE

LATINOAMÉRICA GASTO MILLONES $	2022R	CUOTA	*RANKING*
BRASIL	1.425,44	37,34%	1
MÉXICO	1.305,01	28,96%	2
RESTO DE LATINOAMÉRICA	847,20	19,96%	
CHILE	207,75	5,33%	3
COLOMBIA	196,44	4,94%	4
ARGENTINA	98,21	3,46%	5
TOTAL	**4.080,05**	**100,00%**	

Por otro lado, como decíamos al principio de este apartado, Latinoamérica es un mercado **floreciente** de ciberseguridad y en expansión, y las proyecciones de Gartner hasta el 2027 dan un gasto total de la región en temas de ciberseguridad de **6.348,99 millones de dólares**. Esto supone un incremento global de un **55%**, y que situaría a esta región muy por encima de la siguiente en el *ranking* de 50 países visto antes.

La Figura 12 detalla más este crecimiento y expansión proyectado. **Brasil (+62%) y México (+47%)** siguen concentrando más de la mitad del gasto en la región, pero cabe destacar que otros países (que ahora tienen mucha menos cuota) adquirirán un porcentaje mayor, al tener una proyección **de incremento de gasto mayor que los dos anteriores** (Ej.: Chile con un **107%** y Colombia con un **75%** de incremento).

En lo relativo al resto de países agrupados por Gartner, también es importante destacar que tienen proyectada una tasa de crecimiento muy significativa (**+53%**), volviendo a dejar patente que la región **Latinoamérica es un mercado en plena expansión**.

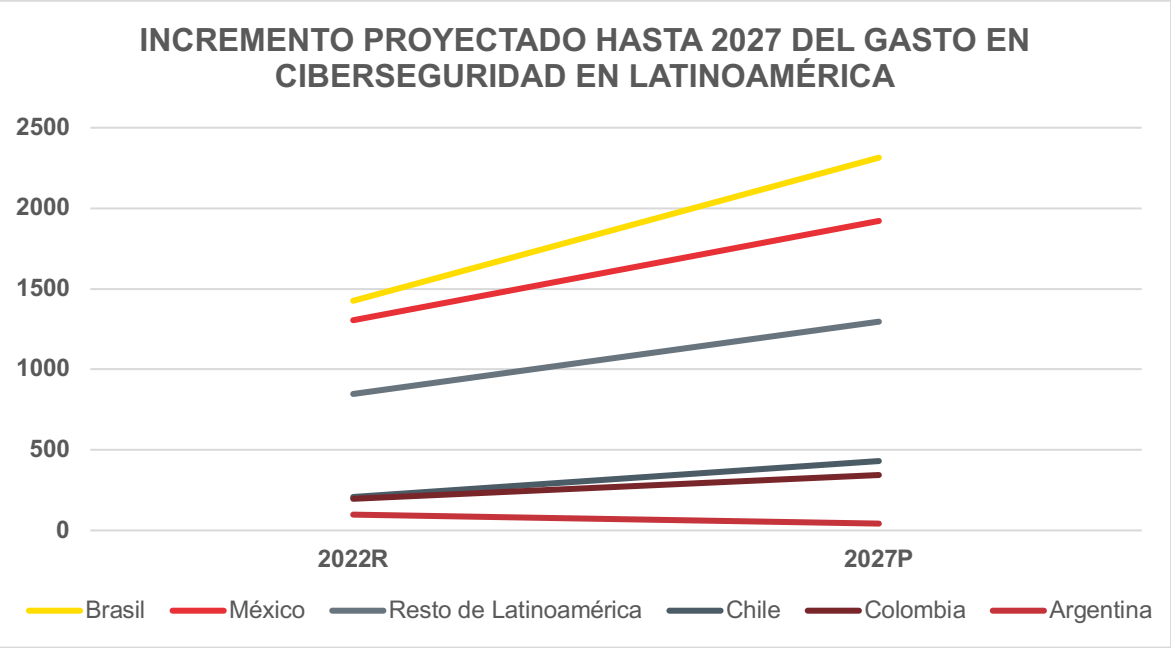


Figura 12. Gasto proyectado por países destacados de la región de Latinoamérica en 2027. Datos: [1]. Análisis: INCIBE

Nuevamente, si **dividimos el gasto por tipo de solución** de los países de la región Latinoamérica, usando la misma clasificación que en la sección anterior (Tabla 6), vemos que los **servicios de seguridad**, seguidos de lejos por el **equipamiento de seguridad en red** y la **protección de la infraestructura,** son las áreas en las que hay más gasto. Esta **es la misma distribución del gasto** que pudimos ver en el caso de España (ver Tabla 2), lo cual deja claro que hay una **sinergia** en las áreas en las que las empresas de ambas regiones invierten, que puede ser de ayuda para una futura expansión del mercado en España y Europa Oeste.

Tabla 6. Gasto en ciberseguridad en países latinoamericanos por tipo de solución Datos: [1]. Análisis: INCIBE

LATINOAMERICA GASTO MILLONES DE $	2022R	CUOTA	2027P	CUOTA
Servicios de seguridad	1.478,82	36,25%	1.994,50	31,41%
Protección de infraestructura	627,43	15,38%	964,33	15,19%
Equipamiento de seguridad en red	554,44	13,59%	932,05	14,68%
Gestión de identidades	511,75	12,54%	756,46	11,91%
Software de Seguridad para el consumidor	446,15	10,93%	662,97	10,44%
Seguridad en nube	142,80	3,50%	384,92	6,06%
Seguridad de Aplicaciones	100,78	2,47%	262,37	4,13%
Manejo integrado de riesgos	88,70	2,17%	197,76	3,11%
Seguridad de datos	77,67	1,90%	106,32	1,67%
Otro software de seguridad de la información	33,08	0,81%	50,04	0,79%
Privacidad de datos	18,41	0,45%	37,29	0,59%
TOTAL	**4.080,03**	**100,00%**	**6.349,01**	**100,00%**

Por tanto, vemos que la región latinoamericana **tiene un futuro muy prometedor** proyectado en ciberseguridad y que, por tanto, la expansión de su mercado a la segunda región del *ranking* en cuanto a consumo en ciberseguridad (Europa Oeste) y, más concretamente, al segundo país de dicha región en madurez (España), que además **elimina la barrera del idioma,** es una vía muy atractiva para abrir su mercado y encontrar nuevas oportunidades de negocio.

1.3.2. Ámbito regulatorio, legislativo, administrativo y de oferta y demanda en diferentes países latinoamericanos

1.3.2.1. Análisis comparativo con España según el *ranking* ITU GCI 2020

Gracias al análisis hecho por el *ranking* ITU GCI 2020 a 194 países de todo el mundo usado anteriormente, podemos también hacer un **análisis comparativo de los países latinoamericanos con España** empleando los mismos elementos y dominios (descritos en la Figura 10). En esta sección vamos a usar este análisis para destacar la **puntuación global** en el *ranking*, su **posicionamiento** (que se basa en al ámbito regulatorio y organizativo de cada país) y la **presencia de CSIRT/CERT** en cada país.

¿Qué es exactamente un CSIRT? significa *Computer Security Incident Response Team* y es un equipo de personas dedicado a **la implantación y gestión de medidas tecnológicas** con el objetivo de **mitigar el riesgo** de ataques contra los sistemas de la comunidad a la que se proporcionan ese servicio [5]. El término CSIRT suele emplearse en Europa en lugar del término protegido CERT, registrado en EE.UU.

1.3.2.1.1. Argentina

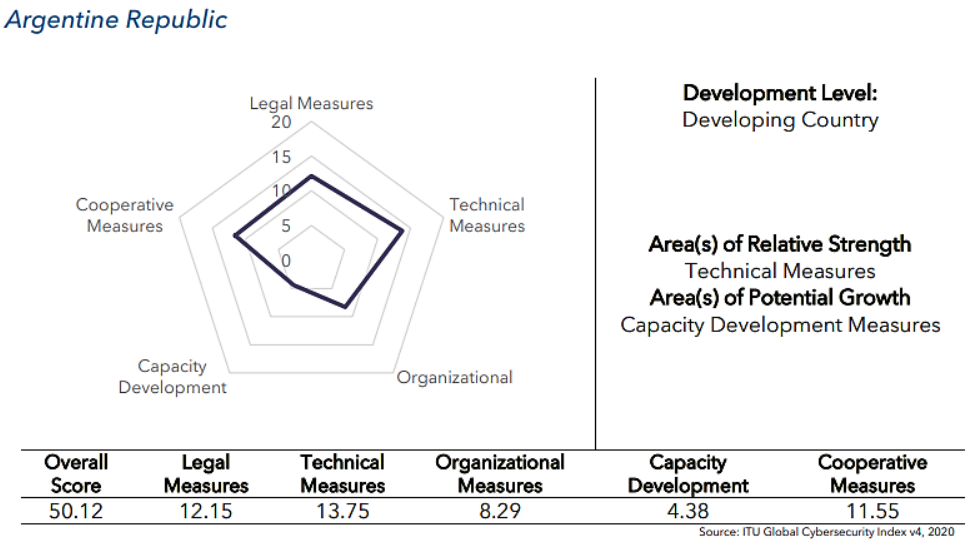
De acuerdo con [6], a pesar del crecimiento de su mercado local, la implementación de la seguridad cibernética en Argentina **todavía se encuentra en su etapa inicial de madurez** (algo que refleja también el estudio de la OEA en la sección siguiente). El crecimiento se ve obstaculizado por las constantes **fluctuaciones del tipo de cambio** y la **devaluación** del peso, lo cual podría explicar parcialmente es estancamiento de crecimiento proyectado hasta 2027 del país observado en la Figura 12.

No obstante, la concienciación de la sociedad y la empresa argentina ha aumentado significativamente dados los problemas que causa el cibercrimen. Argentina se encuentra dentro del grupo de países en Latinoamérica que cuentan con una **Estrategia Nacional de Ciberseguridad** (ver Figura 21) desde 2019.

En los últimos años, se han tomado numerosas medidas para **implementar políticas y realizar cambios administrativos y regulatorios** que han afectado de manera positiva. Además de la Estrategia Nacional de Ciberseguridad mencionada, se implementaron también **políticas** relativas a la seguridad de los datos personales y la **buena praxis** en el uso de las TIC.

También ha desarrollado una **oferta educativa** para su población en estos aspectos. Varias las universidades ofrecen una **educación en seguridad cibernética**. Por otra parte, el Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires (BA-CSIRT) también da la oportunidad mediante charlas de sensibilización sobre seguridad cibernética y el uso de las TIC.

En relación con los **CSIRT**, Argentina cuenta con **seis** [7]. Según el *ranking* ITU, ocupa la **posición 91** con una **puntuación de 50,12/100**. Como puede apreciarse en la Figura 13, el punto fuerte de Argentina son las **medidas técnicas y legales**, que destacan sobre las demás, fruto del trabajo hecho en esta vía que mencionábamos antes. El carácter de país en desarrollo en materia de ciberseguridad se ve fundamentalmente en los aspectos **organizacionales** y de **desarrollo de capacidades**.



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
50.12	12.15	13.75	8.29	4.38	11.55

Source: ITU Global Cybersecurity Index v4, 2020

Figura 13. Desglose de la puntuación de Argentina en el ranking ITU GCI 2020

1.3.2.1.2. México

Según [8] México es un país **con un largo camino por delante** en materia de ciberseguridad. Cuenta con una elevada tasa de ataques del cibercrimen y **medidas e iniciativas insuficientes contra ellos en estos momentos**, tanto públicas como privadas.

En lo referente al grado de digitalización de la economía mexicana, las TIC se encuentran en una fase de **adopción acelerada**, aunque lejos aún del nivel de desarrollo de los países de Europa Occidental o América del Norte.

No obstante, México es el **segundo país con mayor penetración digital** de América Latina, solo por detrás de Brasil. El porcentaje de usuarios de Internet en el país en 2019 fue del 70,1 %, por un 90,7% de España, fundamentalmente debido al uso de teléfonos inteligentes. La media de crecimiento anual del 2014 al 2019 fue de un 5,1 %.

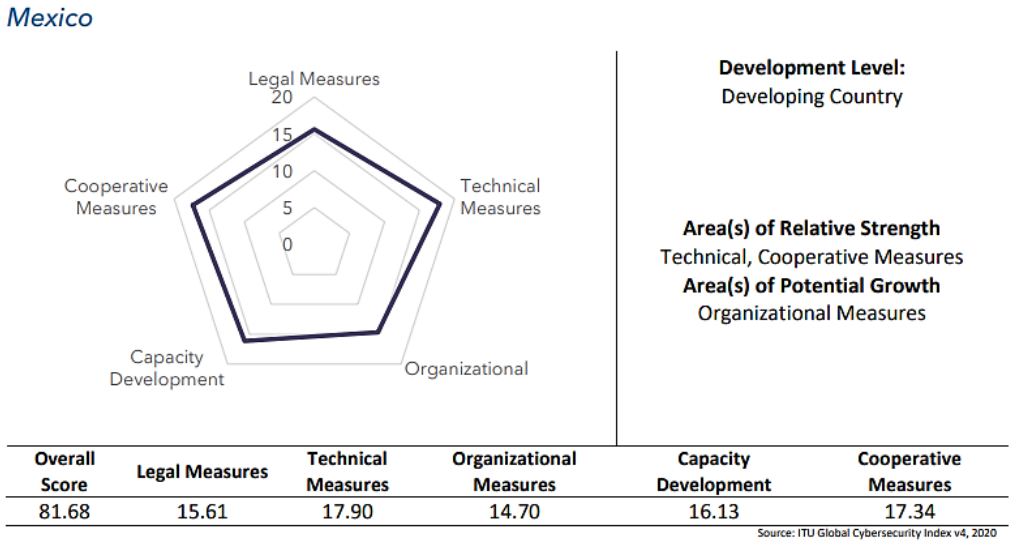
El **comercio electrónico** también ha experimentado un considerable desarrollo en los últimos años, creciendo un 28,6 % en 2019 respecto al año anterior, por encima de la media mundial, de un 20,7%.

México elaboró en 2017 su **Estrategia Nacional de Ciberseguridad** con el objetivo de fortalecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político, y de definir objetivos estratégicos para los diferentes actores implicados.

No obstante, el país sigue teniendo por delante **un largo camino en materia de regulación de ciberseguridad**, ya que la legislación al respecto es escasa. Uno de los problemas a los que se enfrenta el sistema es la **limitada coordinación** entre organismos

públicos y privados. Estos puntos débiles se reflejan claramente en el análisis hecho por la ITU (ver Figura 14).

Hoy en día, no existen exigencias en cuanto a medidas de seguridad cibernética, ni las organizaciones están obligadas a informar sobre incidentes a las autoridades, lo que hace que la recolección de estadísticas sobre ciberataques sea muy difícil y el país se considere **en desarrollo** en materia de ciberseguridad por la ITU. Con todo ello, el país se encuentra en el **puesto 52 en el *ranking* de la ITU,** con una puntuación de **81,68/100** (Figura 14). Además, cuenta con **3 CSIRT** [7].



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
81.68	15.61	17.90	14.70	16.13	17.34

Source: ITU Global Cybersecurity Index v4, 2020

Figura 14. Desglose de la puntuación de México en el ranking ITU GCI 2020

1.3.2.1.3. Brasil

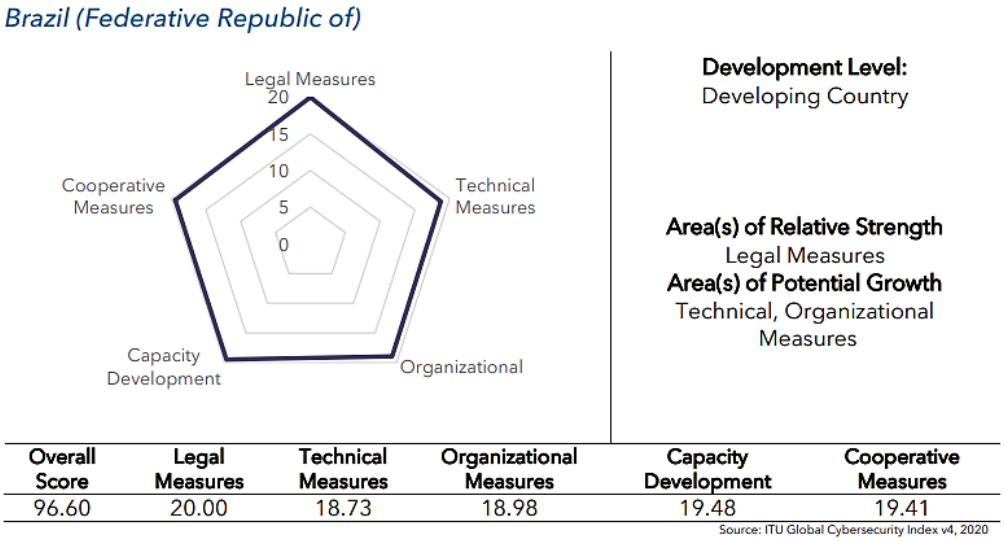
Según [9], el 83 % de los domicilios del país cuentan con conexión a Internet en 2022. No obstante, según el informe de 2021 *Internet Organised Crime Threat Assessment* (IOCTA) de la Europol, "***la falta de una legislación adecuada*** *en materia de ciberdelincuencia ha convertido a Brasil en el primer objetivo y la principal fuente de ataques en línea en América Latina; el 54 % de los ciberataques denunciados en Brasil se habrían originado en el país*".

Este documento continúa diciendo que "*al igual que Estados Unidos, Brasil es un* ***importante anfitrión de sitios web de phishing****, y algunos informes sitúan a Brasil como una de las diez principales fuentes de ciberataques del mundo*". Esta panorámica de **auge de la ciberdelincuencia** en el país causa que la ciberdelincuencia provoque pérdidas anuales en el país por valor de 20.000 millones de € y que sea un país con una muy elevada tasa de víctimas de *phishing* y *ransomware*

La madurez del país en estos aspectos se ha visto **impulsada recientemente a través de cambios legislativos** y por los efectos de la COVID-19 pero, en general, la mayor parte de los sectores de la economía necesitan ampliar medidas de ciberseguridad, más aún tras la **aprobación de la LGPD, de obligado cumplimiento**.

No obstante, todo este impulso a la mejora de la ciberseguridad del país, tan necesario por el índice de cibercriminalidad tan elevado que presenta, hace que el país ahora mismo se sitúe en el ***ranking*** **18 en la ITU** con una puntuación de **96,60/100** (Figura 15), sólo por detrás de EEUU y Canadá en la región de América (ver Figura 20). No obstante, el margen

de mejora aún es alto, algo que se refleja en que solo hay constancia de **un CSIRT** en el país [7] y que el ITU lo considera un país en vías de desarrollo en materia de ciberseguridad.



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
96.60	20.00	18.73	18.98	19.48	19.41

Source: ITU Global Cybersecurity Index v4, 2020

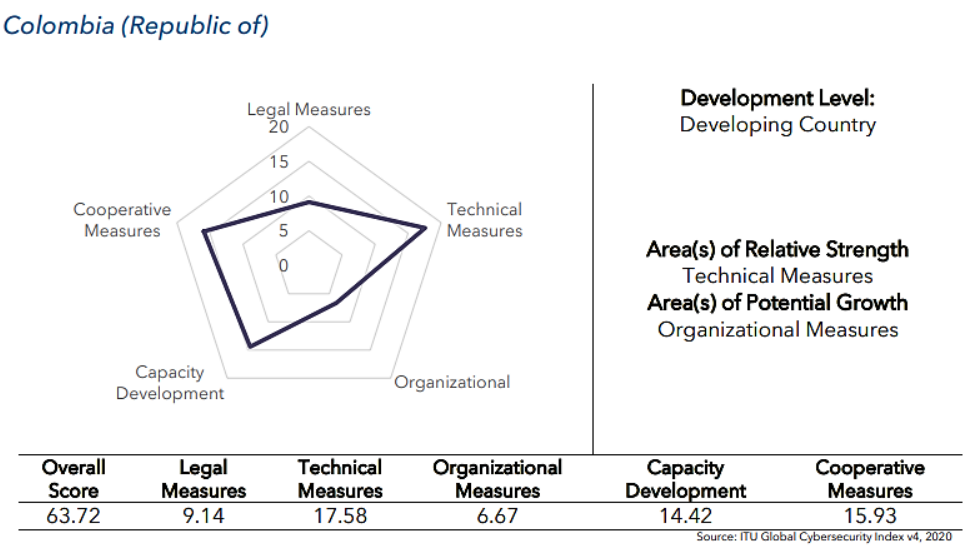
Figura 15. Desglose de la puntuación de Brasil en el ranking ITU GCI 2020

1.3.2.1.4. Colombia

Según [10], Colombia es uno de los países de Latinoamérica **en pleno crecimiento** de la transformación digital y penetración de Internet. A causa de ello, el nivel de ataques cibernéticos a los que se ha sometido también ha crecido considerablemente. Es el segundo país de la región con más incidentes de ciberseguridad hasta agosto de 2021.

El sector de la ciberseguridad colombiano se divide en dos categorías principales: **desarrollo de *software* y *hardware* y servicios**. La mayor fortaleza de Colombia es en la aplicación de las capacidades técnicas a través de los organismos nacionales y sectoriales. El país tiene **6 CSIRTs** en estos momentos [7], siendo uno de los países de la región de América Latina **con mayor nº de ellos**. Gracias a su trabajo el país cuenta con mecanismos de notificación para la protección de la infancia en línea, por ejemplo.

No obstante, Colombia debe mejorar aún **en medidas organizativas y legales**: legislación sobre ciberseguridad, normativa de protección de datos y sobre infraestructuras críticas, como se aprecia claramente en la Figura 16. Por todo ello, la ITU lo considera un país en vías de desarrollo en materia de ciberseguridad, ocupando la **posición 81** en el *ranking* de la ITU con una puntuación de **63,72/100**.



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
63.72	9.14	17.58	6.67	14.42	15.93

Source: ITU Global Cybersecurity Index v4, 2020

Figura 16. Desglose de la puntuación de Colombia en el ranking ITU GCI 2020

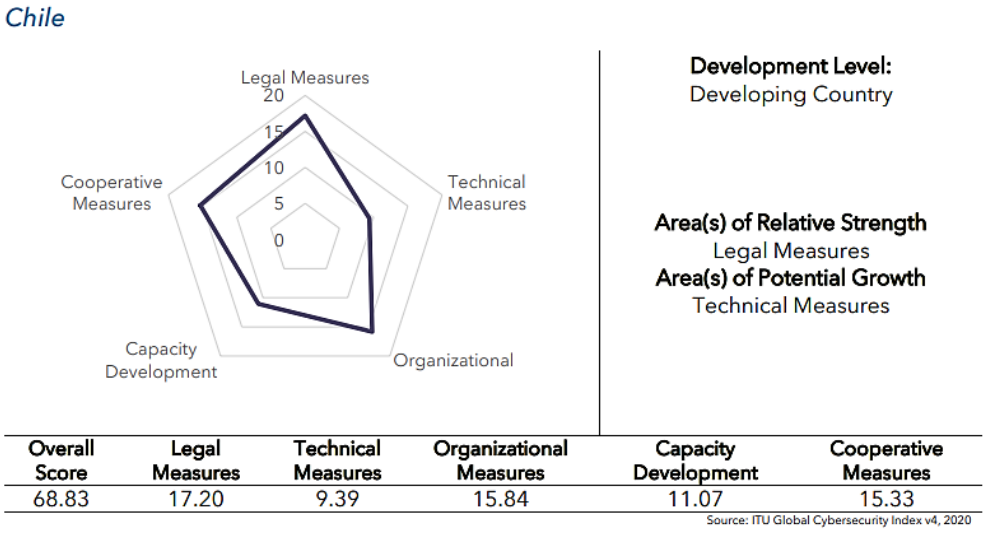
1.3.2.1.5. Chile

Según [11], en Chile el sector de la ciberseguridad es un **mercado en crecimiento**, con una inversión creciente en los últimos años. El país creó hace pocos años su Política Nacional de Ciberseguridad (PCNS) como instrumento público para la mejora del país en este aspecto. Con ella, se pretende crear una **estrategia completa** que se desarrolle a lo largo de los años frente a los ciberataques que se vayan produciendo contra el país.

Los **ciberdelitos** en Chile han aumentado también en los últimos años, dada su elevada tasa de penetración de Internet y su economía estable. Por ello, la ciberseguridad es el sector con **mayor previsión de crecimiento** en las empresas chilenas.

No obstante, Chile aún tiene un margen de mejora grande en temas de **colaboración público-privada**, existiendo un déficit de información en cuanto al estado de la seguridad en el sector público o privado del país. Con la creación del PCNS se pretende crear una **cultura de ciberseguridad** en el país, y también hay **iniciativas educativas** en forma de grados y postgrados en esta temática.

En estas circunstancias, el país ocupa la **posición 74** en el *ranking* ITU, con una puntuación de **68,83/100**, teniendo además operativo **1 CSIRT** [7]. La ITU lo considera un país en vías de desarrollo en materia de ciberseguridad (Figura 17).



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
68.83	17.20	9.39	15.84	11.07	15.33

Source: ITU Global Cybersecurity Index v4, 2020

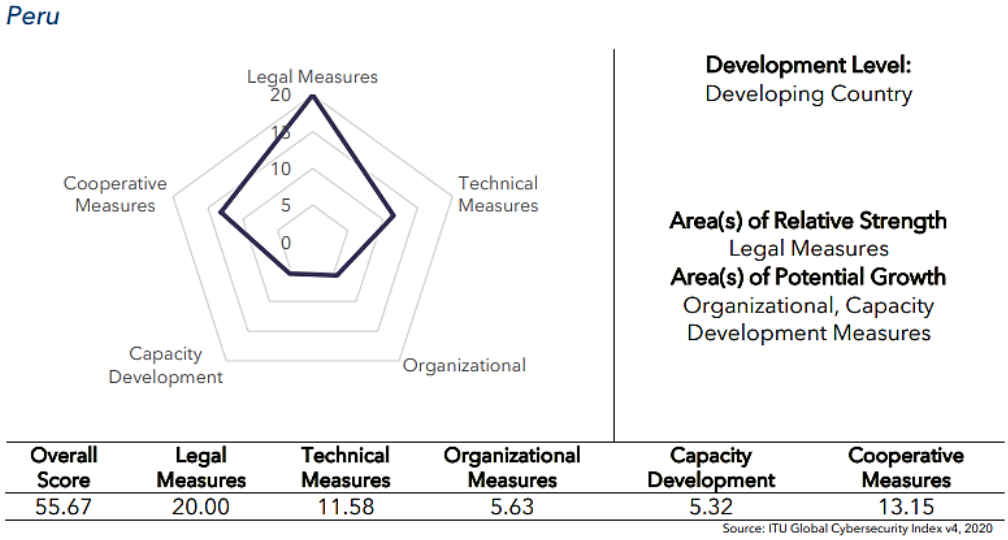
Figura 17. Desglose de la puntuación de Chile en el ranking ITU GCI 2020

1.3.2.1.6. Perú

Según [12], Perú invierte el 0,12% de su PIB en seguridad informática, cifra **mucho menor** de lo que destinan sus países vecinos. Las empresas peruanas invierten por lo general la mitad de lo que dedican sus homólogas en países de la región, siendo el sector financiero el que más fondos dedica a esta materia.

Esta menor inversión en ciberseguridad no se debe a una falta de interés en el sector, sino a que **la economía peruana está aún en proceso de digitalización**. Actualmente, se está trabajando en impulsar distintas iniciativas que eleven el nivel de innovación del país. Fruto de ello es el incremento del uso de la nube, tanto en el entorno corporativo como estatal, el aumento del número de servicios online que el gobierno ofrece y diversos cambios en el marco legal.

En la actualidad Perú cuenta con **3 CSIRT** [7] y ocupa el **puesto 86** en el *ranking* de la ITU con una puntuación de **55,67/100** (Figura 18), penúltimo país entre los analizados solo por delante de Argentina (Tabla 7), siendo un país en vías de desarrollo en materia de ciberseguridad.



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
55.67	20.00	11.58	5.63	5.32	13.15

Source: ITU Global Cybersecurity Index v4, 2020

Figura 18. Desglose de la puntuación de Perú en el ranking ITU GCI 2020

1.3.2.1.7. Uruguay

Según [13], Uruguay cuenta con un **marco de ciberseguridad** basado en estándares internacionales para la mejora de la seguridad cibernética de la infraestructura crítica y las organizaciones públicas, aunque no sea una estrategia nacional de seguridad cibernética como las destacadas en la Figura 21.

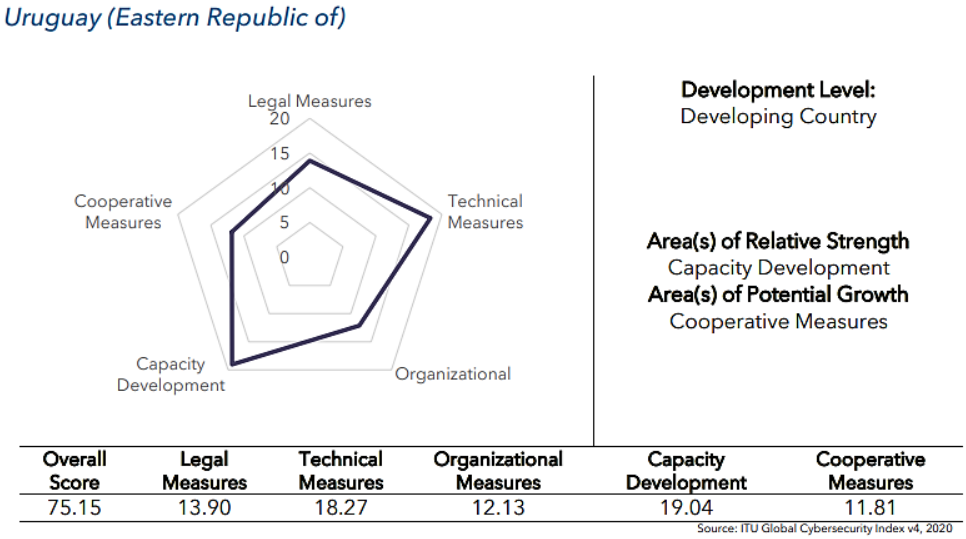
El país tiene además **2 CSIRT** [7] y proyectos para el fortalecimiento de la ciberseguridad a nivel nacional. El país posee proveedores de servicios de seguridad cibernética, y parece haber una buena **conciencia general** sobre el tema en el sector privado. No obstante, es el gobierno el que parece estar brindando más servicios de seguridad cibernética y capacitación.

En este sentido, el gobierno ofrece **cursos de seguridad y defensa cibernéticas**, que están disponibles para participantes del sector público y privado. Además, tiene una serie de **guías y buenas prácticas**, que proporcionan recursos para cualquiera que quiera estar más informado sobre seguridad cibernética. De manera conjunta, hay varias universidades que ofrecen capacitaciones y cursos sobre seguridad cibernética.

Con respecto al **marco legal y regulatorio**, hay algunos proyectos de ley para la protección contra los delitos cibernéticos. Por otro lado, el país cuenta con **legislación sobre la protección de datos personales y privacidad**, que se aplica a las bases de datos de los sectores público y privado.

Uruguay ha establecido también su Plan de Gobierno Electrónico 2020, cuyo objetivo es crear valor público a través de servicios que satisfagan las necesidades, expectativas y preferencias de los ciudadanos. Además, el gobierno electrónico se incluyó en la Agenda Digital 2020 del país, como parte del pilar relativo a la innovación de la relación entre el gobierno y sus ciudadanos.

Con todo ello, el país ocupa la **posición 64** en el *ranking* de la ITU, con una puntuación de **75,15/100** (Figura 19), siendo categorizado como país en vías de desarrollo en materia de ciberseguridad.



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
75.15	13.90	18.27	12.13	19.04	11.81

Source: ITU Global Cybersecurity Index v4, 2020

Figura 19. Desglose de la puntuación de Uruguay en el ranking ITU GCI 2020

1.3.2.1.8. Análisis global

En las secciones anteriores hemos mencionado la puntuación y el *ranking* de los países latinoamericanos analizados por la ITU en la clasificación mundial. No obstante, también es importante ver el ***ranking* dentro de la región** en la que estos países se encuadran (**América**), lo que aparece en la Figura 20. Vemos claramente como **Brasil es el único de los países analizados que alcanza una puntuación próxima a EEUU** y **Canadá**, principales exponentes de esta región.

Table 5: GCI results: Americas region

Country Name	Overall Score	Regional Rank
United States of America**	100	1
Canada**	97.67	2
Brazil	96.6	3
Mexico	81.68	4
Uruguay	75.15	5
Dominican Rep.	75.07	6
Chile	68.83	7
Costa Rica	67.45	8
Colombia	63.72	9
Cuba	58.76	10
Paraguay	57.09	11
Peru	55.67	12
Argentina	50.12	13
Panama	34.11	14
Jamaica**	32.53	15
Suriname	31.2	16
Guyana	28.11	17
Venezuela	27.06	18
Ecuador	26.3	19

Figura 20. Ranking por países en la región de América según el ranking ITU GCI 2020

Es importante destacar también cuantos de los países de los analizados tienen ya establecida **una estrategia nacional de seguridad**, como en el caso de España. Si atendemos a las indicaciones del *ranking* ITU (Figura 21), **sólo Perú carece de dicha estrategia** entre los países analizados en este informe, lo cual puede explicar que sea el país que acaba en las últimas posiciones tanto en este *ranking* como en el que analizaremos en la sección siguiente.

Figura 21. Países Latinoamericanos con una Estrategia Nacional de Ciberseguridad según el ranking ITU GCI 2020

Como decíamos antes, la principal ventaja del *ranking* ITU es que **podemos comparar los países analizados con España** con un conjunto de criterios común (Tabla 7). Vemos **como Brasil es el único país que obtiene puntuaciones muy similares a España** en todos los apartados. Ambos países alcanzan puntuaciones idénticas en los apartados **Legal** y **Organizacional**, aunque hay una gran distancia entre ambos en el *ranking* de países a nivel mundial.

La tabla permite ver claramente los puntos fuertes de cada país respecto a España y, por tanto, **dónde sería más probable** que empresas especializadas en esas áreas de los países latinoamericanos analizados pueden **aportar ideas innovadoras** si desembarcan en el mercado europeo. Por ejemplo, **Brasil** tiene unas puntuaciones comparables en todos los apartados a España, mientras que **México** destaca más en los aspectos **Técnicos** y de **Cooperación**.

Uruguay se muestra más fuerte también es aspectos **Técnicos** y de **Desarrollo de capacidades**, mientras **Chile** (en el aspecto **Legal**) y **Colombia** (en el aspecto **Técnico**) tienen una fortaleza próxima a los valores evaluados por España. Finalmente, **Perú** destaca sobre todo en su aspecto **Legal**.

No obstante, esta conclusión debe tomarse como una probabilidad y no como un hecho. Aunque alcance puntuaciones sustancialmente más bajas que España en alguno de los cinco dominios analizados, no quiere decir que una empresa especializada en ellos no pueda aportar valor innovador en España (y, a través de ella, en países europeos a los que podrá acceder más fácilmente posteriormente).

Ha de tenerse en cuenta que este análisis es algo global, y no refleja de una forma directa o inmediata la existencia de empresas y polos de innovación en un aspecto concreto, aunque el país en sí tenga una valoración baja en el mismo. Por otro lado, **el acceso al mercado europeo** permite trabajar a países latinoamericanos con países de la región Europa Oeste que estén menos desarrollados en alguno de estos aspectos, aportando valor y encontrando nuevas vías de expansión de mercado.

Otro aspecto es que la introducción de *start-ups* latinoamericanas en España y Europa también podría servir para **lograr un experiencia y aprendizaje** en determinados aspectos colaborando con empresas del país de destino. Esta colaboración puede **revertir luego en una mejora en la madurez de estos aspectos en el país de origen de la empresa**, lográndose un efecto positivo "de vuelta" por esta vía.

Tabla 7. Resumen de los aspectos Latinoamericanos analizados vs España. Datos: [3]. Análisis: INCIBE

	España	Brasil	México	Uruguay	Chile	Colombia	Perú	Argentina
Legal	**20,00**	**20,00**	15,61	13,90	17,20	9,14	**20,00**	12,15
Técnico	19,54	18,73	17,90	18,27	9,39	17,58	11,58	13,75
Organizacional	18,98	18,98	14,70	12,13	15,84	6,67	5,63	8,29
Desarrollo de capacidades	**20,00**	19,48	16,13	19,04	11,07	14,42	5,32	4,38
Cooperación	**20,00**	19,41	17,34	11,81	15,33	15,93	13,15	11,55
TOTAL	**98,52**	**96,60**	**81,68**	**75,15**	**68,83**	**63,74**	**55,68**	**50,12**
Nº CSIRTs	17	1	3	2	1	6	3	6
***Ranking* ITU 2020**	4	18	52	64	74	81	86	91

Por último, cabe destacar la **gran diferencia en el nº de CSIRT** presentes en España [14] frente a los presentes los países latinoamericanos estudiados, existiendo una gran ventaja en España en este aspecto.

1.3.2.2. Análisis comparativo entre países Latinoamericanos según la OEA

Para entender mejor el nivel de madurez de los países latinoamericanos analizados en la sección anterior, vamos a hacer un análisis **complementario** de dichos países usando los **criterios establecidos por la OEA** en [15]. De esta forma, este informe quiere ofrecer un análisis del estado de la ciberseguridad de los países analizados más completo, al analizarlos desde dos puntos de vista diferentes.

El estudio de la OEA está **centrado únicamente en países Latinoamericanos**, y usa unos **criterios alternativos a los vistos en la ITU** en la sección anterior. La evaluación de los niveles de madurez de ciberseguridad se divide en **cinco dimensiones**, que son aspectos esenciales y específicos de la misma:

- **D1: Política y estrategia de ciberseguridad**
- **D2: Cultura cibernética y sociedad**
- **D3: Educación, capacitación y habilidades en ciberseguridad**
- **D4: Marcos legales y regulatorios**
- **D5: Estándares, organizaciones y tecnologías.**

Cada dimensión se subdivide en un conjunto de **factores** que describen y definen lo que significa poseer capacidad de seguridad. Estos factores indican **cómo mejorar la madurez** de cada país en cada dimensión. En las secciones siguientes dedicadas a cada dominio, se muestran tablas por países que detallan los factores concretos que subdividen cada dimensión (las filas que aparecen **en negrita**). Cada factor puede contemplar varios **aspectos más concretos**, que también aparecen en dichas tablas **en cursiva**.

El modelo de la OEA busca ofrecer directamente **una evaluación del nivel de madurez** de las capacidades de ciberseguridad de los países latinoamericanos, asignándoles una **etapa de madurez**. Cada etapa corresponde a su grado de logro en materia de ciberseguridad.

Hay **cinco etapas de madurez** que se fijan por medio de una evaluación. Estas van desde la más básica (**inicial**) hasta la más avanzada (**dinámica**). En las tablas que estudian a cada país que veremos después aparecerán numeradas del 1 (**Inicial**) al 5 (**Dinámica**). Esto permite situar numéricamente a cada país en cada una de esas etapas, y por tanto valorar fácilmente y comparar en que punto está en cada apartado, y cuando le queda por avanzar en el futuro. La definición de las etapas es la siguiente:

1. **Inicial**: **No existe madurez en ciberseguridad** o se encuentra en un estadio muy embrionario. Puede haber discusiones iniciales sobre el desarrollo de capacidades de ciberseguridad, pero **no se han tomado medidas concretas**. También faltan evidencias observables de las capacidades de seguridad cibernética.
2. **Formativa**: Algunos aspectos de ciberseguridad **han comenzado a crecer y formularse**, pero pueden ser ad hoc, desorganizados, mal definidos, o simplemente nuevos. Sin embargo, se puede demostrar claramente la existencia de evidencias de este aspecto.
3. **Consolidada**: Los indicadores están **instalados y funcionando**. Sin embargo, no se le ha dado mucha consideración a la **asignación de recursos**. Se han tomado pocas decisiones acerca de los beneficios con respecto a la inversión relativa en este aspecto, pero la etapa **es funcional y está definida**.
4. **Estratégica**: En esta etapa se han tomado decisiones sobre qué indicadores de este aspecto **son importantes y cuáles lo son menos** para la organización o el Estado en particular. Refleja el hecho de que estas elecciones se han realizado condicionadas por las circunstancias particulares de ambas entidades.
5. **Dinámica**: En esta etapa existen **mecanismos claros** para alterar la estrategia en **función de las circunstancias prevalentes**, como la sofisticación tecnológica del entorno de amenaza, el conflicto global o un cambio significativo en un área de preocupación. Las organizaciones dinámicas han desarrollado **métodos para cambiar las estrategias** con calma. Sin embargo, se habilita la toma de decisiones

rápida, la reasignación de recursos y la atención constante al entorno cambiante de la ciberseguridad.

1.3.2.2.1. Política y Estrategia de Seguridad Cibernética

Esta dimensión contempla el diseño de **estrategia y resiliencia de ciberseguridad** de cada país analizado. La Figura 22 y la Tabla 8 muestran la madurez de cada uno de los países estudiados en este aspecto. El **valor medio de cada factor** dentro de la dimensión ha sido calculado mediante la **media aritmética de sus aspectos más concretos**, por estar más fuertemente vinculados entre ellos. **El valor medio final de la dimensión** para cada país, por contemplar factores más diversos entre ellos, se ha calculado **usando la media geométrica de la media de sus factores**.

Tabla 8. Análisis del dominio D1 de los países latinoamericanos estudiados según la OEA. Datos: [15]. Análisis: INCIBE

D1: POLÍTICA Y ESTRATEGIA DE SEGURIDAD CIBERNÉTICA

		Argentina	México	Brasil	Colombia	Chile	Perú	Uruguay
1-1	**Estrategia Nacional de Seguridad Cibernética ($\bar{X}$)**	**2,33**	**2,67**	**2,00**	**4,33**	**3,33**	**1,67**	**3,67**
	Desarrollo de la Estrategia	2	3	2	5	4	2	4
	Organización	3	2	2	4	3	2	4
	Contenido	2	3	2	4	3	1	3
1-2	**Respuesta a Incidentes ($\bar{X}$)**	**3,00**	**3,25**	**3,75**	**3,75**	**2,75**	**1,75**	**4,50**
	Identificación de Incidentes	4	4	4	3	3	2	4
	Organización	3	3	4	4	3	2	5
	Coordinación	3	3	4	4	2	2	5
	Modo de Operación	2	3	3	4	3	1	4
1-3	**Protección de la Infraestructura Crítica (IC) ($\bar{X}$)**	**2,00**	**2,00**	**3,00**	**3,67**	**2,00**	**1,67**	**2,67**
	Identificación	2	2	3	3	2	2	2
	Organización	2	2	3	4	2	2	3
	Gestión de Riesgos y Respuesta	2	2	3	4	2	1	3
1-4	**Manejo de Crisis ($\bar{X}$)**	**2,00**	**2,00**	**3,00**	**4,00**	**2,00**	**2,00**	**3,00**
	Manejo de Crisis	2	2	3	4	2	2	3
1-5	**Defensa Cibernética ($\bar{X}$)**	**2,00**	**2,67**	**2,67**	**3,33**	**2,67**	**2,00**	**3,00**
	Estrategia	2	4	3	4	3	2	3
	Organización	3	2	3	3	3	2	3
	Coordinación	1	2	2	3	2	2	3
1-6	**Redundancia de Comunicaciones ($\bar{X}$)**	**2,00**	**3,00**	**2,00**	**2,00**	**2,00**	**2,00**	**4,00**
	Redundancia de Comunicaciones	2	3	2	2	2	2	4
	Media geométrica	**2,20**	**2,55**	**2,67**	**3,42**	**2,41**	**1,84**	**3,41**

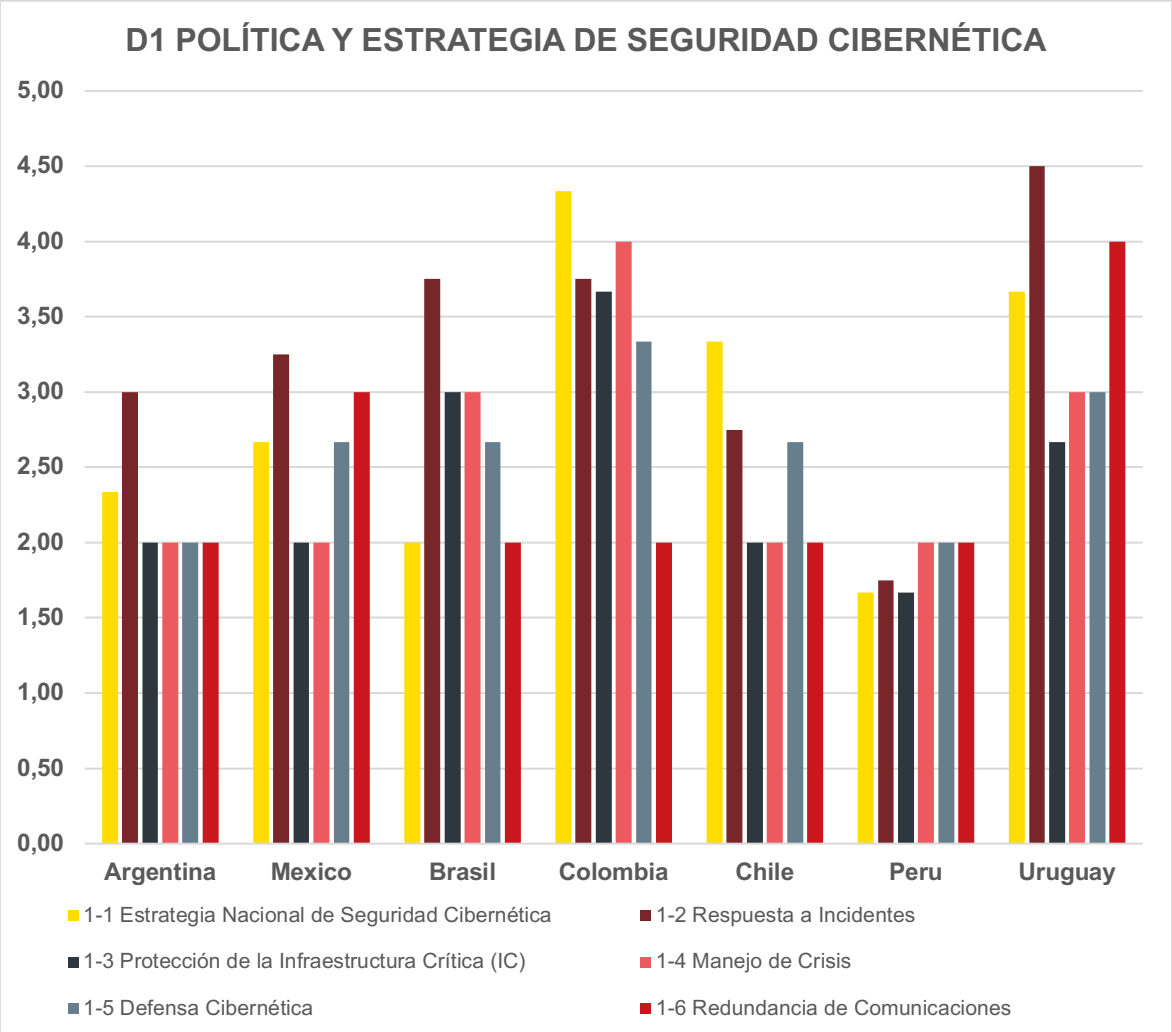


Figura 22. Gráfico comparativo entre países Latinoamericanos del dominio D1 del estudio de la OEA. Datos: [15]. Análisis: INCIBE

El análisis de los factores de la dimensión D1 revela que Uruguay y Colombia son los países que tienen un nivel de madurez medio superior al resto de países analizados en este aspecto. Ambos tienen esta dimensión claramente **consolidada** y con algunos de sus factores que ya se encuentran claramente en una etapa de madurez **estratégica**. El resto de los países analizados se encuentra aún en una fase de madurez **formativa**, salvo Perú, que aún se encuentra inmersa en una fase **Inicial,** aunque con claras muestras de estar cerca de pasar a la siguiente fase.

1.3.2.2.2. Cultura Cibernética y Sociedad

Este dominio estudia si cada país **hace un esfuerzo por fomentar una cultura de ciberseguridad** responsable en su sociedad. La Figura 23 y la Tabla 9 muestran la madurez de cada uno de los países estudiados en este aspecto. El análisis de valores medios de cada factor y finales se ha hecho **idéntico al de la dimensión D1**.

Tabla 9. Análisis del dominio D2 de los países latinoamericanos estudiados según la OEA. Datos: [15]. Análisis: INCIBE

D2: CULTURA CIBERNÉTICA Y SOCIEDAD

		Argentina	México	Brasil	Colombia	Chile	Perú	Uruguay
2-1	**Mentalidad de Seguridad Cibernética ($\bar{X}$)**	**2,33**	**3,00**	**2,33**	**3,00**	**3,00**	**2,33**	**3,67**
	Gobierno	2	3	2	4	3	2	5
	Sector Privado	3	3	3	2	3	3	3
	Usuarios	2	3	2	3	3	2	3
2-2	**Confianza y Seguridad en Internet ($\bar{X}$)**	**2,00**	**3,00**	**3,00**	**3,00**	**3,00**	**2,33**	**4,33**
	Confianza y Seguridad en el Internet del Usuario	2	3	3	3	3	2	4
	Confianza del Usuario en los Servicios de Gobierno Electrónico	2	3	3	3	3	2	5
	Confianza del Usuario en los Servicios de Comercio Electrónico	2	3	3	3	3	3	4
2-3	**Comprensión del Usuario de la Protección de Información Personal en Línea ($\bar{X}$)**	**2,00**	**2,00**	**2,00**	**2,00**	**3,00**	**2,00**	**4,00**
	Comprensión del Usuario de la Protección de Información Personal en Línea	2	2	2	2	3	2	4
2-4	**Mecanismos de Denuncia ($\bar{X}$)**	**2,00**	**3,00**	**2,00**	**3,00**	**3,00**	**2,00**	**4,00**
	Mecanismos de Denuncia	2	3	2	3	3	2	4
2-5	**Medios y Redes Sociales ($\bar{X}$)**	**2,00**	**3,00**	**2,00**	**3,00**	**3,00**	**2,00**	**3,00**
	Medios y Redes Sociales	2	3	2	3	3	2	3
	Media geométrica	**2,06**	**2,77**	**2,24**	**2,77**	**3,00**	**2,13**	**3,77**

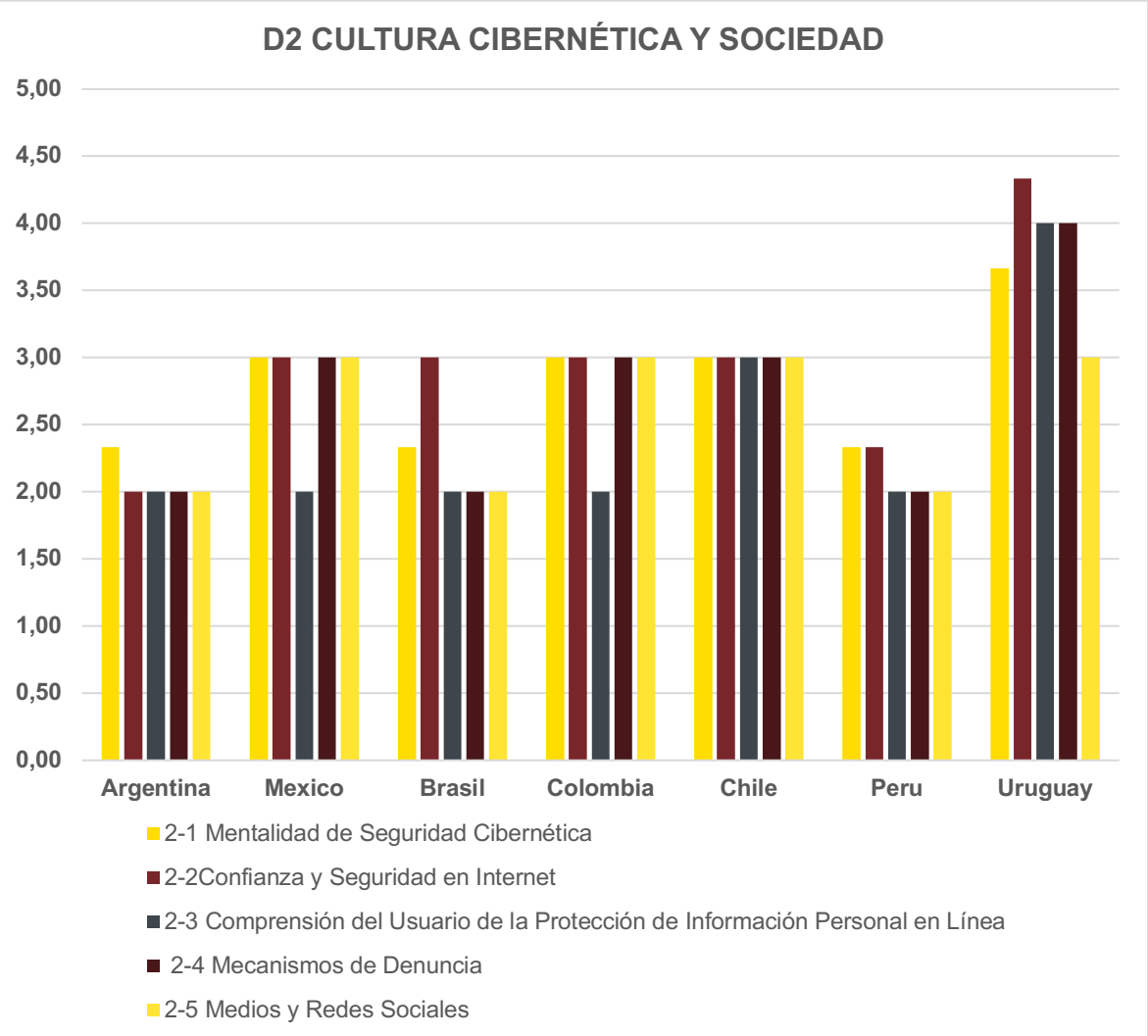


Figura 23. Gráfico comparativo entre países Latinoamericanos del dominio D2 del estudio de la OEA. Datos: [15]. Análisis: INCIBE

El análisis de los factores de la dimensión D2 revela que Uruguay es sin duda el país más avanzado en este aspecto, con una capacidad **consolidada** que está cercana a la estratégica en madurez. El resto de los países se mueven dentro del nivel **formativo** de esta capacidad, con la excepción de Chile, que muestra una capacidad media **consolidada**.

1.3.2.2.3. Formación, Capacitación y Habilidades de Seguridad Cibernética

Este dominio mide el **desarrollo del conocimiento de ciberseguridad** en cada país analizado. La Figura 24 y la Tabla 10 muestran la madurez de cada uno de los países estudiados en este aspecto. El análisis de valores medios de cada factor y finales se ha hecho **idéntico al de la dimensión D1**.

Tabla 10. Análisis del dominio D3 de los países latinoamericanos estudiados según la OEA. Datos: [15]. Análisis: INCIBE

D3: FORMACIÓN, CAPACITACIÓN Y HABILIDADES DE SEGURIDAD CIBERNÉTICA

		Argentina	México	Brasil	Colombia	Chile	Perú	Uruguay
3-1	**Sensibilización ($\bar{X}$)**	**2,50**	**3,00**	**3,00**	**3,00**	**3,00**	**2,00**	**3,50**
	Programas de Sensibilización	2	3	3	3	3	2	4
	Sensibilización Ejecutiva	3	3	3	3	3	2	3
3-2	**Marco para la Formación ($\bar{X}$)**	**2,00**	**3,00**	**2,50**	**2,50**	**2,00**	**1,50**	**3,00**
	Provisión	3	3	3	3	2	2	3
	Administración	1	3	2	2	2	1	3
3-3	**Marco para la Capacitación Profesional ($\bar{X}$)**	**2,50**	**3,00**	**3,00**	**3,00**	**3,00**	**2,00**	**3,50**
	Provisión	2	3	3	3	3	2	4
	Apropiación	3	3	3	3	3	2	3
	Media geométrica	**2,32**	**3,00**	**2,82**	**2,82**	**2,62**	**1,82**	**3,32**

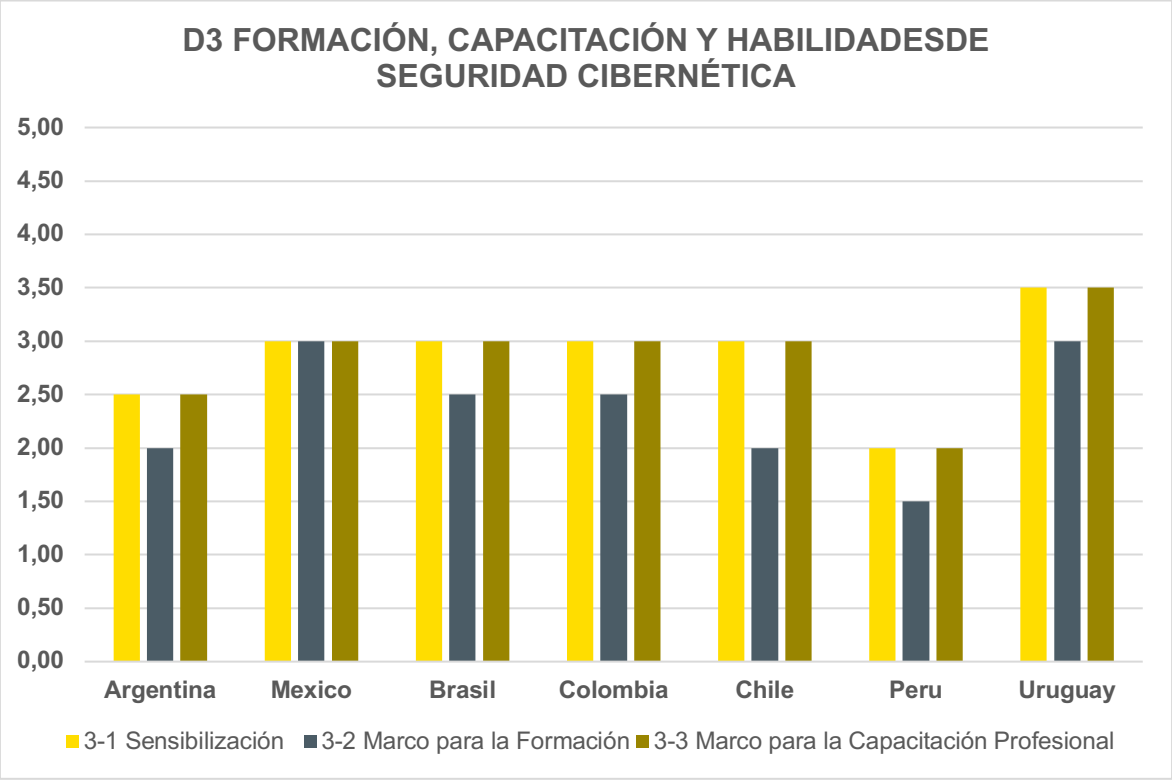


Figura 24. Gráfico comparativo entre países Latinoamericanos del dominio D3 del estudio de la OEA. Datos: [15]. Análisis: INCIBE

El análisis de los factores de la dimensión D3 pone de nuevo a Uruguay a la cabeza de este aspecto, con una capacidad **consolidada**. El segundo país es México, que también

desarrolla este dominio al mismo nivel. El resto de los países se mueven en niveles **formativos**, con la excepción de Perú, que aún no ha alcanzado ese nivel de madurez y sus capacidades medias en ese dominio son aún **iniciales**.

1.3.2.2.4. Estándares, Organizaciones y Tecnologías

Este dominio mide la **creación de marcos legales y regulatorios efectivos** por parte de los países analizados. La Figura 25 y la Tabla 11 muestran la madurez de cada uno de los países estudiados en este aspecto. El análisis de valores medios de cada factor y finales se ha hecho de nuevo **idéntico al de la dimensión D1**.

Tabla 11. Análisis del dominio D4 de los países latinoamericanos estudiados según la OEA. Datos: [15]. Análisis: INCIBE

D4: MARCOS LEGALES Y REGULATORIOS

		Argentina	México	Brasil	Colombia	Chile	Perú	Uruguay
4-1	**Marcos Legales ($\bar{X}$)**	**3,13**	**3,00**	**3,75**	**2,88**	**3,25**	**2,63**	**3,00**
	Marcos Legislativos para la Seguridad de las TIC	3	3	4	3	3	3	4
	Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea	4	3	4	3	3	3	5
	Legislación Sobre Protección de Datos	3	3	4	3	3	3	5
	Protección Infantil en Línea	3	3	3	3	2	3	2
	Legislación de Protección al Consumidor	3	3	4	2	4	2	2
	Legislación de Propiedad Intelectual	3	3	3	3	5	2	2
	Legislación Sustantiva Contra el Delito Cibernético	3	3	4	3	3	3	2
	Legislación Procesal Contra el Delito Cibernético	3	3	4	3	3	2	2
4-2	**Sistema de Justicia Penal ($\bar{X}$)**	**2,67**	**3,00**	**3,00**	**2,33**	**2,33**	**2,00**	**2,67**
	Fuerzas del Orden	3	4	4	3	3	2	3
	Enjuiciamiento	3	3	3	2	2	2	2
	Tribunales	2	2	2	2	2	2	3
4-3	**Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético ($\bar{X}$)**	**2,00**	**2,50**	**2,00**	**2,50**	**3,00**	**2,00**	**3,00**
	Cooperación Formal	2	2	2	3	3	2	2
	Cooperación Informal	2	3	2	2	3	2	4
	Media geométrica	**2,55**	**2,82**	**2,82**	**2,56**	**2,83**	**2,19**	**2,88**

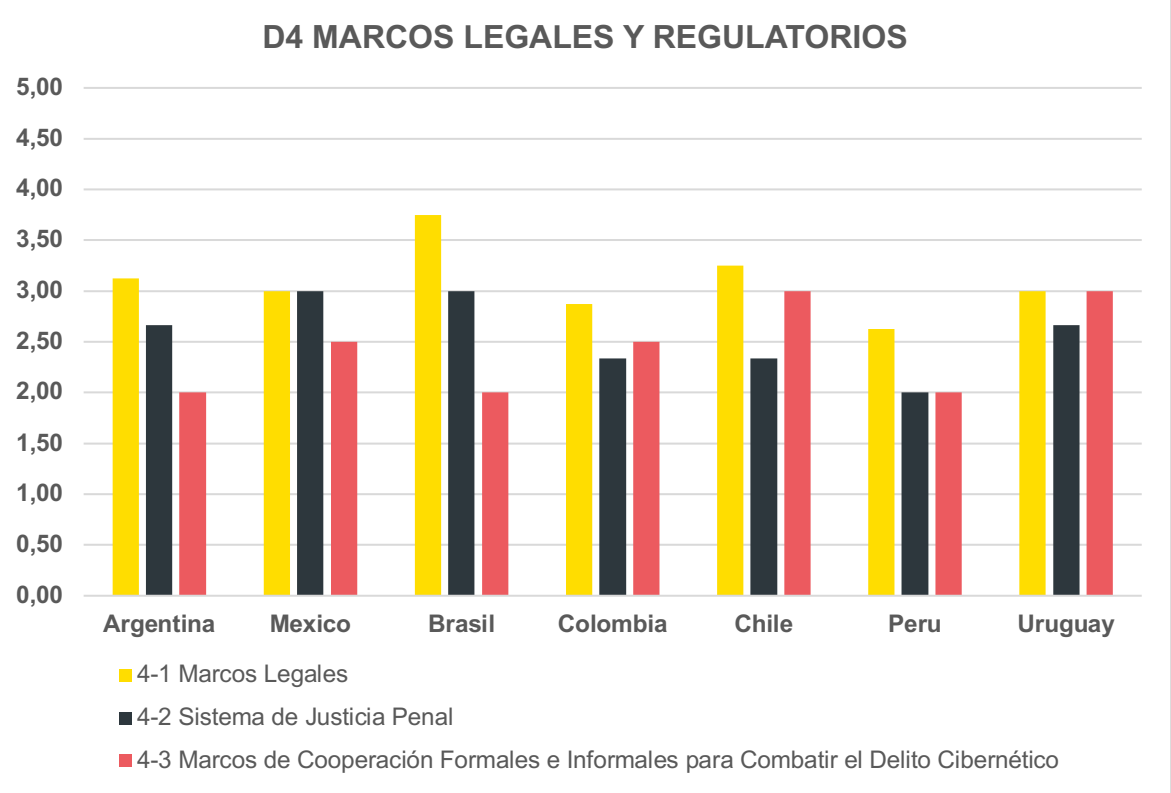


Figura 25. Gráfico comparativo entre países Latinoamericanos del dominio D4 del estudio de la OEA. Datos: [15]. Análisis: INCIBE

El análisis de los factores de la dimensión D4 revela que todos de los países analizados alcanza en media una madurez de esta dimensión **formativa**, aunque 4 países (México, Brasil, Chile y Uruguay) están relativamente cerca de conseguir **consolidarla**. Llama especialmente la atención la **máxima puntuación** obtenida por Uruguay en los aspectos "Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea" y "Legislación Sobre Protección de Datos" dentro del factor "Marcos Legales", señal de que se ha hecho mucho trabajo en ambos aspectos.

1.3.2.2.5. Marcos Legales y Regulatorios

Este dominio mide el **control de riesgos a través de estándares, organizaciones y tecnologías** de cada país analizado. La Figura 26 y la Tabla 12 muestran la madurez de cada uno de los países estudiados en este aspecto. El análisis de valores medios de cada factor y finales se ha hecho también **idéntico al de la dimensión D1**.

Tabla 12. Análisis del dominio D5 de los países latinoamericanos estudiados según la OEA. Datos: [15]. Análisis: INCIBE

D5 ESTÁNDARES, ORGANIZACIONES Y TECNOLOGÍAS

		Argentina	México	Brasil	Colombia	Chile	Perú	Uruguay
5-1	**Cumplimiento de los Estándares ($\bar{X}$)**	**2,00**	**2,33**	**2,67**	**2,33**	**2,67**	**1,67**	**4,00**
	Estándares de Seguridad de las TIC	2	2	4	2	3	2	4
	Estándares en Adquisiciones	2	2	2	2	3	1	4
	Estándares en el Desarrollo de Software	2	3	2	3	2	2	4

5-2	**Resiliencia de la Infra. de Internet (X̄)**	**2,00**	**3,00**	**3,00**	**3,00**	**3,00**	**2,00**	**4,00**
	Resiliencia de la Infraestructura de Internet	2	3	3	3	3	2	4
5-3	**Calidad del Software (X̄)**	**2,00**	**2,00**	**2,00**	**2,00**	**2,00**	**2,00**	**4,00**
	Calidad del Software	2	2	2	2	2	2	4
5-4	**Controles Técnicos de Seguridad (X̄)**	**2,00**	**3,00**	**3,00**	**3,00**	**2,00**	**2,00**	**4,00**
	Controles Técnicos de Seguridad	2	3	3	3	2	2	4
5-5	**Controles Criptográficos (X̄)**	**2,00**	**3,00**	**3,00**	**2,00**	**2,00**	**2,00**	**5,00**
	Controles Criptográficos	2	3	3	2	2	2	5
5-6	**Mercado de Seguridad Cibernética (X̄)**	**2,00**	**2,50**	**3,00**	**2,00**	**2,50**	**1,50**	**3,00**
	Tecnologías de Seguridad Cibernética	2	3	3	2	2	1	3
	Seguro Cibernético	2	2	3	2	3	2	3
5-7	**Divulgación Responsable (X̄)**	**2,00**	**1,00**	**3,00**	**2,00**	**2,00**	**1,00**	**4,00**
	Divulgación Responsable	2	1	3	2	2	1	4
	Media geométrica	**2,00**	**2,27**	**2,78**	**2,30**	**2,28**	**1,69**	**3,96**

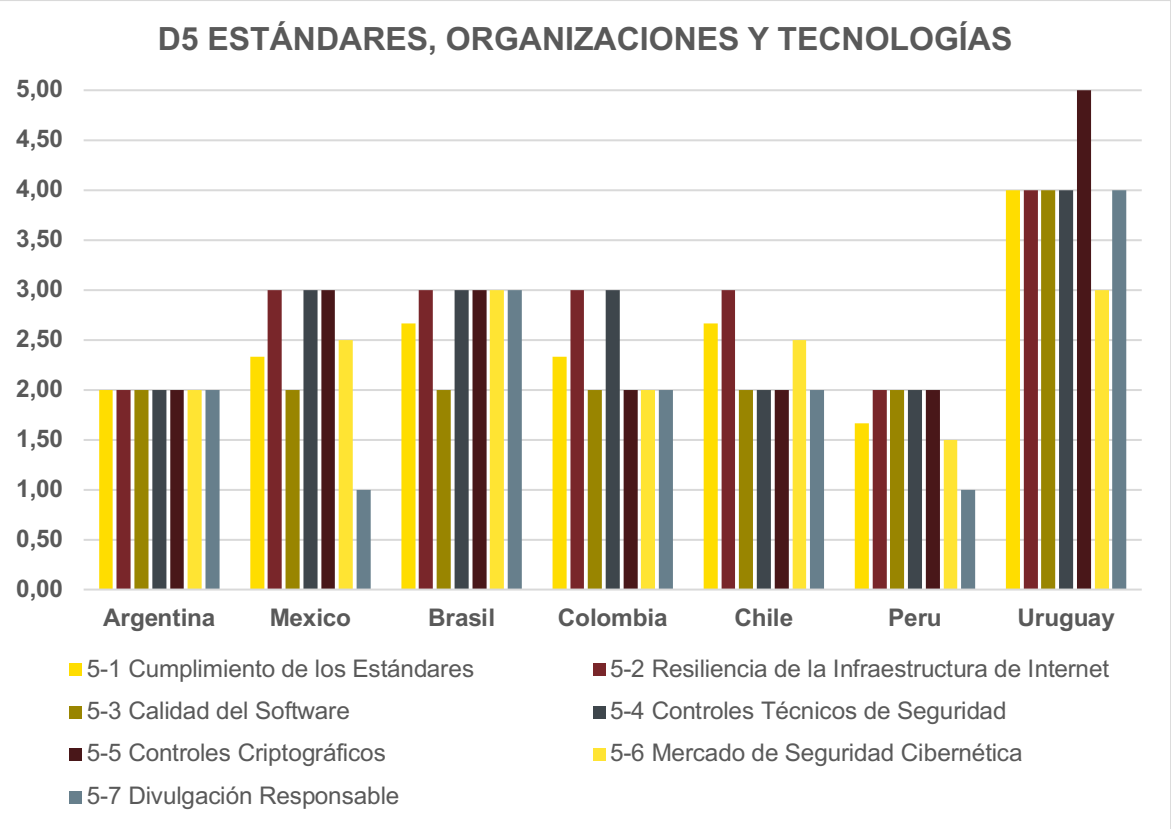


Figura 26. Gráfico comparativo entre países Latinoamericanos del dominio D5 del estudio de la OEA. Datos: [15]. Análisis: INCIBE

En el análisis de los factores de la dimensión D5, llama especialmente la atención la importante ventaja que Uruguay lleva al resto de países analizados, logrando tener una madurez media casi **estratégica** en esa dimensión, con un aspecto, los **controles criptográficos**, en un nivel de madurez **dinámico** (el máximo). El resto de los países analizados tienen un nivel de madurez medio **formativo** y, de nuevo, es Perú la que posee un nivel de madurez más bajo, al ser aún **inicial** en media.

1.3.2.3. Análisis global

Para hacer un análisis global de cada país, tomamos las **medias geométricas** de cada una de las 5 dimensiones del *ranking* OEA de cada país analizado. Con esos 5 valores, calculamos de nuevo su media geométrica para obtener un **índice de madurez medio de los cinco aspectos, en forma de un único valor numérico** (ver Tabla 13). Este valor nos permite establecer un *ranking* de los países analizados, que presenta un **orden diferente** al que tienen según el *ranking* ITU analizado en el apartado anterior (Tabla 7).

En primer lugar, Perú y Argentina son **los dos países en las posiciones más atrasadas** en ambos estudios, a bastante distancia del resto. En ambos *ranking*s uno de los aspectos más débiles de ambos países tiene que ver con la **seguridad de las organizaciones**.

No obstante, el orden relativo del resto de los países analizados **cambia entre ambos *ranking*s**. Esto indica que, si bien ambos índices miden algunos aspectos similares, en realidad **los análisis de la ITU y la OEA pueden considerarse complementarios**. Tenemos así dos análisis de los países desde **puntos de vista alternativos** en un momento del tiempo similar (ambos estudios fueron realizados alrededor del 2020).

Tabla 13. Resumen global de puntuación de los 5 dominios de los países latinoamericanos estudiados según la OEA. Datos: [15]. Análisis: INCIBE

	Uruguay	Colombia	México	Brasil	Chile	Argentina	Perú
D1 Política y Estrategia de Seguridad Cibernética	3,41	3,42	2,55	2,67	2,41	2,20	1,84
D2 Cultura Cibernética y Sociedad	3,77	2,77	2,77	2,24	3,00	2,06	2,13
D3 Formación, Capacitación y Habilidades de Seguridad Cibernética	3,32	2,82	3,00	2,82	2,62	2,32	1,82
D4 Marcos Legales y Regulatorios	2,88	2,56	2,82	2,82	2,83	2,55	2,19
D5 Estándares, Organizaciones y Tecnologías	3,96	2,30	2,27	2,78	2,28	2,00	1,69
Media geométrica	**3,45**	**2,75**	**2,67**	**2,66**	**2,62**	**2,22**	**1,92**

Como puede verse en la Tabla 13, **la principal diferencia** entre los resultados del *ranking* de la OEA y la ITU **es el resultado obtenido por Uruguay**. Si en el *ranking* ITU Uruguay es el tercer país entre los analizados, por detrás de Brasil y México, el *ranking* de la OEA lo sitúa el **primero de todos**, con un nivel de madurez medio **consolidado** y a bastante distancia del **formativo** alcanzado por el resto de los países (salvo Perú).

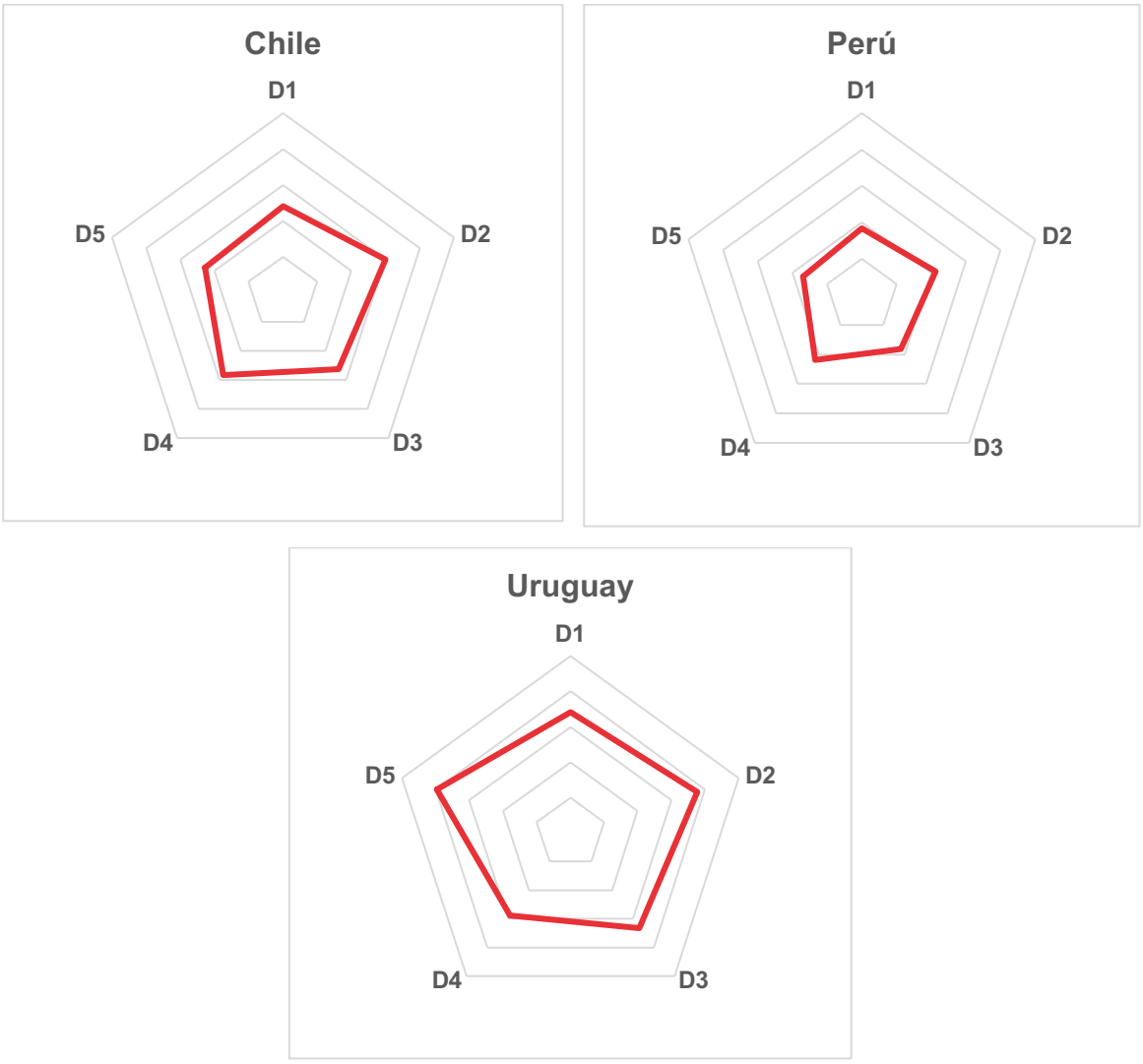
Colombia, antepenúltimo país de los estudiados según el *ranking* de la ITU, es el **segundo en el *ranking* del estudio de la OEA**, si bien en ambos *ranking*s los aspectos relativos a la seguridad de las organizaciones son los que obtienen puntuaciones más bajas.

México y Brasil aparecen en posiciones adyacentes en ambos *ranking*s, si bien en distinto orden. Mientras que en el *ranking* de la OEA aparecen como países con un nivel de madurez medio **casi idéntico**, la diferencia de puntuación y posición entre ambos en el *ranking* ITU es más acusada. Finalmente, Chile se encuentra en posiciones medias en ambos *ranking*s.

Por tanto, podemos concluir que la unión de los factores estudiados en ambos *ranking*s permite tener **una visión más completa del estado y madurez de la ciberseguridad en cada país**. Países como Uruguay, que en *ranking* ITU aparece en una posición más atrasada, sin embargo, en el ***ranking* de la OEA** (especializado en la **madurez** de los aspectos de ciberseguridad y **hecho solo a países latinoamericanos**, principal objetivo de estudio de este informe) es el primero, a una distancia significativa del resto de los países estudiados.

No obstante, como decíamos anteriormente, la gran ventaja del *ranking* ITU es que **permite comparar a los países latinoamericanos con países del resto del mundo** con el mismo conjunto de criterios, cosa que el *ranking* de la OEA ni permite ni contempla. De esta manera, tenemos dos comparaciones complementarias de países latinoamericanos: la primera extrapolable a países del resto del mundo y la segunda exclusivamente entre ellos.

Para finalizar, mostramos estos **gráficos radiales** (idénticos a los usados en el *ranking* ITU) con los valores medios del *ranking* de la OEA. Esto permite mostrar de forma clara las **fortalezas y debilidades** de cada país en las cinco dimensiones estudiadas.



1.4. Estudio de casos de éxito: Argentina y México

Una vez analizado el consumo en el mercado de ciberseguridad y el grado de madurez de estos en diferentes aspectos de la ciberseguridad en una representación de los países latinoamericanos, a continuación, vamos a hablar de las **empresas de ciberseguridad** en **dos de los países analizados** en los *ranking*s anteriores como representantes del resto.

Para ello hemos elegido **México** y **Argentina**. Son dos países que en los *ranking*s analizados se encuentran en extremos opuestos y por tanto permiten ver el negocio de la ciberseguridad desde la perspectiva de países que han sido evaluados con resultados muy diferentes.

El objetivo de esta sección es mostrar claramente que **hay un gran ecosistema de empresas en los países latinoamericanos** que cubren los aspectos claves de ciberseguridad, y que podrían dar el salto al mercado español, y a través al europeo, siguiendo el proceso que detallaremos en la sección 1.5.

Si además tenemos en cuenta el desglose de consumo de ciberseguridad en España destacado en la Tabla 2 y la **línea de negocio** de las empresas analizadas (incluida en las tablas de empresas que veremos a continuación), podemos ver más fácilmente si una

empresa latinoamericana concreta trabaja en un sector donde hay una inversión mayoritaria en España.

1.4.1. México

Según [8] el mercado mexicano de ciberseguridad se encuentra **muy fragmentado**. Las principales empresas son multinacionales de *hardware* y software, servicios de tecnología, consultoras y administradores de seguridad. Existe una **elevada presencia de empresas extranjeras**, principalmente estadounidenses. Ejemplos son: Rockwell, Kaspersky, Paloalto Networks, Cisco Systems, Trend Micro, Belden Solutions, Broadcom, Attivo Networks, Primx, Fortinet, Alestra, EY, IBM, Deloitte, KPMG, PWC o Thales.

1.4.1.1. Ecosistema de *start-up* en México

Según [16], México es el **segundo mercado de *start-up* de América Latina** tras Brasil. La principal actividad emprendedora del país se sitúa en su **capital** (Ciudad de México) y **Monterrey**, aunque el país tiene otros polos de emprendimiento:

- **Ciudad de México**: Concentra la mayoría de las **nuevas empresas *Fintech*** y la mayoría de las **corporaciones internacionales**. Es un destino atractivo para fondos de inversión internacionales y locales.
- **Monterrey**: Tiene una gran presencia de *start-up* con soluciones innovadoras en sectores de **fabricación y comercio electrónico**. Destacan corporaciones industriales como Cemex y Xignux. Nuevo León tiene también una gran actividad industrial. Cuenta además con varias universidades, aceleradoras e incubadoras. Describiremos más este polo de emprendimiento en la subsección 1.4.1.3.
- **Guadalajara**: Es uno de los estados con mayor crecimiento en la formación de negocios. Cuenta con varias universidades que fomentan las incubadoras, y es la sede de algunas de las principales empresas tecnológicas internacionales.
- **Puebla**, **Querétaro** y **Pachuca** se consideran también polos de innovación, al contar con universidades que promueven la innovación mediante incubadoras y aceleradoras.

México **no cuenta con una regulación específica** para emprendimiento y *start-up*. Estas empresas deben regularse según la **Ley General de Sociedades Mercantiles**. A pesar de ello, es uno de los sectores económicos **con mayores expectativas de crecimiento**, (ha crecido un 16% anual desde 2010), **destacando los servicios de seguridad** y la digitalización de los servicios financieros.

La presencia en México de *start-up* españolas en sectores como *healthtech*, *fintech* e *insurtech*, *proptech* y *edtech*, entre otros, es significativa. En 2021, los sectores económicos con el mayor porcentaje de *start-up* en el país fueron el *software* y datos y *fintech*, concentrando el 25,6 % de las *start-up* registradas en el país.

Como elementos para generar un **entorno que favorezca el emprendimiento**, México tiene una oferta muy variada de **aceleradoras** y de **fondos de capital riesgo**, que en los últimos tiempos están creciendo gracias a fondos internacionales procedentes de EEUU y de España. Entre los inversores, las principales fuentes de ahorro se concentran en *family offices*, corporativos y fondos de pensiones.

México cuenta con varias *start-up* "**unicornio**" (su cotización es superior a 1.000 millones de dólares), entre las que destacan estas 8, cinco de las cuales pertenecen al sector *fintech*.

Tabla 14. Start-up "unicornio" destacables en México

Nombre Empresa	Web	Sector
Kavak	https://www.kavak.com/	Compraventa y alquiler de coches
Bitso	https://bitso.com/	Criptomonedas
Clip	https://www.clip.mx/clip-para-empresas	Pagos electrónicos
Konfío	https://konfio.mx/	Créditos empresariales
Merama	https://www.merama.io/	Aceleración de crecimiento de empresas
Nowports	https://nowports.com/	Transportes y envíos
Clara	https://www.clara.com/es-mx/	Administración de gastos de empresas
Stori	https://www.storicard.com/	Líneas y tarjetas de crédito

Según la Asociación Mexicana de Venta Online (AMVO, https://www.amvo.org.mx/), México tendrá **el 25 % de los unicornios de América Latina** al corto plazo. Existen 30 *start-up* cercanas a alcanzar este status de "unicornio".

Según [16], entre los sectores con expectativas de crecimiento **destacan los servicios de ciberseguridad** (de especial relevancia para este informe), la digitalización de los servicios financieros, la atención médica en línea y la industria de seguros. México tiene una necesidad creciente de soluciones para que sus consumidores saquen partido de nuevas oportunidades mediante herramientas digitales y automatización, impulsando el emprendimiento en el país. Entre ellas podemos destacar:

- **Era digital**: El auge de la economía digital obliga a las empresas a digitalizarse y a agilizar procesos.
- **IA y Análisis de datos**: El desarrollo del 5G impulsará el crecimiento de *start-up* de IoT e IA.
- ***Start-up* de ESG**: La necesidad de abordar retos en las tres dimensiones de la sostenibilidad (económica, social y ambiental) fomenta la aparición de empresas en el sector, incluyendo las de atención médica y soluciones limpias.
- **Necesidades de ciberseguridad**: El incremento de la digitalización de las empresas implica aumentar las soluciones para protegerlas de ataques. México cuenta ya con un ecosistema de empresas de ciberseguridad, que describiremos en la siguiente subsección.

1.4.1.2. Principales empresas de ciberseguridad mexicanas

El país tiene un buen número de empresas de ciberseguridad **mexicanas**, como Nordstern Technologies, Totalsec, VdV Netwoks o CSI consultores. Estas cubren un **amplio espectro de soluciones** relacionadas con ciberseguridad, con clientes nacionales e internacionales. Muchas de estas soluciones pueden **ser candidatas para implantar en España en forma de *start-up*** que las adapte a la realidad del mercado español y europeo a través de él.

De acuerdo con la información ofrecida por [17], la Tabla 15 lista las **empresas de ciberseguridad mexicanas más relevantes**.

Tabla 15. Principales empresas de ciberseguridad en México

Empresa	Línea de negocio
2Secure	Seguridad de la Información, Desarrollo de software, consultoría en tecnología de la Información, Informática Forense e Investigación y Desarrollo orientados a la seguridad
Alestra	Ofrece soluciones tecnológicas a todo el sector empresarial mexicano, corporaciones nacionales, empresas multinacionales y clientes institucionales
ARAME	Seguridad gestionada, arquitectura de seguridad, protección de identidad, detección y respuesta a amenazas
ASI	Servicios y soluciones de TI para mejorar negocios y protección de información
BMobile Grupo Scanda	Tecnología, procesos y conocimientos necesarios para que el usuario cree un entorno adecuado para la movilidad empresarial
Consultoría de sistemas avanzados CAS	Consultoría y soporte técnico para Tecnologías de la Información (TI) en el nicho de administración de servidores, seguridad de la información, conectividad, continuidad comercial y soporte al usuario
Eyesec	Servicios nacionales e internacionales dentro del sector gubernamental, privado y financiero
GLAC	Consultoría en Seguridad Pública, Seguridad Nacional e Inteligencia
HackingMexico	Sistemas de seguridad informática para empresas y particulares. Desde el seguimiento de los empleados hasta la prevención del fraude.
HD Latinoamérica	Proteger los recursos informáticos y patrimoniales de las instancias y organismos gubernamentales
IQsec	Ofrecer a las organizaciones soluciones integrales de seguridad informática basadas en necesidades específicas
KIO Cyber	Diagnóstico y solución de problemas de seguridad informática
Lighttech	Ofrecen, implementan, respaldan, administran y monitorizan tecnología de protección y detección de los principales fabricantes
N3XAsec	Seguridad informática y la informática forense especializada en servicios y tecnologías de la información, con el fin de garantizar la protección de los activos digitales
Netrix	servicios gestionados, servicios profesionales y soluciones llave en mano relacionados con la seguridad
ProtektNet	Seguridad de TI de las empresas mediante la automatización de sus sistemas de control
Scitum	Proteger, detectar y actuar ante las nuevas amenazas que existen en el mundo digital (entorno digital seguro)
Zero Uno	Protección de la información para prevenir fraudes, piratería, robos y otros problemas de seguridad

1.4.1.3. El papel del instituto tecnológico Monterey

El Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) (también conocido como el Tecnológico de Monterrey o el "Tec de Monterrey"), es una universidad privada mexicana con su sede principal en Monterrey, Nuevo León. Se trata de **uno de los principales polos de innovación del país**, que impulsa acciones relacionadas con la educación y la creación de *start-up* [18], entre las cuales hay acciones para facilitar la creación de **ideas innovadoras de ciberseguridad**.

Por ejemplo, en 2018 [19] se creó **el primer *hub* de ciberseguridad en América Latina** mediante una alianza entre el Tec de Monterrey, CISCO, Deloitte, IBM, Thales y la Universidad de Texas. Este *hub* pretende encontrar espacios para que *start-up*,

investigadores, alumnos e inversores colaboren a la hora de capacitar talento en el área de ciberseguridad.

Otra iniciativa de muy reciente implantación (2023) es la **Academia de Ciberseguridad para Comunicadores** [20], como alianza entre Microsoft y el Tec de Monterrey. Esta academia tiene como objetivo formar a periodistas, creadores de contenido y profesionales de comunicación y relaciones públicas en ciberseguridad, para que sean capaces de entender, articular e impulsar cambios profundos para lograr un conocimiento de tecnologías, prácticas y conciencia sobre ciberseguridad en sus redacciones y organizaciones, respectivamente**.**

Otra iniciativa del Tec de Monterrey es el ***Cybersecurity BootCamp*** [21]. Es un programa online de alta exigencia y con posibilidad de cursarse a tiempo parcial, que adopta un **enfoque multidisciplinario** para lograr la competencia en TI, redes y seguridad de la información moderna, a lo largo de 24 semanas intensivas.

Por tanto, estas iniciativas, entre otras, muestra el **claro compromiso del Tec de Monterrey** con la innovación en el país, especialmente en ciberseguridad, con el impulso a la creación de talento y a la innovación hecho a través de ellas.

1.4.1.4. Vínculos con España

La implantación de empresas mexicanas en España se facilita gracias a la gran **colaboración institucional** que existe entre España y México [8]. España **es un país de referencia en este sector**, gracias a la labor del Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia (CNI), y del Instituto Nacional de Ciberseguridad (INCIBE), que han desarrollado diversas actividades de **formación y de consultoría** en materia normativa con la administración mexicana

Empresas españolas con presencia en México son, por ejemplo: Elevenpaths (división de ciberseguridad de Telefónica), Minsait (división de Indra), S21Sec, Electronic identification, Innotec System (grupo Entelgy), S2 GRUPO, Countercraft, Continuum Security, Mnemo, GMV, One Esecurity, Ondata Internacional Spamina, Everis, Enigmedia, Scati Labs, Ikusi, Prosegur, Innotech, OpenCloud y Buguroo.

Como decíamos, este gran ecosistema de empresas puede ayudar a empresas mexicanas a “dar el salto” a España colaborando con ellas para facilitar acceso a proveedores, lugares, potenciales clientes, etc., con la posible ayuda de los programas de apoyo al emprendimiento que pueda tener en un momento dado el Tec de Monterrey, por ejemplo.

Para fomentar este “salto”, existen además **instrumentos de apoyo y programas públicos de emprendimiento** presentes en ambos países. Describimos a continuación los más relevantes [16].

1.4.1.4.1. Mexicanos

- **BID LAB** (https://bidlab.org/es): Laboratorio de innovación que busca **empoderar a las poblaciones vulnerables** y fomentar su crecimiento inclusivo, fomentando el conocimiento, las conexiones que faciliten el emprendimiento y su financiación.
- **Banca de Desarrollo** (https://www.gob.mx/cnbv/acciones-y-programas/banca-de-desarrollo-bd): Entidades de la Administración Pública Federal del país pertenecientes al Sistema Bancario Mexicano. Su objetivo es **facilitar el ahorro y**

la financiación, con especial atención en áreas prioritarias para el desarrollo nacional.

- **MIPYMESMX** (https://mipymes.economia.gob.mx/): Plataforma que ofrece herramientas empresariales, contenidos, eventos y programas para el **desarrollo y fortalecimiento de las capacidades emprendedoras**.

1.4.1.4.2. Españoles

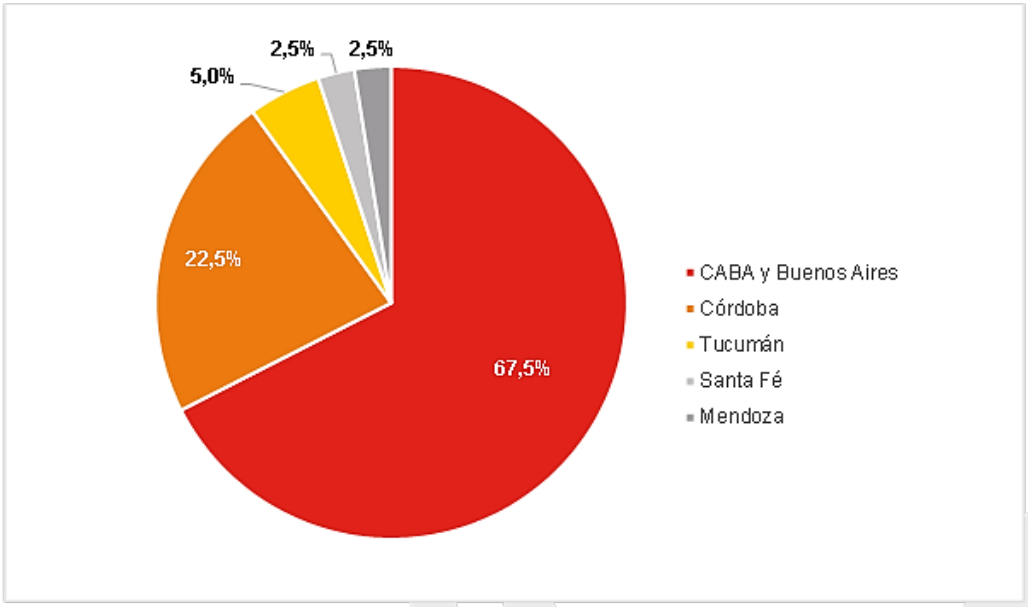
- **Activa Startups** (https://www.boe.es/boe/dias/2021/12/22/pdfs/BOE-A-2021-21192.pdf): Programa de desarrollo de proyectos de colaboración entre pymes y *start-up* mediante **subvenciones para proyectos de innovación de transformación digital**, incorporación de tecnologías emergentes, economía baja en carbono o circular.
- **Programa INNVIERTE (CDTI)** (https://www.cdti.es/index.asp?MP=4&MS=0&MN=1&textobuscado=Programa%2BInnvierte&tipo=1&TR=A&IDR=38&tipoO=Contenido&id=1812&xtmc=Programa_Innvierte&xtcr=3): Parte de la Estrategia Española de Ciencia y Tecnología y de Innovación que promueve la innovación empresarial a través del **apoyo a la inversión de capital de riesgo** en empresas de base tecnológicas o innovadoras.
- **ICEX Localiza** (https://www.icex.es/es/todos-nuestros-servicios/programas-y-servicios-de-apoyo/icex-localiza): Programa que apoya la **implantación o consolidación de las pymes españolas fuera de la UE**. Los proyectos pueden pertenecer a cualquier sector de actividad.
- **ICEX Next** (https://www.icex.es/es/todos-nuestros-servicios/programas-y-servicios-de-apoyo/programa-icex-next/-que-es-): Programa que combina el **asesoramiento especializado** para desarrollar el Plan de Negocio Internacional de cualquier PYME española que tenga un producto, servicio y/o marca propia, con una facturación superior a los 200.000 euros, salvo para *start-up* de base tecnológica.
- **España-Emprende (Cámara de Comercio)** (https://emprende.camara.es/): Programa para dar **apoyo al emprendedor** en todas las fases de vida de la empresa en el que participan múltiples cámaras de comercio del país.
- **Financiación para PYMES y *start-up* innovadoras** (https://spain.representation.ec.europa.eu/empresas-y-financiacion/financiacion-para-pymes-y-start-ups-innovadoras_es)
  - **El Acelerador del CEI** (https://eic.ec.europa.eu/eic-funding-opportunities/eic-accelerator-0_en): Ofrece a PYMEs, empresas emergentes y emprendedores el acceso a subvenciones para financiar proyectos de cierto riesgo y gran potencial. Facilita también el acceso a inversión de capital para actividades comerciales y de refuerzo de la presencia internacional.
  - **El Programa LIFE** (https://www.miteco.gob.es/es/ministerio/servicios/ayudas-subvenciones/programa-life/default.aspx): Apoya proyectos de empresas e instituciones sobre **medio ambiente**.
- **Programa de Atracción de Emprendimiento Femenino** (https://the-break.eu/). *The Break: Women Entrepreneurship & Internationalisation in Spain* es un programa de atracción de emprendimiento femenino que busca atraer proyectos emprendedores liderados por mujeres de la UE.

1.4.2. Argentina

Según [6], Argentina es un país donde existen un gran nº de empresas de ciberseguridad **internacionales** y también **nacionales**. En lo referente a las **internacionales**, el líder es Fortinet, alcanzando un 43 % de la cuota de mercado en 2020. El resto de las principales empresas internacionales presentes en el país son: IBM, Symantec, CISCO y McAfee.

1.4.2.1. Ecosistema de *start-up* en Argentina

De acuerdo con la información recopilada por el ICEX en [22], la actividad emprendedora Argentina **se concentra en su capital** (Ciudad Autónoma de Buenos Aires o CABA) y en otras ciudades de la **provincia de Buenos Aires**. Tal y como se muestra en la Figura 27, la provincia de Córdoba es el segundo gran foco de emprendimiento en el país, aunque a mucha distancia de la zona CABA.



Fuente: https://arcap.org/wp-content/uploads/2022/08/Reporte-primer-semestre-2022-ARCAP.pdf

Figura 27.Localización geográfica de start-up en Argentina en el primer semestre de 2022 (% del total de start-up). Fuente: [22]

Buenos Aires es por tanto el centro del sistema emprendedor argentino, y así se reconoce a nivel mundial, ocupando la **posición 75 en el mundo** y siendo el **4º en importancia** en la región de Sudamérica en 2023 [23].

Argentina también tiene 12 *start-up* que se pueden denominar "**unicornios**" (que, como vimos en la sección dedicada al ecosistema mexicano, son empresas cuya cotización es superior a 1.000 millones de dólares) (ver Tabla 16), siendo el segundo país de Latinoamérica tras Brasil. De entre las empresas del listado destacamos **la empresa de ciberseguridad Auth0**, dedicada a la autenticación y autorización, y adquirida por la estadounidense Okta en 2021, un líder en ese sector.

Tabla 16. Listado de empresas "unicornio" en Argentina. Valoración en MUSD en abril de 2022. Fuente: [22]

Nombre Empresa	Web	Sector	Año creación	Valoración
Mercado Libre	https://mercadolibre.com/	Comercio electrónico	1999	44.800
Globant	https://www.globant.com/es	Desarrollo de software	2003	10.400
OLX	https://www.olx.com/	Comercio electrónico	2006	5.000
Despegar	https://www.despegar.com.ar/	Turismo	1999	1.2009
Auth0	https://auth0.com/	Seguridad informática	2013	6.500
Vercel	https://vercel.com/	Diseño web	2015	1.100
Aleph	https://www.aleph.es/	Publicidad online	2015	2.000
Mural	https://www.mural.co/	Equipos de trabajo virtuales	2011	2.000
Bitfarms	https://bitfarms.com/	Criptomonedas	2017	1.000
Ualá	https://www.uala.com.ar/	Fintech	2017	2.450
Tiendanube	https://www.tiendanube.com/	Comercio electrónico	2015	1.100
Technisys	https://www.technisys.com/es/	Fintech y banca digital	1995	1.100

1.4.2.2. Principales empresas de ciberseguridad argentinas

La competencia entre empresas nacionales argentinas está **muy fragmentada** [6], y quizá por ello sea interesante para muchas de ellas **expandirse** en otras regiones como España [24], dada la ausencia de barrera idiomática y las facilidades existentes que describiremos en la sección 1.5. De acuerdo con [25], las **principales empresas argentinas de ciberseguridad** son las que aparecen en la Tabla 17.

Tabla 17. Principales empresas de ciberseguridad en Argentina

Empresa	Línea de negocio
Amalgama	Producto, diseño, metodología y desarrollo de software
BairesDev	Subcontratación de software, las pruebas y el soporte operativo
Cloud Legion	Ayudar a las organizaciones a mejorar su posición competitiva y eficiencia mediante el uso de la tecnología informática de forma segura
Core Security	Proporciona a las empresas la información de seguridad que necesitan para saber quién, cómo y qué es vulnerable en su organización. Tiene soluciones de gestión de vulnerabilidades, seguridad de red y detección de amenazas
DinoCloud	Ingeniería en la nube y DevOps para soluciones SaaS
FlyDevs	Servicios como aumento de personal, estrategia, análisis, soporte comercial y desarrollo de productos para cualquier tipo de negocio y *start-up*

Fulcrum Digital	Servicios de consultoría en tecnología de la información en los campos de banca y finanzas, seguros, educación superior, servicios alimentarios, atención médica, ciencias de la vida, legal y manufactura
Grupo Datco	Servicios de infraestructura de TI e integración con comunicaciones
IncluIT	Desarrolla equipos de alto rendimiento, capaces de afrontar desafíos y ofrecer servicios y soluciones tecnológicas
Julasoft	Soluciones de ingeniería digital. Ofrecen un servicio integral para la gestión de proyectos de base tecnológica
Neginet	Ayudar a las *start-up* a crecer aumentando sus equipos de desarrollo
Onapsis	Soluciones para proteger las aplicaciones empresariales de SAP y Oracle.
Process Technologies	Soluciones *end-to-end* que incluyen la selección y provisión de licencias de software y su mantenimiento, servicios de consultoría con mesa de ayuda, *hardware* o hosting y financiación completa de la solución
Simplex Software	Servicios de desarrollo de software personalizado y personal de TI dedicado a empresas de todo el mundo
United Virtualities Corp	Acelera los negocios, desarrollando tecnología y brindando servicios de consultoría en torno a ella, ayudando a sus clientes a planificar, desarrollar, implementar y administrar su estrategia tecnológica.
Vates	Consultoría y arquitectura en entornos multiplataforma y de múltiples proveedores
Wolox	Ayuda a los clientes a crear sus productos digitales como una ventanilla única para la creación de software
Zarego	Arquitectura de software y desarrollo personalizado de aplicaciones web y móviles

1.4.2.3. Vínculos con España

En lo relativo a la **relación entre los ecosistemas emprendedores** argentino y español, existen **asociaciones e iniciativas** para facilitar el establecimiento ("*soft landing*") de empresas argentinas en España.

Una de estas **asociaciones** es **ASAEDE** (**Asociación argentino-española de Emprendedores**) [26]. Es una comunidad de emprendedores, directivos y empresarios argentinos en España que ofrece apoyo, asesoramiento, *networking* y la oportunidad de **establecer relaciones duraderas y colaborativas** para el desarrollo y éxito de empresas y proyectos emprendedores.

Como ejemplo de **iniciativas** para facilitar el "*soft landing*" podemos citar **Acelerar España** [27], iniciativa **de carácter filantrópico** cuyo objetivo es acompañar a la internacionalización de *start-up* argentinas en su fase inicial del desembarco en España [22]. Esta iniciativa colabora estrechamente con otra iniciativa española, ***South Summit*** [28], como punto de encuentro para sus empresas. El objetivo es conectar con otros emprendedores, fortalecer su estrategia de internacionalización y ampliar su red de contactos.

Otras **iniciativas públicas y privadas** destacables [22] que han permitido la entrada con éxito al mercado español de múltiples *start-up* argentinas son ***Rising Up in Spain*** [29] y ***España-LATAM Scale-Up*** [30]. Ambas son programas de ***Invest in Spain*** [31], órgano español encargado de la promoción, atracción y mantenimiento de la inversión extranjera en España.

Rising UP in Spain es un programa para **facilitar a emprendedores extranjeros** el establecimiento de *start-up* extranjeras en España y la atracción de talento. En su sexta edición de 2022 se ha incorporado la figura del **socio local** para acoger a *start-up*

extranjeras. La empresa que quiera establecerse en España trabajará durante seis meses con el socio local (empresas y centros de tecnología en España) para desarrollar una necesidad tecnológica concreta vinculada a su negocio. La iniciativa ofrece estas ventajas:

- **Colaboración** con el socio local para el desarrollo un proyecto tecnológico.
- **Espacio de trabajo gratuito** durante 6 meses, facilitado por el socio local.
- **Contactos**: Potenciales clientes, inversores privados, públicos.
- **Asistencia para la creación de la empresa** en España (ver sección 1.5), asesoramiento fiscal y laboral y gestoría.
- **Visibilidad en medios** de comunicación especializados en emprendimiento.
- **Facilitación de la obtención de visados** (visados de emprendedores).

En los últimos cinco años se han presentado 122 empresas argentinas a esta iniciativa, y 10 de ellas resultaron ganadoras, existiendo al menos una ganadora argentina en cada edición.

Por otro lado, ***Spain-Latam Scale-Up*** es una iniciativa de *Invest in Spain*, BID LAB y Endeavor para la **atracción de *start-up*** de América Latina y el Caribe que tengan como objetivo su expansión e implantación en España como puerta de entrada al mercado europeo, tal y como se ha remarcado en este informe. Este programase inició en 2022 y ofrece a los ganadores **una inmersión de 5 días en España** para explorar los ecosistemas emprendedores de Madrid y Barcelona y conectar con actores clave para construir redes, canales de mercado formales y acceder a financiación.

Entre las 13 ganadoras de esta primera edición, se encuentran cuatro *start-up* argentinas:

- **Kilimo** (https://kilimo.com/): Plataforma de gestión de riego que permite monitorizar cultivos.
- **VU Security** (https://www.vusecurity.com/es/): Empresa **de ciberseguridad** especializada en el desarrollo de soluciones para la **protección de la identidad digital** y la **prevención del fraude**, de especial relevancia para este informe
- **MuniDigital** (https://munidigital.tech/): Empresa dedicada al desarrollo de herramientas digitales para gobiernos.
- **TheEye** (https://theeye.io/es/inicio/): Plataforma open source de automatización de procesos de negocios con IA.

Otra iniciativa española que colabora con el ecosistema argentino es **Startup Olé Latam RoadShow** [32]. Organiza encuentros en Chile, Argentina, México, Brasil y Colombia donde se reúnen *start-up*, corporaciones, inversores, aceleradoras, medios de comunicación y miembros de entidades institucionales.

1.5. Procedimiento para la creación de una empresa como extranjero residente fuera de la comunidad europea

Tras hacer un análisis completo del consumo de la ciberseguridad en países latinoamericanos y España, analizar la madurez de dichos países y mostrar empresas en el ramo representativas con el objeto de mostrar una panorámica de las oportunidades de negocio que los países latinoamericanos tienen si deciden “dar el salto” a España, es hora **de detallar en esta sección cómo dar ese “salto”**.

Existen distintas formas jurídicas en España para que puedas crear una *start-up*, pero la que exige menor capital y tiene trámites más sencillos, **gracias a la ley “Crea y Crece”**

[33] sería la **Sociedad de Responsabilidad Limitada** o SRL. Para fundar este tipo de empresa en España solo se requiere un **capital social mínimo simbólico de 1 euro** (**Artículo 2, Punto 1**). En esta sección nos vamos a centrar en detallar los requisitos y pasos para que puedas fundar una empresa de estas características.

Esta ley persigue impulsar que puedas crear tu empresa de una forma **rápida, ágil y al menor coste posible para ti**. Para ello, incentiva el uso de la tramitación telemática con el **Centro de Información y Red de Creación de Empresas** (**CIRCE**) [34] a través del **Documento Único Electrónico** (**DUE**) [35]. Se crea así una ventanilla única para **agilizar y simplificar tus trámites**, gestionada por la Dirección General de Industria y de la PYME del Ministerio de Industria, Comercio y Turismo español [36].

Esta nueva normativa supone un gran ahorro de tiempo a través uso de CIRCE y el DUE para la constitución de la *start-up*, haciendo el proceso mucho más ágil y con pasos que se pueden desarrollar en paralelo, pasando de tardar unas 3 semanas a unos 3 días [37]. Estos pasos los describiremos a lo largo de esta sección.

Para facilitar la constitución de tu *start-up*, esta ley (**Artículo 4**) obliga a determinados actores que intervienen en el proceso a que te proporcionen **una información mínima como fundador de empresas**. Dicha información es relativa a las ventajas que te supone emplear los **Puntos de Atención al Emprendedor** (PAE) [38] (definidos en el **Artículo 5, Punto 4**; **Artículo 2, Punto 6** de la ley "Crea y Crece") y el CIRCE mencionado anteriormente, y corresponde a **los notarios** e **intermediarios** que te asesoren y participen en la creación de tu empresa.

No obstante, esta sección también quiere mostrarte claramente las **ventajas de usar un PAE y el DUE** para la constitución de tu *start-up*, para que tengas claro cómo se ha mejorado en España el fomento ecosistema emprendedor gracias al uso de la **tramitación online** y puedas aprovecharte de estas mejoras.

Es obligatorio que tu empresa **disponga de certificado digital** para la tramitación online, pero éste se solicita una vez la empresa está constituida. Con respecto a los socios, no es obligatorio que dispongan de certificado digital si no hacen una actividad por cuenta propia.

No obstante, si vas a ser el administrador de la empresa, **sí es obligatorio que tengas un certificado digital para poder solicitar el de la empresa** (se hace telemáticamente con el certificado digital del administrador). En el caso de que quieras constituir la empresa de forma telemática **por ti mismo** (sin que te asista un PAE, como veremos posteriormente), sí que será necesario que tengas un certificado digital. Por estos motivos, este informe también incluirá el proceso de petición de un certificado digital.

1.5.1. ¿Y si tengo la doble nacionalidad?

Una persona que tiene dos nacionalidades posee un **doble vínculo jurídico** [39]. En otras palabras, es al mismo tiempo nacional de dos países, gozando de la plena condición jurídica de ciudadanos nacionales de ambos estados.

Si es tu caso, esto no quiere decir que estés sometido/a simultáneamente a las legislaciones de ambos países. Se articulan medios para que una persona con dos nacionalidades pueda **dar preferencia** a una de ellas, y sí tener una referencia a la hora de **articular las distintas relaciones Ciudadano-Estado**.

¿Cómo se establece esta preferencia? La mayor parte de los convenios de doble nacionalidad toma **el domicilio** como punto de referencia para eso. De esta forma, los ciudadanos con doble nacionalidad no estarán sometidos de forma constante a ambas legislaciones, sino sólo a la del país en el que tengan fijado su domicilio.

La gran ventaja para las personas emprendedoras que vengan de Latinoamérica, y que estén en condiciones de adquirir la doble nacionalidad, es que **no deben renunciar a la que tienen actualmente**. Por tanto**, puedes beneficiarte de la tramitación para emprendedores con nacionalidad española** que describiremos en los siguientes apartados si es tu caso.

En cualquier caso, se recomienda que **consultes con un PAE acerca de tu situación concreta**, para determinar si hay alguna particularidad que debas considerar y que la tramitación se haga sin problemas.

1.5.2. El DUE (Documento Único Electrónico) como medio para facilitar los trámites de creación de una sociedad limitada

El CIRCE te permite realizar los trámites de constitución y puesta en marcha de una Sociedad Limitada **por medios telemáticos** (https://paeelectronico.es/es-es/CreaEmpresa/Paginas/Tr%C3%A1mitesSLNE.aspx). Como decíamos, fue potenciado por la mencionada ley “Crea y Crece” [40] para minimizar tus desplazamientos durante el proceso, y que puedas aprovecharte de un **ahorro sustancial en tiempo y costes** como emprendedor.

Otro de los objetivos de esta ley es **simplificar tus trámites**. Siempre tienes la opción de hacerlos por ti mismo, pero si resides en un país Latinoamericano tendrás que familiarizarte con las particularidades de la ley española para ello. El gobierno de España ha pensado en tu caso, y por eso te brinda la posibilidad de usar los PAE para que lo hagas **de manera asistida**.

Por tanto, si necesitas ayuda y guía en todo el proceso, para minimizar las posibles barreras de tramitación que puedas tener para fundar tu *start-up*, te **recomendamos** que acudas a uno de los múltiples Puntos de Atención al Emprendedor (PAE) disponibles en la geografía del país (https://paeelectronico.es/es-es/Servicios/Paginas/BuscadorPAE.aspx). Si lo haces, **el único desplazamiento que tendrás que hacer es acudir a la notaría** (en uno de los pasos para constituir la *start-up* que veremos posteriormente), y además obtendrás toda la **asistencia** necesaria para simplificar todo el proceso (ver Figura 28).

Figura 28. Funciones principales de un PAE [41]

Otra de las razones que aumentaba la complejidad del proceso eran **los diferentes pasos e impresos a cumplimentar** que requería la formación de la *start-up*. Como ya hemos dicho, el impulso del uso del DUE que ha supuesto la ley "Crea y Crece" supone que el proceso te será mucho más sencillo y rápido ahora (**Artículo 5**, **Puntos 5-6**).

El DUE es **un documento único que tienes que rellenar de forma online** [35]. Gracias a él se **automatizarán muchos de los pasos necesarios** para la constitución de tu *start-up* (ver sección 1.5.6). Está regulado en la disposición adicional tercera del texto refundido de la Ley de Sociedades de Capital, aprobado por Real Decreto Legislativo 1/2010, de 2 de julio, y en la Figura 29 puedes ver el aspecto que tiene.

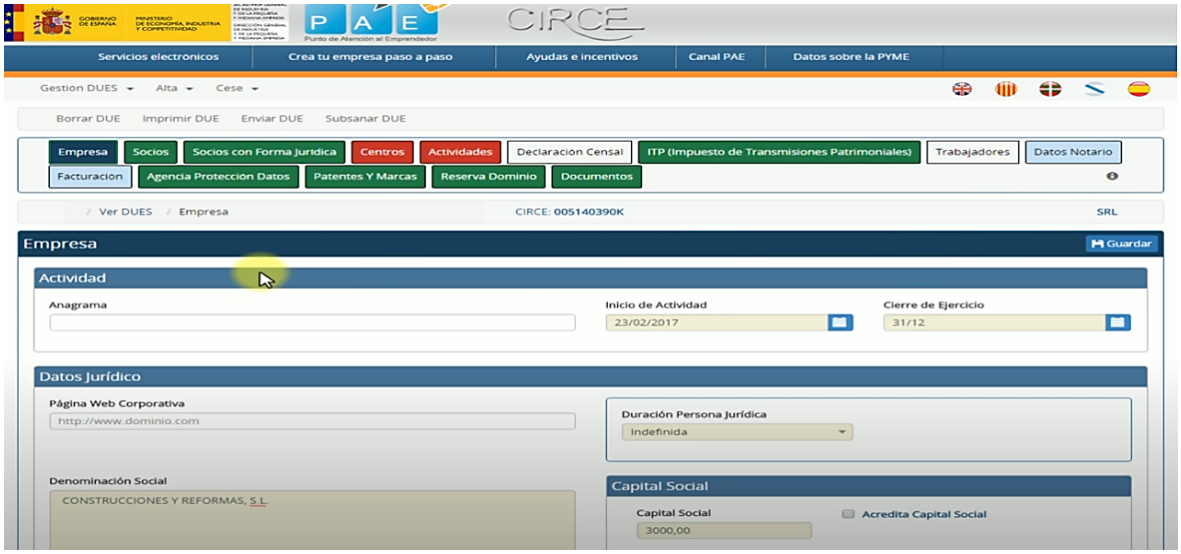


Figura 29. El DUE [35]

Una vez cumplimentes y envíes el DUE, el sistema de tramitación telemática (STT-CIRCE) **envía automáticamente a cada organismo interviniente en el proceso la parte del DUE que le corresponde**. Esto permite que cada organismo realice el trámite que le compete, sin que tengas que preocuparte ni del envío ni de a qué organismo debes hacerlo.

Obviamente, necesitarás **obtener información actualizada** del proceso de constitución de tu *start-up*, y eso también está pensado por el sistema de tramitación. No solo podrás consultar tu expediente telemáticamente: https://paeelectronico.circe.es/Account/LoginConsultaExpediente, sino también **recibir mensajes a tu móvil** cuando terminen los trámites más significativos del proceso que se describirá en la sección 1.5.6.

Podrás optar así fácilmente por la constitución de tu sociedad mediante escritura pública **con formato estandarizado y estatutos tipo** gracias a lo especificado por la ley "Crea y Crece" ([33], **Artículo 15**). En caso de que no tengas estatutos tipo, se aplicará lo dispuesto en dicho Artículo 15, pero con una serie de particularidades desarrolladas en el Artículo 16 de la misma ley que debes cumplir. Se recomienda en ambos casos acudir y pedir asistencia al PAE para conocer los detalles del proceso.

Estos modelos simplificados de los estatutos-tipo en formato estandarizado están disponibles **en todas las lenguas oficiales** en todas las comunidades autónomas, por si fuera necesario para establecer tu *start-up*, y que no tengas que preocuparte de este aspecto. Además, se podrán utilizar **modelos simplificados de apoderamientos** en el formato estandarizado, cuyo contenido (con facultades estandarizadas y codificadas) se desarrollará reglamentariamente también en todas las lenguas oficiales de todas las Comunidades Autónomas.

En cualquier caso, la **agilización y automatización de la creación de la *start-up* requiere el envío y cumplimentación correcta del DUE**, por lo que en las siguientes secciones vamos a detallar lo que se necesita antes de que puedas comenzar el proceso.

1.5.3. Documentación previa necesaria para la obtención del DUE

Antes de pasar a cumplimentar el DUE, es necesario **que estés en posesión de una determinada documentación**. Esta difiere en caso de que seas o no extranjero, y en este último caso si el país de origen pertenece o no a la UE. **Para socios de tu *start-up* no extranjeros** es necesario original y fotocopia del DNI, y de algún documento que acredite el número de afiliación a la seguridad social. Esto puede ser una opción para ti si tienes la doble nacionalidad, y es algo que recomendamos consultar acudiendo a un PAE.

Si resides en **Latinoamérica** y tienes la condición de socio extranjero no de la UE por no tener otra nacionalidad, es necesario **disponer de un NIE** y permiso de residencia y trabajo por cuenta propia (siempre y cuando no seas únicamente un socio capitalista). Un socio extranjero de la UE solo necesita un NIE comunitario.

Por otro lado, en el caso de tener **socios extranjeros capitalistas** (sin residencia ni actividad en la empresa) es necesario aportar el NIE por asuntos económicos. Finalmente, en caso de **socios casados** es necesario el DNI o NIE del cónyuge.

Quizá pueda preocuparte si la obtención de un NIE **implica contraer obligaciones fiscales en España**. **No es así**. El único efecto es tener un número de identificación ante las autoridades españolas para extranjeros que tengan intereses económicos, profesionales o sociales en el país. Por otro lado, los únicos requisitos para obtenerlo son que no te encuentres en el país de forma irregular y que comuniques los motivos por el que lo solicitas. Veamos a continuación cómo hacerlo.

1.5.3.1. Obtener tu NIE

Hay **dos formas de obtener el NIE**, dependiendo de si te encuentras en España o en tu país de origen en el momento en el que vayas a solicitarlo (https://sede.policia.gob.es/portalCiudadano/_es/tramites_extranjeria_tramite_asignacion_nie.php):

1. **Si estás en España**, deberás pedir cita previa para acudir a una **Comisaría de Policía**. Es muy sencillo encontrar una que esté cercana a tu localización actual (https://sede.policia.gob.es/portalCiudadano/_es/dependencias_localizador.php). También es válido hacer el trámite en alguna de las **Oficinas de Extranjería**. Como en caso de las comisarías, también hay muchas repartidas por el territorio nacional (https://www.mptfp.gob.es/portal/delegaciones_gobierno/extranjeria/extranjeria_ddgg.html).

2. **Si estás en tu país de origen**, debes ir a las **Oficinas Consulares** que España haya establecido en él, que puedes consultar aquí: https://www.exteriores.gob.es/es/EmbajadasConsulados/Paginas/index.aspx. El consulado español lo solicitará a su vez a la **Comisaría General de Extranjería**. La obtención del NIE en estos casos puede tardar un **máximo de cinco días** desde la entrada de la solicitud en el registro del órgano competente para su tramitación.

   Ten en cuenta que seguramente **tendrás que pedir cita previa** para la realización de este trámite, por lo que te recomendamos contactar antes con el consultado para ver cómo hacerlo. La **documentación** que tengas que aportar en el consulado debería ser la siguiente, pero se recomienda también hacer la consulta en el consulado por si fuese necesario aportar algún documento adicional:

   - Copia del **pasaporte**

- Rellenar un impreso para explicar las **razones por las que solicitas el NIE** (https://sede.policia.gob.es/portalCiudadano/sede_electronica/extranjeria/EX15.pdf).

- **Pago de la tasa por la gestión** de la obtención de tu NIE (documento Modelo 790, Código 012: https://sede.policia.gob.es/Tasa790_012/).

Una vez que tengas el NIE, **podrás solicitar un certificado electrónico** para simplificar los trámites telemáticos con la administración que vayas a hacer en el futuro. La siguiente sección te explica cómo hacerlo.

1.5.3.2. Obtener tu certificado electrónico

El **Certificado de Persona Física o de Usuario**, es un **documento digital** que contiene tus datos identificativos. Con el podrás identificarte en Internet e intercambiar información con otras personas y organismos **de forma segura**, con la garantía de que sólo tú y tus interlocutores podrán leerla.

Hay **3 formas distintas** para que puedas obtener tu Certificado electrónico de Ciudadano (https://www.sede.fnmt.gob.es/certificados/persona-fisica), y te damos los enlaces donde puedes consultar toda la información de la que más te convenga en tu situación personal:

1. **Con identificación por video** (https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-video-identificacion): es una forma de tramitarlo añadida muy recientemente, que puede ayudarte a hacerlo desde tu país de origen directamente. Necesitas un teléfono móvil para escanear un código QR y **pagar una tasa de 2,99 euros** por el trámite (el certificado en sí es gratis).
2. **Con acreditación presencial en una oficina o consulado de tu país** (https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software). Es la forma "clásica" de hacerlo. Tras seguir las indicaciones y finalizar el trámite, recibirás un correo electrónico de la FNMT con un **código de solicitud**. Hecho esto, tienes que **acreditar tu identidad** como solicitante en un consulado (como en el caso del NIE), presentándote con esta documentación:
   - El **código de solicitud** que te llegó a la cuenta de correo electrónico.
   - **Tarjeta Roja/Verde/Blanca de Identificación de Extranjeros** donde conste el NIE junto con el **pasaporte**, o bien el **documento oficial de concesión del NIE** que vimos en el paso anterior, junto con el **pasaporte**.
3. **Utilizando el DNIe** (https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-con-dnie), aunque sólo si tuvieras uno en vigor por tener, por ejemplo, la doble nacionalidad.

Hecho esto, **recibirás un correo electrónico** de la Fábrica Nacional de Moneda y Timbre indicando que ya puedes descargar el certificado, el cual quedará almacenado en el navegador de tu sistema operativo con un plazo de validez determinado.

1.5.4. Información previa necesaria para la obtención del DUE

Aparte de la documentación mencionada necesitarás disponer de los siguientes **datos** para poder rellenar el DUE satisfactoriamente:

- **Epígrafe AE** (Actividades Económicas) correspondiente a la *start-up* que quieres establecer, que puedes consultar aquí: http://www.epigrafesiae.com/

- **Código de la actividad** que vas a desempeñar según la **Clasificación Nacional de Actividades Económicas** (CNAE), consultable en esta dirección: https://www.cnae.com.es/lista-actividades.php
- **Datos del domicilio de tu empresa** y de la **actividad empresarial** que va a desarrollar (incluidos los metros cuadrados del lugar de la actividad, código postal y teléfono).
- **Porcentajes de participación** en el capital social de la empresa.
- **Datos del administrador/es** y **tipo de administración** que va a tener la empresa (individual, solidaria o mancomunada).
- **Si quieres adscribirte al Régimen Especial de Trabajadores Autónomos** (RETA), es necesario aportar la base de cotización elegida, mutua de Incapacidad Temporal (IT) y si optarás a la cobertura por accidente de trabajo y enfermedad profesional (AT-EP). Para algunos socios es obligatorio (no se puede elegir) estar dado de alta en el RETA, por ejemplo, un socio que tiene más de un 25% de participación y es administrador.
- **Si hay socios casados**, es necesario disponer de documentación que indique el **régimen del matrimonio**.
- En el **aspecto económico** se necesitarán además los siguientes datos:
    - Información para realizar el **pago al Registro Mercantil Provincial** (RMP). Se realizará por domiciliación bancaria, y será necesario que aportes un **número de cuenta o una tarjeta bancaria**.
    - Si el(los/as) administrador(es/as) y/o socios/as deben darse de alta como Autónomo, deberán aportar un **número de cuenta bancaria para realizar la domiciliación de la cuota del RETA**. El socio/a que esté obligado/a al pago no tiene por qué ser el titular de la cuenta.

De acuerdo con lo establecido por la ley “Crea y Crece” [40], los documentos que aportes que por alguna razón estén redactados en lengua extranjera **se acompañarán de una traducción** al castellano, o a otra lengua oficial en la provincia del domicilio social, hecha **por traductor jurado**. Esta disposición se entiende sin perjuicio del régimen lingüístico aplicable en las Comunidades Autónomas en las que otras lenguas españolas distintas del castellano son también oficiales. Ten en cuenta que **para emprendedores latinoamericanos** esta es una **barrera del idioma fácilmente evitable**, como decíamos al principio del informe.

Los documentos públicos extranjeros deberán ir provistos de la correspondiente **apostilla o legalización diplomática**, salvo en los casos exceptuados por disposición de la ley o de los **convenios internacionales** vigentes en España. Recomendamos pedir asesoría a un PAE en caso de que tengas que aportar un documento de este tipo en el proceso para consultar la mejor forma de hacerlo.

En todo caso, la intervención de Cónsul que otorgue dichos documentos, en funciones notariales, así como la legalización por autoridades españolas de documentos notariales otorgados en el extranjero, quedarán **sujetas a las obligaciones tributarias establecidas** en el ordenamiento tributario español.

1.5.5. Trámites previos a la solicitud del DUE

El único trámite previo a la cumplimentación del DUE es la **aportación del Capital Social**. No obstante, en el momento de cumplimentar el DUE **sólo es necesario que indiques el**

importe de capital y la participación de cada socio de tu empresa. Recuerda que gracias a la ley "Crea y Crece" este capital social **puede ser simbólico** (**1€**) si así lo deseas. El objetivo es que puedas **usar estos recursos en otras áreas** que requieran más atención para poner en marcha tus ideas.

No obstante, **lo más recomendable** es seguir aportando el capital social de 3.000 euros. Los socios responden solidariamente frente a la sociedad, y lo que aporta la Ley "Crea y Crece" es que **ya no es obligatorio aportar en la notaría el certificado** de haber ingresado en la cuenta bancaria dicho capital social. Si se pone que el capital social es de 1 euro, contablemente es una empresa **que no puede hacer ninguna operación hasta que los socios de esta no metan dinero**.

Aunque en esta primera fase de la tramitación solo hace falta que indiques el importe, posteriormente será necesario que **hagas la acreditación real de esas aportaciones** al capital que has indicado. Esto tendrás que hacerlo ante el Notario, posteriormente al envío del DUE, y en el momento de la firma de la escritura de constitución (fase del proceso descrito en la sección 1.5.6). Para ello entregarás **un certificado bancario** que acredite el depósito del dinero correspondiente por cada uno de los socios que realiza la aportación.

No será necesario acreditar la realidad de las aportaciones dinerarias si los fundadores de una *start-up* manifiestan en la escritura que responderán solidariamente frente a la sociedad y frente a los acreedores sociales de la realidad de estas. Esto es otra novedad introducida por la ley "Crea y Crece" a la que te puedes acoger si lo deseas.

1.5.5.1. Creación de una cuenta bancaria para el proceso en España

Como mencionamos anteriormente, a partir de la entrada en vigor de la mencionada ley "Crea y Crece", el **capital social mínimo** para la sociedad limitada que los socios habrán de aportar puede ser simbólico (**1 €)**.

Para aportar la cantidad de capital social que desees, una vez que obtengas el **certificado de la denominación social** durante el proceso de tramitación del DUE descrito en la siguiente sección, será imprescindible que **abras una cuenta bancaria a nombre de la empresa** a constituir. Además, también se deberá ingresar el capital inicial mínimo que quieras aportar **de forma íntegra**. La entidad financiera te va a pedir el certificado de denominación social de tu empresa para ello.

A partir de ese momento, el banco te abrirá una cuenta de "**Sociedad en constitución**" y emitirá el **certificado del ingreso del capital social**, que es el que mencionamos que deberá presentarse ante la notaría y que ya no es obligatorio.

Puedes abrir una cuenta bancaria en España desde el extranjero de distintas formas:

1. **De forma online**, siguiendo el procedimiento que la entidad bancaria que hayas elegido establezca para ello
2. **Apoyarse en una oficina de tu entidad o de representación de esta en el extranjero**. Muchas de las entidades españolas tienen oficinas en el extranjero o de representación de esta por acuerdos suscritos con entidades de tu país.

   En este caso dirígete a la oficina donde vayas a abrir la cuenta para que manden la documentación a la que tengas más cerca y allí firmar el contrato de esta, dándose fe de la titularidad de la cuenta.

3. Si no tienes ninguna de estas posibilidades, puedes **mandar un poder** (el recomendable es que sea específico **sólo para la apertura de la cuenta**) a una persona que pueda tramitártelo en España.

   En todas las Embajadas y Consulados de España en el extranjero los españoles y los ciudadanos extranjeros pueden otorgar documentos notariales ante el Cónsul, en funciones notariales, que surtirán efectos ante cualquier autoridad en España sin necesidad de legalización, ni por el Consulado que autorizó el documento, ni por la Sección de Legalizaciones del Ministerio de Asuntos Exteriores y de Cooperación.

1.5.5.2. Envío del DUE

Una vez que hayas llevado a cabo las actuaciones indicadas en las secciones anteriores, y estés en posesión de la información y documentación requerida, **podrás cumplimentar y enviar el DUE**. Como ya se ha dicho, la cumplimentación del DUE se puede realizar de dos maneras:

1. **Hacerlo tú mismo/a**. En este caso será necesario que dispongas de un certificado electrónico (ver sección 1.5.3.2). Una vez lo envíes telemáticamente, el DUE será revisado por los técnicos de la DGIPYME y, si detectan algún error, se pondrán en contacto contigo para subsanarlo. En caso contrario, pondrán en marcha el resto del proceso.
2. **Asistido por un PAE**, para que te ayuden a cumplimentar el DUE. Esta **es la forma que recomendamos** para que el proceso sea más ágil y menos propenso a errores.

Dado que tu sociedad necesitará una **denominación** que no podrá coincidir con ninguna de las sociedades ya existentes en España, durante este proceso se solicitará la **reserva de la denominación** al Registro Mercantil Central. Para ello deberás aportar **hasta cinco denominaciones sociales alternativas**. El Registro Mercantil Central emitirá el correspondiente **certificado negativo de denominación** (certificando que ninguna otra empresa tiene la misma denominación), siguiendo el orden que propongas, dentro de las 6 horas hábiles siguientes a la solicitud.

Con el envío del DUE, se genera una **solicitud de cita con la Notaría** elegida para el otorgamiento de la **escritura pública** de constitución de tu sociedad. Esta cita **se obtiene de forma inmediata** por medio de una comunicación en tiempo real con el sistema de la Agenda Notarial, que facilita los datos de la notaría, la fecha y hora de la cita. Deberás acudir en la fecha y hora de esta cita aportando el certificado de desembolso del capital social (visto en el apartado 1.5.5). La **escritura pública contendrá la siguiente información**:

- **La identidad** del socio o socios.
- **La voluntad de constituir** una sociedad de responsabilidad limitada.
- **Las aportaciones que cada socio** realice a la sociedad y la numeración de las participaciones asignadas en pago.
- La determinación del **modo concreto en que inicialmente se organice la administración**, en caso de que sus estatutos prevean diferentes alternativas.
- La **identidad de la persona** o personas que se encarguen inicialmente de la **administración y de la representación social**.
- Los **pactos y condiciones** que los socios juzguen convenientemente establecer, siempre que no sean contrarios a lo establecido en las leyes.

- Los **estatutos de la sociedad** en los que deberá constar al menos la siguiente información. La elaboración de los estatutos se puede simplificar si se usan los **estatutos tipo** mencionados en el apartado 1.5.2.
  - La **denominación** de la sociedad.
  - El **objeto social**.
  - El **domicilio social**.
  - El **capital social**, las participaciones en que se divida, su valor nominal y su numeración correlativa y, si fueran desiguales, los derechos que cada una atribuya a los socios y la cuantía o a la extensión de éstos.
  - El modo o modos de **organizar la administración** de la sociedad, el número de administradores (o, al menos, el número máximo y el mínimo), así como el plazo de duración del cargo y el sistema de retribución, si la tuvieren.
  - El modo de **deliberar y adoptar sus acuerdos** los órganos colegiados de la sociedad.

1.5.6. Pasos que realiza el sistema telemático de creación de empresas, sin intervención del emprendedor, una vez cumplimentado el DUE

Como comentábamos anteriormente, gracias a la ley “Crea y Crece” [40] el envío del DUE hace que **no tengas que intervenir en los siguientes procesos** que tienen lugar para la constitución de tu *start-up*, que ahora se realizaran automáticamente, agilizando trámites.

- **Solicitud del NIF provisional**: La Administración Tributaria, con la información suministrada por la Notaría, envía el NIF provisional. A continuación, se comunica la Declaración Censal a la Administración Tributaria competente, procediendo a la realización del Alta Censal.
- **Liquidación del Impuesto de Transmisiones Patrimoniales y Actos Jurídicos Documentados**: La ley “Crea y Crece” establece que la constitución de sociedades está **exenta del pago** del Impuesto de Transmisiones Patrimoniales y Actos Jurídicos Documentados (ITP/AJD). Sin embargo, es necesaria la obtención del **justificante del impuesto** (Modelo 600) por parte de la Comunidad Autónoma pertinente. Esta justificación se obtiene a través del STT-CIRCE, **sin que tengas que preocuparte de solicitarla**.
- **Inscripción en el Registro Mercantil Provincial**: El Registrador realiza la calificación de la Sociedad y la inscribe en el Registro. El Registro Mercantil Provincial enviará los datos de la resolución de inscripción firmados electrónicamente, para que el sistema pueda continuar con la tramitación.
- **Trámites en la Seguridad Social**: Con el envío del DUE, la Tesorería General de la Seguridad Social genera los Códigos de Cuenta de Cotización. Además, proceden a la afiliación, en su caso, y al alta de los socios y de los trabajadores de la empresa, si los hubiese.
- **Expedición de la Escritura inscrita**: La Notaría recibe la información del Registro Mercantil Provincial e incorpora a la matriz de la escritura, los datos de la resolución de inscripción registral. Esta procederá a la calificación e inscripción dentro del plazo de las **6 horas hábiles** siguientes a la recepción telemática de la escritura, entendiéndose por horas hábiles a estos efectos las que queden comprendidas dentro del horario de apertura fijado para los registros.

Tras la citada inscripción, **tu empresa adquiere personalidad jurídica**, lo que la capacitaría para presentarse a iniciativas de fomento del emprendimiento como *Cybersecurity Ventures* [42].

- **Solicitud del NIF definitivo de la sociedad**: La Administración Tributaria confirmará el NIF definitivo al STT-CIRCE, para lo cual se le remitirá previamente una copia autorizada de la Escritura inscrita. Asimismo, te notificará la finalización del proceso y **remitirá el NIF definitivo** al domicilio fiscal de la sociedad.

Con este trámite **finaliza el proceso de creación de tu empresa**. Ahora, de acuerdo con lo indicado por la ley "Crea y Crece" [33], el sistema de tramitación telemática del CIRCE dará traslado inmediato a los fundadores que así lo soliciten y al notario autorizante de la escritura de constitución y de la certificación electrónica a que se refiere el apartado anterior, sin coste adicional.

Dicha certificación será necesaria para **acreditar la correcta inscripción** en el Registro de las sociedades, así como la inscripción del nombramiento de los administradores designados en la escritura.

Asimismo, podrás solicitar en cualquier momento, una vez inscrita la sociedad, una **certificación actualizada del contenido de la hoja registral** de aquella que será expedida por el Registrador bajo su firma electrónica, y provista de un código de validación de conformidad con lo previsto para las certificaciones con información continuada.

La autoridad tributaria competente notificará telemáticamente al sistema de tramitación telemática del CIRCE el carácter definitivo del Número de Identificación Fiscal. Este último lo trasladará de inmediato a los fundadores de la empresa.

Cuando el registrador **aprecie defectos u obstáculos** que impidieran la inscripción de tu empresa, extenderá una **nota de calificación negativa** y la notificará al CIRCE, que la trasladará de inmediato a los fundadores y al notario. Los fundadores de una empresa podrán en este caso atribuir al notario autorizante la f**acultad de subsanar electrónicamente los defectos advertidos** por el registrador en su calificación, siempre que aquel se ajuste a la calificación y a la voluntad manifestada por las partes.

Desde el Punto de Atención al Emprendedor se procederá también a **realizar los trámites relativos al inicio de actividad** de tu empresa, mediante el envío de la información contenida en el DUE a la autoridad tributaria, a la Tesorería General de la Seguridad Social, y en su caso, a las administraciones locales y autonómicas para llevar a cabo las comunicaciones, registros y solicitudes de autorizaciones y licencias necesarias para la puesta en marcha de la empresa. La publicación de la inscripción de la sociedad en el "**Boletín Oficial del Registro Mercantil**" (BORME) estará **exenta del pago de tasas (Artículo 12** de la ley "Crea y Crece"**)**.

1.5.7. Trámites complementarios a la solicitud del DUE

Hay una serie de **trámites complementarios** que puedes realizar si los consideras necesarios a través de la cumplimentación del DUE.

- **Solicitud de reserva de Marca o Nombre Comercial en la Oficina Española de Patentes y Marcas (OEPM)**: Este trámite es opcional y se hace si lo solicitas al rellenar el DUE. Una vez hagas la solicitud, y pagues la cantidad requerida a través del STT-CIRCE, la Oficina Española de Patentes y Marcas continuará con el procedimiento administrativo ordinario para el registro del signo distintivo.

El registro de una marca o un nombre comercial otorga a tu empresa el **derecho exclusivo a impedir que terceros comercialicen productos/servicios idénticos o similares** con el mismo signo distintivo.

- **Solicitud de Licencias en el Ayuntamiento**: En aquellos ayuntamientos que colaboran con CIRCE, o estén adheridos al proyecto **Emprende en 3** [43], se realizará la **solicitud de licencias o la declaración responsable** según el tipo de actividad de la empresa.
- **Comunicación de los contratos de trabajo al Servicio Público de Empleo Estatal**: Este trámite consiste en realizar la legalización o alta de los contratos de trabajo de los trabajadores por cuenta ajena, si los hubiera.

1.5.8. Trámites no incluidos en el sistema

Existen una serie de trámites necesarios para constituir tu empresa que **todavía no están cubiertos por CIRCE**. Entre ellos:

- **La comunicación de la apertura del centro de trabajo**: Este es un trámite incluido en el procedimiento telemático únicamente en la Región de Murcia y la Comunidad de Madrid por el momento. Es necesario en caso de que tengas contratados trabajadores.
- **La obtención y legalización de los libros**:
  - Legalización del Libro de actas, del Libro registro de socios, del Libro-registro de acciones nominativas y del Libro registro de contratos entre el socio único y la sociedad en el **Registro Mercantil Provincial**.
  - Legalización del Libro diario y del Libro de inventarios y Cuentas Anuales en el **Registro Mercantil Provincial.**
- **Inscripción, en su caso, en otros organismos oficiales y/o registros**
  - Darse de alta en el Censo de empresarios ante la **Agencia Tributaria.**
  - Dar de alta a socios y administradores en los correspondientes regímenes de la Seguridad Social en la **Tesorería General de la Seguridad Social**.

Debes también tener en cuenta que, dependiendo de la naturaleza de tu actividad y del lugar físico donde la desarrolles, puede que debas **cumplir algunos requisitos más**, como por ejemplo el de disponer de una **licencia de actividad**, que deberás solicitar al Ayuntamiento. Se recomienda contactar con dicho ayuntamiento para ver en qué casos es necesario y el procedimiento de solicitud.

1.6. Ayudas y reglamentación para la creación de *start-up* en 2023 en España

Si una empresa latinoamericana “da el salto” a España, una vez fundada y establecido su domicilio social en el país, puede acceder a todos los fondos y ayudas a nivel nacional y autonómica (compra pública innovadora, etc.), así como aprovecharte de las **ventajas y ayudas** para las empresas emergentes que el gobierno del país ha puesto en marcha.

Para que las conozcas, en esta sección daremos referencias a información de la ley “**Crea y Crece**” [33] y la “**Ley de Start-ups**” [44] que sean interesante (gestión, información, financiación, etc.) en cada una de las fases vistas para la creación de tu *start-up*.

1.6.1. Creación de la *start-up*

La **"Ley de *Start-ups*"** española favorece la inversión con medidas que faciliten el desarrollo y crecimiento de empresas emergentes innovadoras de base tecnológica. Contempla una serie de **incentivos** de naturaleza **fiscal**, **societaria** y **otras áreas.** Además de requerirles desarrollar un **proyecto innovador** y con un **modelo de negocio escalable**, como mencionamos antes, define (**Artículo 3**) requisitos para beneficiarse de sus incentivos como:

- Empresa de **nueva creación o llevar menos de 5 años** inscrita (7 años para ciertos sectores). Esto daría a una *start-up* en ciberseguridad que desarrolle su tecnología en España tiempo suficiente para su consolidación, prueba y puesta en marcha.
- Empresa **localizada en España** que no puede surgir de modificaciones estructurales de empresas tradicionales.
- **60 % de la plantilla con un contrato laboral en España**. Aquí vuelve a cobrar importancia el hecho de que **no hay barreras idiomáticas** con emprendedores latinoamericanos que decidan establecerse en España.
- **No haber distribuido dividendos** o retornos en caso de cooperativas.
- **No cotizar en un mercado regulado**.

Por tanto, el primer paso es estudiar su **artículo 4** para ver como solicitar tu evaluación como *start-up* en https://www.enisa.es/. Otros aspectos que considerar antes de esto son:

- Los beneficios para **nómadas digitales** para visado y residencia (**CAPÍTULO V BIS**), que facilitan atraer talento extranjero para desarrollar **innovaciones**.
- Si necesitas estar en un **entorno controlado de prueba** *(regulatory sandbox),* que exceptúen la normativa general durante un año bajo la supervisión de regulador y te permita evaluar la utilidad, viabilidad y el impacto de tus innovaciones (**Artículo 16**). Te permitiría por ejemplo probar **ideas de negocio en ciberseguridad** en un entorno más flexible.
- Si te beneficia la compra pública innovadora (**Título III**)
- Las distintas facilidades en el acceso a ayudas públicas

1.6.2. Crecimiento de la *start-up*

Cuando tu *start-up* de ciberseguridad sea calificada como emergente por la ENISA, tendrá derecho a una serie de beneficios **fiscales** para ayudar a su crecimiento definidos en la "**Ley de *Startups***":

- **Artículo 7**:
  - **Reducción del tipo impositivo** en el impuesto de sociedades a un 15%
  - Posibilidad de **aplazar la deuda tributaria** entre 12 y 16 meses en los primeros ejercicios
- **Disposición final tercera**
  - **Exención fiscal por entrega de acciones** o participaciones a los empleados de las empresas (*stock options*) de hasta 50.000 € al año
  - **Elevación de la base máxima de deducción** por inversión de 60.000 a 100.000 €/año y del tipo de deducción del 30 al 50%
  - **Las comisiones a éxito de las gestoras de capital riesgo** (*carried interest*) tributarán con una exención de hasta el 50%, beneficiando a estas fuentes de financiación típicas de *start-up* mencionadas antes.

También tendrán **beneficios desde el punto de vista formal y societario**, como por ejemplo la posibilidad de adquirir **autocartera** hasta un 20% para entrega a empleados, administradores y colaboradores de estas empresas **(Artículo 10)**.

Por otro lado, la ley "**Crea y Crece**" también contiene medias para **impulsar** la creación de empresas y **facilitar** su **crecimiento** y **expansión**, como medidas específicas para **combatir la morosidad comercial** y evitar tensiones en los presupuestos de tesorería de tu *start-up* [45], como la adopción general y obligatoria la **factura electrónica** (**Artículo 12**), limitar el acceso a subvenciones a empresas morosas **(Artículo 11)** y mejorar la identificación de empresas morosas **(Artículo 9, Punto 1; Artículo 13; Artículo 9, Punto 2).**

Esta ley también incluye una serie de medidas para que tu *start-up* pueda **operar y crecer mejor**, eliminando regulaciones innecesarias y haciendo procesos más ágiles [45], como facilitar que pueda ejercer su actividad económica **en todo el territorio nacional** (**Artículo 6**, **Puntos 1-2**). También amplia el catálogo de actividades económicas **exentas de licencia** [40] (**Artículo 8**).

Finalmente, en esta ley se combate una de las causas principales de fallo en las *start-up* mencionadas antes, **facilitando que encuentres fuentes de financiación** como el ***crowdfunding*** (**Capítulo V**), la inversión colectiva y el capital riesgo (**Capítulo VI**) [40].

1.6.3. Cese de actividad

El nuevo marco legislativo español también contempla una serie de medidas que actúan en estos casos. Por ejemplo, **la ley de *start-up*** contempla la exención de incurrir en **causa de disolución por pérdidas** en los 3 primeros años **(Artículo 13)**.

Por otro lado, la ley "**Crea y Crece**" da más garantías a los acreedores haciendo que, mientras que el capital de constitución no alcance los 3000€, haya que hacer una **reserva mínima del 20% del beneficio** y que, en caso de **liquidación**, los socios de la empresa respondan con la diferencia entre 3000€ y el capital suscrito inicialmente.

1.7. Conclusiones

En este informe hemos tratado de hacer un recorrido completo por el **mercado de la ciberseguridad en España, Europa y especialmente Latinoamérica**, hablando del consumo de soluciones de ciberseguridad, cómo se divide el mismo y el motivo por el que España es un país atractivo como destino para empresas latinoamericanas en el ramo.

Por otro lado, se ha hecho otro análisis que permite tener una idea del **grado de madurez en ciberseguridad** de una representación de países latinoamericanos, destacando sus fortalezas y debilidades y creando un perfil del país que puede ayudar a mostrar en qué áreas hay un mayor desarrollo de soluciones e innovación a nivel global, que pueden ser potencialmente más exportables y expandir el mercado de la ciberseguridad en el país correspondiente.

Una tercera sección mostró un **listado de las empresas más relevantes** (y sus líneas de negocio) en dos de esos países, que dan una idea clara de la diversidad del mercado existente en ellos, aunque se hayan evaluado en posiciones muy diferentes en los rankings que miden la madurez de la ciberseguridad en cada país.

No obstante, todo este análisis previo tiene como objetivo **facilitar a empresas latinoamericanas a que inviertan en España**, como puerta de acceso al mercado europeo. No podríamos hacer esto de forma completa sin detallar de forma pormenorizada el procedimiento de establecimiento de una *start-up* en España y las ventajas de las que puede disfrutar una vez establecida, gracias a la labor legislativa y de impulso hecha por el gobierno de España en este sentido. Este objetivo final ha sido el centro de la última parte de este informe.

Con toda esta información esperamos sinceramente **ayudar y animar a emprendedores/as a "dar el salto" al mercado español** por las oportunidades a la hora de establecer nuevos mercados para el negocio de ciberseguridad que supone y que hemos intentado destacar de manera clara en este informe.

2. REFERENCIAS

[1] Gartner, "Forecast: Information Security and Risk Management, Worldwide, 2020-2026, 2Q22 Update," Gartner, 2022.

[2] INCIBE, "Estrategia española conjunta de las industrias de ciberseguridad y ciberdefensa," 2023.

[3] I. T. Union, "Global Security Index 2020," 2020.

[4] ISMS Forum, "III Indicador de madurez en Ciberseguridad," 2022.

[5] CSIRT.es, "FAQ: ¿Qué es un CSIRT/CERT?," 2023. [Online]. Available: https://www.csirt.es/index.php/es/faq. [Accessed 19 6 2023].

[6] ICEX, "El mercado de la ciberseguridad en Argentina," Buenos Aires, 2021.

[7] CSIRTAmericas Network, "Protegiendo a las Américas en el ciberespacio," 2023. [Online]. Available: https://csirtamericas.org/es. [Accessed 20 6 2023].

[8] ICEX, "Ciberseguridad en México," 2020.

[9] ICEX, "Ciberseguridad en Brasil," 2022.

[10] ICEX, "Ciberseguridad en Colombia," 2021.

[11] ICEX, "El mercado de la Ciberseguridad en Chile," Santiago de Chile, 2017.

[12] ICEX, "Ciberseguridad en Perú," 2018.

[13] revistaciberseguridad.com, "Estrategia de ciberseguridad en Uruguay," 21 4 2023. [Online]. Available: https://revistaseguridad360.com/noticias/ciberseguridad-en-uruguay/. [Accessed 21 6 2023].

[14] ciberseguridad.com, "Organimos y entidades en España," 2023. [Online]. Available: https://ciberseguridad.com/normativa/espana/organismos/. [Accessed 20 6 2023].

[15] OEA, "CIBERSEGURIDAD: Riesgos, avances y el camino a seguir en América Latina y el Caribe," 2020.

[16] B. Arrieta Sagredo, "El ecosistema de emprendimiento en Mexico," ICEX, Mexico, 2023.

[17] ciberseguridad.com, "Empresas de Ciberseguridad en México," 2023. [Online]. Available: https://ciberseguridad.com/empresas/mexico/. [Accessed 23 6 2023].

[18] f6s.com, "10 Top Cyber Security Startups and Companies in Mexico," 2023. [Online]. Available: https://www.f6s.com/companies/cyber-security/mexico/co. [Accessed 23 6 2023].

[19] forbes.com.mx, "Crean en México el primer hub de ciberseguridad en América Latina," 26 11 2018. [Online]. Available: https://www.forbes.com.mx/crean-el-primer-hub-de-ciberseguridad-en-america-latina/. [Accessed 23 6 2023].

[20] tekiosmag.com, "Microsoft y el Tec de Monterrey anuncian academia de ciberseguridad para comunicadores," 30 5 2023. [Online]. Available: https://tekiosmag.com/2023/05/30/microsoft-y-el-tec-de-monterrey-anuncian-academia-de-ciberseguridad-para-comunicadores/. [Accessed 23 6 2023].

[21] maestriasydiplomados.tec.mx, "Cybersecurity BootCamp (Programa en Línea)," 2023. [Online]. Available: https://maestriasydiplomados.tec.mx/programas/cybersecurity-bootcamp-programa-en-linea. [Accessed 23 6 2023].

[22] A. González Gozalo, "El ecosistema de startups en Argentina," ICEX, Buenos Aires (Argentina), 2022.

[23] StartupBlink, "The Startup Ecosystem of Buenos Aires," StartupBlink, 2023. [Online]. Available: https://www.startupblink.com/startup-ecosystem/buenos-aires-ar. [Accessed 31 7 2023].

[24] Revista Byte, "La firma de ciberseguridad VU acelera su expansión en España," 12 5 2022. [Online]. Available: https://revistabyte.es/actualidad-it/ciberseguridad-vu-acelera-expansion/. [Accessed 23 6 2023].

[25] ciberseguridad.com, "Empresas de Ciberseguridad en Argentina," 2023. [Online]. Available: https://ciberseguridad.com/empresas/argentina/. [Accessed 23 6 2023].

[26] ASAEDE, "Asociación Argentino Española de Emprendedores," 2023. [Online]. Available: https://www.asaede.org/. [Accessed 31 7 2023].

[27] Acelerar España, "Internacionalizando startups argentinas," 2023. [Online]. Available: https://www.acelerar.es/. [Accessed 31 7 2023].

[28] South Summit, "South Summit," 2023. [Online]. Available: https://www.southsummit.io/. [Accessed 31 7 2023].

[29] ICEX, "Programa Rising Up in Spain," ICEX, 2023. [Online]. Available: https://www.investinspain.org/content/icex-invest/es/rising-up-in-spain.html. [Accessed 31 7 2023].

[30] ICEX, "Programa España-LATAM Scale-Up," ICEX, 2023. [Online]. Available: https://www.investinspain.org/latam-scaleup. [Accessed 31 7 2023].

[31] ICEX, "Programas Invest in Spain," ICEX, 2023. [Online]. Available: https://www.investinspain.org/es/index. [Accessed 31 7 2023].

[32] Startup OLE Accelerator, "Startup Olé Latam ReadShow," 2023. [Online]. Available: http://startupole.eu/latam-roadshow/. [Accessed 31 7 2023].

[33] G. d. España, "Ley 18/2022, de 28 de septiembre, de creación y crecimiento de empresas," 29 9 2022. [Online]. Available: https://www.boe.es/boe/dias/2022/09/29/pdfs/BOE-A-2022-15818.pdf. [Accessed 21 4 2023].

[34] G. d. España, "Centro de Información y Red de Creación de Empresas (CIRCE)," [Online]. Available: https://administracion.gob.es/pag_Home/Tramites/miEmpresaEnTramites/Iniciativas/CIRCE.html. [Accessed 25 4 2023].

[35] Ministerio de Industria, Comercio y Turismo, "Videotutoriales para la cumplimentación del DUE," 2023. [Online]. Available: https://paeelectronico.es/es-es/CanalPAE/VideosTutoriales/paginas/cursos-online.aspx. [Accessed 11 6 2023].

[36] Gobierno de España, "Ministerio de Industria, Comercio y Turismo," 2023. [Online]. Available: https://www.mincotur.gob.es/es-es/Paginas/index.aspx. [Accessed 11 6 2023].

[37] BreakEven Assessors s. l., "¿Por qué la constitución de Sociedades es más rápida y eficiente por via telématica CIRCE?," 2019. [Online]. Available: https://beasl.es/servicios/creacion-empresas/circe/. [Accessed 11 6 2023].

[38] Gobierno de España, "Puntos de Atención al Emprendedor," 2023. [Online]. Available: https://paeelectronico.es/es-es/Paginas/PagInicio.aspx. [Accessed 11 6 2023].

[39] Ministerio de Justicia, "Tener la Doble Nacionalidad," 2023. [Online]. Available: https://www.mjusticia.gob.es/eu/ciudadania/nacionalidad/que-es-nacionalidad/tener-doble-nacionalidad. [Accessed 11 6 2023].

[40] G. d. España, "El Congreso aprueba la Ley "Crea y Crece", una de las principales reformas del Plan de Recuperación," 15 9 2022. [Online]. Available: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/asuntos-economicos/Paginas/2022/150922-aprobacion-congreso-ley-crea_y_crece.aspx. [Accessed 22 4 2023].

[41] INAEM Orienta, "Puntos de Atención al Emprendedor (PAE) ➞servicios gratuitos de información, tramitación y asesoría empresarial individualizada," 2 6 2023. [Online]. Available: https://orientacionprofesionalonline.blogspot.com/2023/06/puntos-de-atencion-al-emprendedor-pae.html. [Accessed 11 6 2023].

[42] INCIBE, "Cybersecurity Ventures," 2023. [Online]. Available: https://www.incibe.es/en/entrepreneurship/ventures. [Accessed 11 6 2023].

[43] Gobierno de España, "Emprende en 3," 2023. [Online]. Available: https://administracion.gob.es/pag_Home/Tramites/miEmpresaEnTramites/Iniciativas/Emprende-en-3.html. [Accessed 11 6 2023].

[44] BOE, "Ley 28/2022 (21/12/2022) de fomento del ecosistema de las empresas emergentes," 23 12 2022. [Online]. Available: https://www.boe.es/buscar/act.php?id=BOE-A-2022-21739. [Accessed 4 3 2023].

[45] Datisa, "Ley crea y crece ¿Qué es? ¿Cuándo se aplica? ¿En qué me afecta?," [Online]. Available: https://datisa.es/ley-crea-y-crece-que-es-cuando-se-aplica-en-que-me-afecta/. [Accessed 24 4 2023].