MITTELSTAND GLOBAL
MARKTERSCHLIESSUNGS-PROGRAMM FÜR KMU

Zivile Sicherheit in Spanien

Handout zur Zielmarktanalyse

Geschäftsanbahnung
10.11.2025-13.11.2025

Durchführer

trAIDe
your partner in global business

Mit der Durchführung dieses Projekts im Rahmen des Bundesförderprogramms Mittelstand Global/ Markterschließungsprogramm beauftragt:

trAIDe

your partner in global business

Das Markterschließungsprogramm für kleine und mittlere Unternehmen ist ein Förderprogramm des:

Bundesministerium für Wirtschaft und Energie

MITTELSTAND GLOBAL
MARKTERSCHLIESSUNGS-PROGRAMM FÜR KMU

IMPRESSUM

Herausgeber
trAIDe GmbH
Hohenstaufenring 42
50674 Köln
www.traide.de

Text und Redaktion
trAIDe GmbH

Stand
September 2025

Gestaltung und Produktion
trAIDe GmbH

Bildnachweis
trAIDe GmbH

Die Studie wurde im Rahmen des Markterschließungsprogramms für das Geschäftsanbahnungsprojekt Spanien aus dem Bereich zivile Sicherheit (Exportinitiative zivile Sicherheitstechnologien und -dienstleistungen) erstellt.
Das Werk, einschließlich aller seiner Teile, ist urheberrechtlich geschützt.
Die Zielmarktanalyse steht der Germany Trade & Invest GmbH sowie geeigneten Dritten zur unentgeltlichen Verwertung zur Verfügung.
Sämtliche Inhalte wurden mit größtmöglicher Sorgfalt und nach bestem Wissen erstellt. Der Herausgeber übernimmt keine Gewähr für die Aktualität, Richtigkeit, Vollständigkeit oder Qualität der bereitgestellten Informationen. Für Schäden materieller oder immaterieller Art, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen unmittelbar oder mittelbar verursacht werden, haftet der Herausgeber nicht, sofern ihm nicht nachweislich vorsätzliches oder grob fahrlässiges Verschulden zur Last gelegt werden kann.

Inhalt

Inhalt **1**

Abbildungsverzeichnis **1**

Tabellenverzeichnis **1**

Abkürzungsverzeichnis **2**

1 Abstract **3**

2 Wirtschaftsdaten kompakt **4**

Weitere Informationen über die zivile Sicherheit in Spanien 10

3 Branchenspezifische Informationen **11**

3.1 Marktpotenziale und -chancen 11
3.1.1 Segmentierung des Marktes 12
3.1.2 Sozioökonomische, politische und gesellschaftlich-kulturelle Rahmenbedingungen 13
3.1.3 Marktentwicklung 15
3.1.4 Der Arbeitsmarkt und das (Aus-)Bildungswesen 16
3.1.5 Sicherheitspolitische Entwicklungen im Zielmarkt 18
3.1.6 Die aktuelle Gesetzeslage und geplante Reformen 18
3.1.7 Regelungen für öffentliche Aufträge und deren Vergabe 19

3.2 Aktuelle Vorhaben, Projekte und Ziele 20

3.3 Wettbewerbssituation / Politische und Rechtliche Rahmenbedingungen 21
3.3.1 Wichtige Akteure des zivilen Sicherheitsmarktes 21
3.3.2 Untersuchung der Wettbewerbssituation 22
3.3.3 Bestehende Bestimmungen und Lizenzierung 24
3.3.4 Hinweise zu Finanzierungsmöglichkeiten, staatliche Anreize und Angebote 25

3.4 SWOT-Analyse 27

4 Kontaktadressen **28**

Quellenverzeichnis **32**

Abbildungsverzeichnis

Abbildung 1 Meist betroffene Sektoren von Cyberangriffen in Spanien 2024 11
Abbildung 2 Wald- und Buschbrände in Europa, Sommer 2025 12
Abbildung 3 Überschwemmungsregionen in Spanien, Oktober 2024 15

Tabellenverzeichnis

Tabelle 1 Weitere Informationen über die zivile Sicherheit in Spanien 10
Tabelle 2 Durchschnittliche Bruttomonatslöhne nach Region [1)] 17
Tabelle 3 Wichtige Akteure des spanischen Marktes für zivile Sicherheit 22
Tabelle 4 SWOT Analyse Spanien 27
Tabelle 5 SWOT Analyse Sicherheitsmarkt Spanien 27
Tabelle 6 Wichtige Entscheidungsträger in der spanischen Wirtschaft 28
Tabelle 7 Relevante Messen im Bereich der zivilen Sicherheit und Cybersicherheit 31

Abkürzungsverzeichnis

AECID – Agencia Española de Cooperación Internacional para el Desarrollo (spanische Agentur für internationale Entwicklungszusammenarbeit)

AHK – Auslandshandelskammer (hier: Deutsche Handelskammer für Spanien)

BOE – Boletín Oficial del Estado (spanisches Gesetzblatt)

BORME – Boletín Oficial del Registro Mercantil (spanisches Handelsregisterblatt)

CAGR – Compound Annual Growth Rate (jährliche Wachstumsrate)

CER – Critical Entities Resilience (Gesetz zum Schutz und zur Resilienz kritischer Einrichtungen)

CNPIC – Centro Nacional para la Protección de las Infraestructuras Críticas (Nationales Zentrum zum Schutz Kritischer Infrastrukturen)

CNPREC – Centro Nacional para la Protección y Resiliencia de las Entidades Críticas (erweiterte Koordinationsstelle für Resilienz)

COVID-19 – Coronavirus Disease 2019

DANA – Depresión Aislada en Niveles Altos (isolierte Höhentiefs; Wetterphänomen)

E-Commerce – Electronic Commerce (elektronischer Handel)

ENISA – European Union Agency for Cybersecurity

EUGO – EU-Portal für Verwaltungsverfahren („Ventanilla Única“)

EUR – Euro

EUSF – European Union Solidarity Fund (EU-Solidaritätsfonds)

FCAS – Fondo de Cooperación para Água y Saneamiento (Wasserfonds)

FONPRODE – Fondo para la Promoción del Desarrollo (Förderfonds für Entwicklung)

GICC – German Intelligence Community Conference

GTAI – Germany Trade & Invest (Außenwirtschaftsagentur der Bundesrepublik Deutschland)

ICEX – Instituto Español de Comercio Exterior (Spanische Außenhandelsagentur)

ISC – International Information System Security Certification Consortium (im Kontext: Cybersecurity Workforce Report)

ISD – Internet Security Days

ISMS – Informationssicherheits-Managementsystem

IT – Informationstechnologie

KI – Künstliche Intelligenz

KMU – Kleine und mittlere Unternehmen

MUE – Militärische Notfalleinheit (Unidad Militar de Emergencias – UME)

NATO – North Atlantic Treaty Organization (Nordatlantikpakt-Organisation)

NIS2 – EU-Richtlinie zur Netz- und Informationssicherheit (zweite Version)

NTT – Nippon Telegraph and Telephone Corporation (japanischer IT-Konzern)

OT – Operational Technology (Betriebstechnologie)

SASE – Secure Access Service Edge (Netzwerkarchitekturmodell)

SEPI – Sociedad Estatal de Participaciones Industriales (Staatliche Industriebeteiligungsgesellschaft Spaniens)

USD – United States Dollar (US-Dollar)

UME – Unidad Militar de Emergencias (Militärische Notfalleinheit)

ZEC – Zona Especial Canaria (Sonderwirtschaftszone der Kanaren)

1 Abstract

Spanien zählt mit rund 48 Millionen Einwohnern zu den größten Volkswirtschaften Europas und bietet deutschen Unternehmen im Bereich zivile Sicherheit und Katastrophenschutz ein dynamisches Marktumfeld. Die geografischen und klimatischen Gegebenheiten des Landes führen regelmäßig zu Naturereignissen wie Überschwemmungen, Dürren, Waldbränden oder Erdbeben, die erhebliche wirtschaftliche und gesellschaftliche Schäden verursachen können. In Verbindung mit einer stark urbanisierten Bevölkerung und der hohen Konzentration von Industrie- und Dienstleistungszentren entsteht ein erheblicher Bedarf an Prävention, Notfallmanagement und resilienten Infrastrukturen. Kommunen, Zivilschutzbehörden und öffentliche Institutionen sind dabei zentrale Auftraggeber, was deutschen Anbietern von Frühwarnsystemen, mobilen Kommunikationslösungen, Notstromtechnik und innovativen Schutzkonzepten attraktive Einstiegsmöglichkeiten eröffnet.

Darüber hinaus verfolgt Spanien eine ambitionierte Modernisierungsagenda, die durch staatliche Programme und europäische Mittel umfangreich finanziert wird. Förderinstrumente wie die Agenda España Digital 2025, der nationale Aufbau- und Resilienzplan sowie die EU-Initiativen Next Generation EU und EU-Solidaritätsfonds (EUSF) unterstützen nicht nur Infrastruktur- und Nachhaltigkeitsprojekte, sondern setzen zunehmend auch sicherheitsrelevante Schwerpunkte. Für deutsche Unternehmen ergibt sich daraus ein Marktumfeld, in dem politische Priorisierung, öffentlicher Finanzierungsrahmen und gesellschaftliches Sicherheitsbewusstsein zusammenwirken. Neben großen Infrastrukturprojekten entstehen dadurch auch zahlreiche Ausschreibungen auf regionaler und kommunaler Ebene, die gezielt kleine und mittelständische Anbieter adressieren.

Ein weiterer wichtiger Aspekt ist die institutionelle Landschaft Spaniens, die Forschung und Innovation zunehmend in den Mittelpunkt stellt. Das nationale Cybersecurity-Institut INCIBE und das Forschungsnetzwerk RENIC bündeln wissenschaftliche Exzellenz im Bereich IT-Sicherheit, während im Katastrophenschutz durch nationale Strategien wie den Plan „Horizon 2035“ Forschung, Innovation und evidenzbasierte Prävention fest in die Strukturen integriert werden. Ergänzt wird dies durch europäische Programme wie Horizon Europe, die Projekte in den Bereichen Resilienz, Krisenmanagement und digitale Sicherheit fördern. Für deutsche Anbieter eröffnen sich hier Kooperationsfelder, sowohl auf wissenschaftlicher Ebene als auch in praxisnahen Pilotprojekten.

Im Bereich Cybersecurity ist Spanien in den vergangenen Jahren zu einem europäischen Brennpunkt geworden: Das Land zählt laut internationalen Studien zu den am stärksten von Cyberangriffen betroffenen Staaten weltweit. Unternehmen, öffentliche Verwaltung und kritische Infrastrukturen sehen sich einer wachsenden Bedrohungslage ausgesetzt, was Investitionen in Sicherheitstechnologien und integrierte Plattformlösungen beschleunigt. Staatliche Programme wie das Kit Digital oder die Investitionen im Rahmen der Komponente 15 des Resilienzplans schaffen dabei nicht nur Marktvolumen, sondern fördern auch die Verbreitung standardisierter Sicherheitslösungen, von denen insbesondere deutsche Anbieter profitieren können. Parallel dazu gewinnen Themen wie Künstliche Intelligenz in der Gefahrenprävention, satellitengestützte Kommunikation und resiliente IT-Architekturen an Bedeutung, wodurch sich zusätzliche Kooperationsfelder mit spanischen Unternehmen und Behörden ergeben.

Besonders stark gefragt sind derzeit Technologien zur Absicherung kritischer Infrastrukturen, darunter Energieversorgung, Gesundheitswesen, Transportnetze und Wasserversorgung. Durch die Umsetzung der europäischen Richtlinien NIS2 und CER verschärfen sich die Anforderungen an Betreiber erheblich, was Investitionen in Zugangskontrollsysteme, Videoüberwachung, Drohnenerkennung und redundante Kommunikationsnetze notwendig macht. Deutsche Unternehmen können hier mit ihrer Erfahrung in der Entwicklung von Hochsicherheitslösungen punkten und durch Partnerschaften mit spanischen Akteuren wie Indra oder Telefónica Tech direkten Marktzugang gewinnen.

Insgesamt bietet Spanien deutschen Unternehmen ein vielschichtiges Marktumfeld, in dem ziviler Bevölkerungsschutz, Katastrophenprävention und Cybersecurity gleichermaßen nachgefragt werden. Die Kombination aus hoher Bedrohungslage, umfangreichen staatlichen und europäischen Förderinstrumenten sowie einer technologieorientierten Modernisierungsstrategie macht den spanischen Markt zu einem der spannendsten Zielmärkte für die deutsche Sicherheitswirtschaft.

2 Wirtschaftsdaten kompakt

Bevölkerung & Ressourcen

Bevölkerung und Demografie

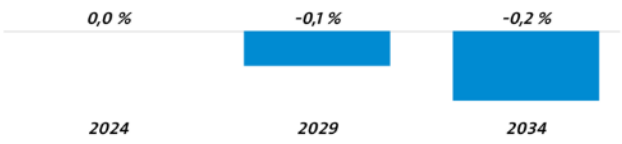
Einwohnerzahl

2024	*47,9 Mio.*
2029	*47,7 Mio.*
2034	*47,3 Mio.*

Fertilitätsrate 2023 | 1,1

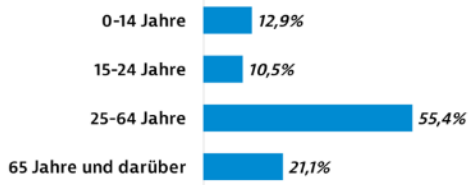
Durchschnittliche Anzahl der Geburten pro Frau

Bevölkerungswachstum



Altersstruktur

2024



Analphabetenquote 2020 | 1,0 %

Anteil an der Bevölkerung ab 15 Jahren in %

Fläche und Sprache

Fläche 2022 | 505.978 km²

Geschäftssprache(n) Spanisch, Englisch

Rohstoffe und Ressourcen

Rohstoffe

Fossil und mineralisch

Kohle | Braunkohle | Eisenerz | Kupfer | Blei | Zink | Uran | Wolfram | Quecksilber | Pyrit | Magnesit | Flussspat | Gips | Sepiolith | Kaolin | Pottasche

Gas - Fördermenge

Daten für diese Kennzahl nicht verfügbar oder nicht anwendbar.

Erdöl - Fördermenge

Daten für diese Kennzahl nicht verfügbar oder nicht anwendbar.

Gas - Reserven

Daten für diese Kennzahl nicht verfügbar oder nicht anwendbar.

Erdöl - Reserven

Daten für diese Kennzahl nicht verfügbar oder nicht anwendbar.

Wirtschaftslage

Währung und Wechselkurse

Währung - Bezeichnung Euro
1 Euro = 100 Cent

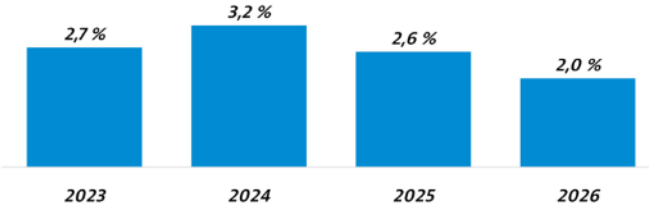
Währung - Kurs 1 € = 1,13 US$
04/2025

Wechselkurse im Jahresdurchschnitt

	2022	2023	2024
1 € =	1,05 US$	1,08 US$	1,08 US$

Wirtschaftliche Leistung

Wirtschaftswachstum
Bruttoinlandsprodukt (BIP), Veränderung zum Vorjahr, real



BIP
Nominal

	2024	2025	2026
US$ (Mrd.)	1.722,2	1.799,5	1.886,2
Euro (Mrd.)	1.591,6	1.671,0	1.742,0

BIP/Kopf
Nominal

	2024	2025	2026
US$	35.092	36.192	37.489
Euro	32.431	33.608	34.622

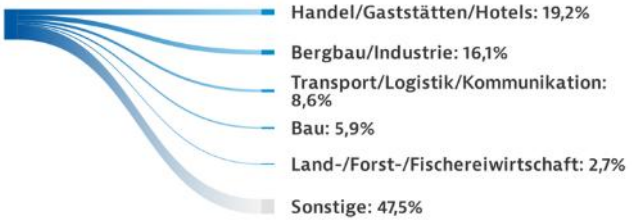
BIP/Kopf in Kaufkraftstandards
Nominal

2022	31.600 KKS
2023	34.500 KKS
2024	36.300 KKS

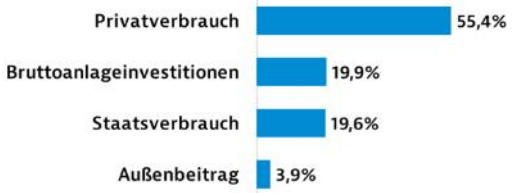
Ausgaben für F&E
% des BIP

2020	1,4 %
2021	1,4 %
2022	1,4 %

BIP-Entstehung
Anteil an nominaler Bruttowertschöpfung in %; 2023

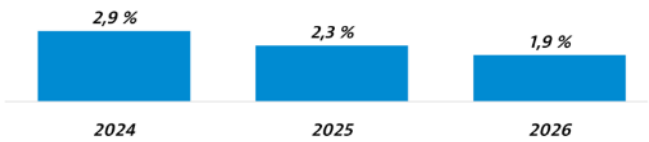


BIP-Verwendung
Anteil an Bruttoinlandsprodukt in %; 2023

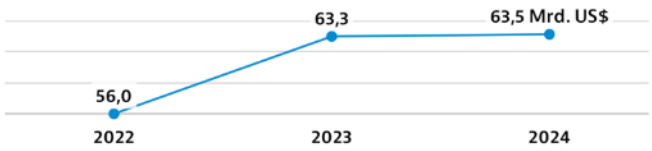


Makroökonomische Stabilität

Inflationsrate



Währungsreserven



Leistungsbilanzsaldo
% des BIP

2024	3,1 %
2025	2,7 %
2026	2,8 %

Arbeitslosenquote

2024	11,4 %
2025	10,4 %
2026	9,9 %

Investitionsquote
% des BIP, brutto, öffentlich und privat

2024	20,5 %
2025	*21,1 %*
2026	*21,3 %*

Öffentliche Finanzen & Verschuldung

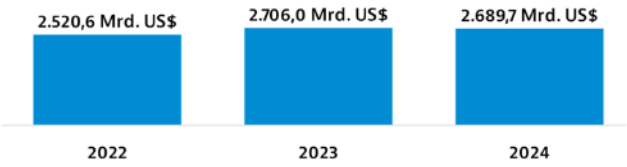
Haushaltssaldo
% des BIP

2024	*-3,2 %*
2025	*-2,8 %*
2026	*-2,5 %*

Staatsverschuldungsquote
% des BIP, brutto

2024	*101,8 %*
2025	*100,9 %*
2026	*100,8 %*

Auslandsverschuldung



Ausländische Direktinvestitionen

FDI - Nettotransaktionen

2021	38.318 Mio. US$
2022	44.885 Mio. US$
2023	35.914 Mio. US$

FDI - Bestand

2021	799.149 Mio. US$
2022	812.740 Mio. US$
2023	897.268 Mio. US$

FDI - Hauptländer
Anteil in %, Bestand; 2023

Luxemburg: 15,8% | Niederlande: 13,8% | Vereinigtes Königreich: 12,5% | Frankreich: 11,0% | Deutschland: 10,0% | Italien: 5,0% | USA: 4,7%

FDI - Hauptbranchen
Anteil in %, Zufluss; 2023

verarbeitendes Gewerbe: 16,9% | Handel: 14,1% | Bergbau und Gewinnung von Erdöl und Erdgas: 12,4% | Informations- und Kommunikationstechnologien: 11,6% | Energie: 7,4% | Immobilien: 6,7%

Außenwirtschaft

Warenhandel

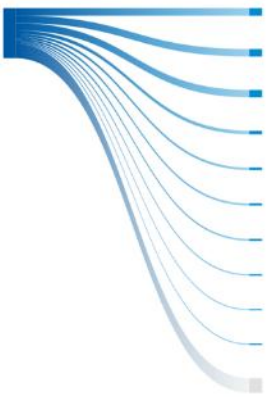
Warenhandel
Veränderung zum Vorjahr in %, Abweichungen durch Rundungen

	2022	%	2023	%	2024	%
Exporte (Mrd. US$)	424,3	8,4	420,2	-1,0	403,7	-3,9
Importe (Mrd. US$)	499,1	17,1	469,0	-6,0	451,3	-3,8
Saldo (Mrd. US$)	-74,8		-48,9		-47,6	

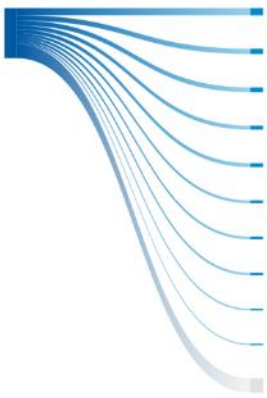
Exportquote
Exporte/BIP in %

2022	29,3 %
2023	25,9 %
2024	23,4 %

Ausfuhrgüter nach SITC
Anteil an den Warenexporten; 2024

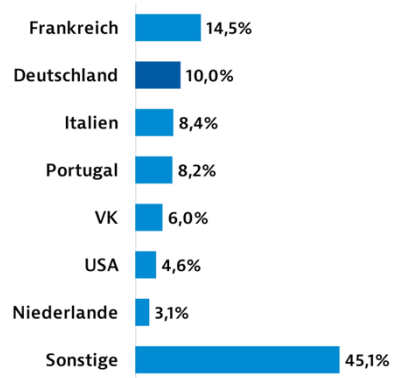


Einfuhrgüter nach SITC
Anteil an den Warenimporten; 2024

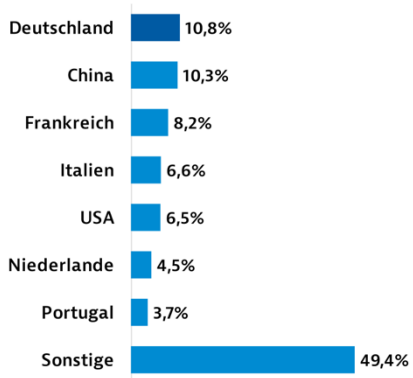


Handelspartner

Hauptabnehmerländer
Anteil an den Warenexporten; 2024



Hauptlieferländer
Anteil an den Warenimporten; 2024



Dienstleistungshandel

Dienstleistungshandel (mit dem Ausland)
Veränderung zum Vorjahr in %, Abweichungen durch Rundungen

	2022	%	2023	%	2024	%
DL-Exporte (Mrd. US$)	164,0	40,4	197,1	20,2	220,4	11,8
DL-Importe (Mrd. US$)	88,6	14,3	95,9	8,1	111,6	16,4
Saldo (Mrd. US$)	75,4		101,2		108,8	

Freihandelsabkommen

Freihandelsabkommen mit Ländergruppen (ohne EU)

Das Land profitiert im Rahmen seiner EU-Mitgliedschaft von den Freihandelsabkommen der EU. Derzeit bestehen Abkommen mit 78 Staaten; weitere Freihandelsabkommen werden zurzeit verhandelt.

Zu bilateralen Abkommen siehe www.wto.org -> Trade Topics, Regional Trade Agreements, RTA Database, By country/territory

Mitgliedschaft in Zollunion

EU, seit 01.01.1986 (EG)

Warenhandel mit Deutschland

Warenhandel Deutschlands mit dem Land
Veränderung zum Vorjahr in %, Abweichungen durch Rundungen

	2022	%	2023	%	*2024*	*%*
Dt. Exporte (Mrd. Euro)	50,0	13,8	54,0	8,1	*53,6*	*-0,7*
Dt. Importe (Mrd. Euro)	37,6	10,1	38,6	2,7	*38,0*	*-1,6*
Saldo (Mrd. Euro)	12,3		15,4		*15,6*	

Rangstelle bei deutschen Exporten
2024; 1 = beste Bewertung

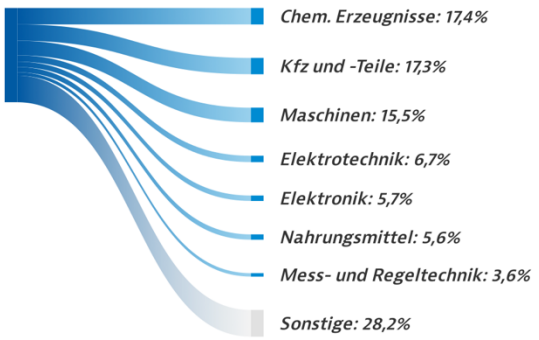
Rang 11 *von 238*

Rangstelle bei deutschen Importen
2024; 1 = beste Bewertung

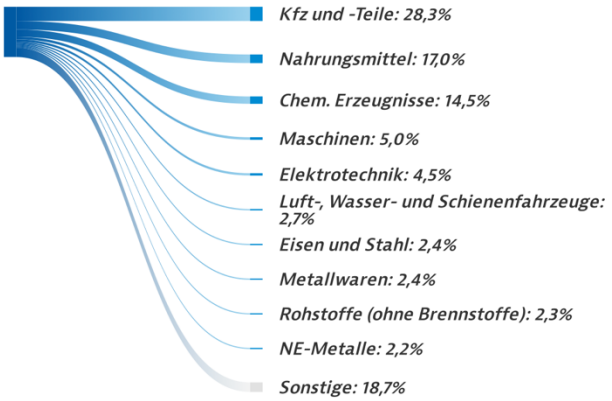
Rang 11 *von 238*

Deutsche Aus- und Einfuhrgüter

Deutsche Exportgüter nach SITC
Anteil an den Gesamtexporten; 2024



Deutsche Importgüter nach SITC
Anteil an den Gesamtimporten; 2024



Bilateraler Dienstleistungshandel

Dienstleistungshandel Deutschlands mit dem Land
Veränderung zum Vorjahr in %, Abweichungen durch Rundungen

	2022	%	2023	%	2024	%
DL-Exporte (Mrd. Euro)	10,9	40,1	11,3	3,3	12,7	12,3
DL-Importe (Mrd. Euro)	17,2	54,0	20,0	16,4	20,7	3,3
Saldo (Mrd. Euro)	-6,3		-8,8		-8,0	

Bilaterale Direktinvestitionen

Deutsche Direktinvestitionen (Bestand)
2021 | 44.864 Mio. Euro
2022 | 45.792 Mio. Euro
2023 | 46.311 Mio. Euro

Direktinvestitionen des Landes in Deutschland (Bestand)
2021 | 12.115 Mio. Euro
2022 | 15.060 Mio. Euro
2023 | 12.153 Mio. Euro

Deutsche Direktinvestitionen (Nettotransaktionen)
2022 | +8.918 Mio. Euro
2023 | +4.857 Mio. Euro
2024 | +1.506 Mio. Euro

Direktinvestitionen des Landes in Deutschland (Nettotransaktionen)
2022 | +2.630 Mio. Euro
2023 | +31 Mio. Euro
2024 | +102 Mio. Euro

Bilaterale Kooperation

Doppelbesteuerungs-abkommen
Abkommen vom 03.02.2011; in Kraft seit 01.01.2013

Investitionsschutz-abkommen
Kein Abkommen

Bilaterale öffentliche Entwicklungszusammenarbeit
Daten für diese Kennzahl nicht verfügbar oder nicht anwendbar.

Anlaufstellen

Deutsche Auslandsvertretung
Madrid, https://spanien.diplo.de

Auslandsvertretung des Landes in Deutschland
Berlin, https://www.exteriores.gob.es/Embajadas/berlin/de/Paginas/index.aspx

Auslandshandelskammer
Madrid, www.ahk.es

Nachhaltigkeit & Klimaschutz

Emissionen

Treibhausgasemissionen pro Kopf In Tonnen CO2-Äquivalent	2012	7,2 tCO_2e
	2022	5,8 tCO_2e
Treibhausgasemissionen Anteil weltweit in %	2012	0,7 %
	2022	0,5 %
Emissionsintensität pro Mio. US$ BIP In Tonnen CO2-Äquivalent	2012	290,0 tCO_2e
	2022	204,6 tCO_2e
Emissionsstärkste Sektoren Anteil in %; 2022	Transport: 32,9% | Elektrizität/Wärme: 23,2% | Landwirtschaft: 13,7%	

Energie und Nachhaltigkeit

Erneuerbare Energien Anteil am Primärenergieangebot in %	2011	11,8 %
	2021	16,7 %
Stromverbrauch In Kilowattstunden pro Kopf	2022	5.151 kWh pro Kopf
Sustainable Development Goals Index 2023; 1 = beste Bewertung	Rang 14 von 167	

Geschäftsumfeld

Einschätzung des Geschäftsumfelds

Länderkategorie für Exportkreditgarantien 0 = niedrigste Risikokategorie, 7 = höchste	Keine Risikoeinstufung
Corruption Perceptions Index 2024; 1 = beste Bewertung	Rang 46 von 180
Logistics-Performance-Index 2023; 1 = beste Bewertung	Rang 13 von 139
Internetqualität 2024; 1 = beste Bewertung	Rang 8 von 121

Weiterführende Informationen

Weitere Informationen zu Wirtschaftslage, Branchen, Geschäftspraxis, Recht, Zoll, Ausschreibungen und Entwicklungsprojekten können Sie unter www.gtai.de/spanien abrufen.

Quellen: Germany Trade & Invest bemüht sich, in allen Datenblättern einheitliche Quellen zu nutzen, sodass die Daten für unterschiedliche Länder möglichst vergleichbar sind. Wenn die Standardquellen nicht verfügbar sind, greifen wir auf andere Quellen zurück oder weisen keine Daten aus. Dies ist bei einem Vergleich dieser Daten mit den Angaben in Datenblättern zu anderen Ländern zu berücksichtigen.

Umstrittene Gebiete werden als eigene Entitäten und zu keinem der beanspruchenden Staaten gehörend dargestellt. Die Bundesregierung unterstützt die territoriale Unversehrtheit der Ukraine in den Grenzen, die seit 1991 international anerkannt sind.

Die Bezeichnung „Länder" in den Wirtschaftsdaten kompakt umfasst Staaten, Provinzen und Territorien. Sie spiegelt nicht die Position der Bundesregierung hinsichtlich des Status eines Landes oder einer Region wider.

Germany Trade & Invest ist die Wirtschaftsförderungsgesellschaft der Bundesrepublik Deutschland. Die Gesellschaft sichert und schafft Arbeitsplätze und stärkt damit den Wirtschaftsstandort Deutschland. Mit über 50 Standorten weltweit und dem Partnernetzwerk unterstützt Germany Trade & Invest deutsche Unternehmen bei ihrem Weg ins Ausland, wirbt für den Standort Deutschland und begleitet ausländische Unternehmen bei der Ansiedlung in Deutschland.

Ansprechperson bei Germany Trade & Invest:

Edda vom Dorp
T +49 228 24 993 303
edda.vom-dorp@gtai.de

Germany Trade & Invest, Standort Bonn
Villemombler Straße 76, 53123 Bonn, Deutschland
T +49 228 24 993 0
trade@gtai.de
www.gtai.de

Germany Trade & Invest, Hauptsitz
Friedrichstraße 60, 10117 Berlin, Deutschland
T +49 30 200 099 0
invest@gtai.de
www.gtai.de

Weitere Informationen über die zivile Sicherheit in Spanien

GTAI-Informationen zu Spanien	Link
Prognosen zu Investitionen, Konsum und Außenhandel	Wirtschaftsausblick von GTAI
Potenziale kennen, Risiken richtig einschätzen	SWOT-Analyse
Kulturelle Hintergründe und Regeln für den Geschäftskontakt	Verhandlungspraxis kompakt
Kurzanalyse zur Verteidigungswirtschaft	Branche kompakt
Länderspezifische Basisinformationen zu relevanten Rechtsthemen in Spanien	Recht kompakt

Tabelle 1 Weitere Informationen über die zivile Sicherheit in Spanien

3 Branchenspezifische Informationen

3.1 Marktpotenziale und -chancen

Spanien zählt mit rund 48 Millionen Einwohnern zu den größten Volkswirtschaften Europas und bietet deutschen Unternehmen ein attraktives Marktumfeld mit stabiler industrieller Basis und hoher internationaler Vernetzung. Die enge wirtschaftliche Verflechtung mit Deutschland – über 1.000 deutsche Unternehmen sind in Spanien aktiv – eröffnet zusätzliche Zugänge zu Partnerschaften und etablierten Vertriebsnetzen. Ein zentraler Standortvorteil Spaniens liegt in der exzellent ausgebauten Verkehrs- und Telekommunikationsinfrastruktur, die von deutschen Unternehmen vor Ort regelmäßig positiv bewertet wird. Gleichzeitig wird auf regionaler Ebene eine starke wirtschaftliche Konzentration beobachtet, insbesondere in Madrid, Katalonien und im Baskenland, wo bedeutende Technologie-, Chemie- und Maschinenbaucluster angesiedelt sind. Diese Konzentration begünstigt Investitionen in sicherheitsrelevante Technologien wie etwa Frühwarnsysteme oder intelligente Infrastrukturkomponenten.[1]

Das Thema Cybersecurity gewinnt in Spanien aufgrund zunehmender digitaler Vernetzung und wachsender Bedrohungslagen stark an Bedeutung. Besonders sensible Sektoren wie Tourismus und Banken sind häufig Ziel von Angriffen, was Investitionen in Echtzeit-Erkennungssysteme und biometrische Sicherheitslösungen notwendig macht. Auch der Mittelstand und Kleinstunternehmen geraten vermehrt unter Druck, ihre digitale Sicherheit zu verbessern – unterstützt durch staatliche Programme wie das „Kit Digital“ mit einem Fördervolumen von 3 Milliarden Euro. Gleichzeitig ist der Bedarf an Fachkräften im Bereich Cybersicherheit besonders hoch – ein Umstand, der sich in deutlich überdurchschnittlichen Gehältern widerspiegelt. Dies verdeutlicht die Dringlichkeit technologischer Lösungen zur Effizienzsteigerung im Bereich IT-Security – ein Feld, in dem deutsche Anbieter gezielt ansetzen können.[2]

Laut einer Studie von Deloitte besteht unter spanischen IT-Verantwortlichen Konsens darüber, dass das Einbinden des Managements die Wirksamkeit von Cybersecurity-Maßnahmen erheblich verbessert. Damit eröffnet sich für Anbieter strategischer Sicherheitslösungen eine zusätzliche Ebene der Markterschließung im Top-Management großer Unternehmen. Die Studie benennt zudem einen Paradigmenwechsel: Weg von punktuellen Maßnahmen, hin zu einem ganzheitlichen Sicherheitsverständnis, das bereits im Designprozess digitaler Systeme verankert ist.[3] Diese Entwicklung schafft Raum für integrierte Sicherheitsplattformen und intelligente Sicherheitsarchitekturen – ein Potenzial insbesondere für deutsche Anbieter mit entsprechender Systemkompetenz.

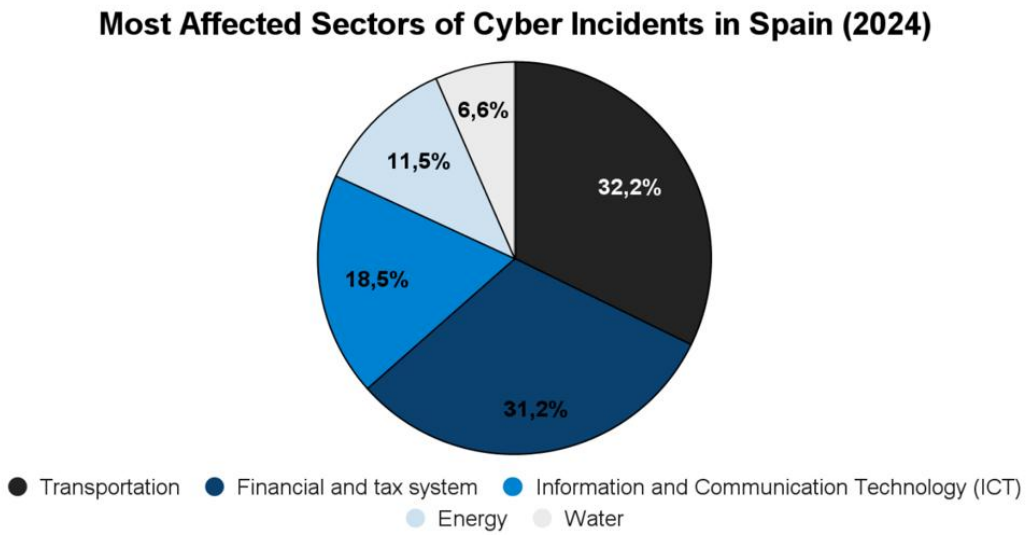


Abbildung 1 Meist betroffene Sektoren von Cyberangriffen in Spanien 2024[4]

[1] https://www.gtai.de/de/trade/spanien-wirtschaft/wirtschaftsstandort
[2] https://www.gtai.de/de/trade/spanien/wirtschaftsumfeld/unternehmen-lassen-sich-cybersicherheit-mehr-kosten-930418
[3] https://www.deloitte.com/es/es/services/risk-advisory/perspectives/estado-ciberseguridad-2024.html
[4] Abbildung aus Experteninterview LP

3.1.1 Segmentierung des Marktes

Naturgefahren wie Überschwemmungen, Dürren, Waldbrände und Erdbeben stellen in Spanien weit verbreitete und regionsspezifische Risiken dar. Insbesondere die intensive Bebauung von Küstenregionen sowie der voranschreitende Klimawandel mit zunehmenden Extremwetterereignissen erhöhen die Gefährdungslage und damit den Bedarf an entsprechenden Schutzmaßnahmen. Daraus ergeben sich spezifische Marktsegmente für Anbieter von Frühwarnsystemen, resilienter Infrastruktur, Notstromlösungen, mobilen Kommunikationssystemen und Geo-Informationsdiensten. [5] Ein aktuelles Beispiel sind die großflächigen Waldbrände im Sommer 2025 in Andalusien und Katalonien. Über den EU-Katastrophenschutzmechanismus wurden dabei auch deutsche Einsatzkräfte eingebunden, um die spanische Unidad Militar de Emergencias (UME) und lokale Feuerwehren zu unterstützen. Der Einsatz verdeutlichte nicht nur die wachsende Relevanz internationaler Zusammenarbeit im Bevölkerungsschutz, sondern auch den hohen Bedarf an moderner Ausrüstung, länderübergreifend kompatibler Kommunikationstechnik und effizienter Einsatzlogistik.[6] [7] Kommunale Verwaltungen und Zivilschutzbehörden sind dabei zentrale Zielgruppen, da sie für Evakuierungsmaßnahmen, Risikoprävention und Bevölkerungsschutz zuständig sind. Neben technischen Lösungen gewinnen auch naturbasierte Schutzmaßnahmen wie angepasste Landnutzung, Entsiegelung oder Vegetationsbarrieren an Bedeutung, wodurch sich neue Marktsegmente im Bereich nachhaltiger Sicherheitsplanung eröffnen. Auch die Konzeption und Integration von Notfallplänen und Schulungskonzepten für Bevölkerung und Einsatzkräfte stellt ein wichtiges Marktpotenzial dar.[8] Strukturierte Reaktionsprotokolle und Ausstattung für den möglichen Krisenfall – etwa Notfallkits, Evakuierungspläne oder mobile Rettungseinheiten – sind zunehmend gefragt, insbesondere in Risikoregionen. Dies schafft zusätzliche Bedarfe für Unternehmen, die logistische, organisatorische oder technische Notfalllösungen anbieten.[9]

Abbildung 2 Wald- und Buschbrände in Europa, Sommer 2025[10]

[5] https://www.xatakamovil.com/conectividad/malla-b-sirdee-sistemas-comunicacion-segura-estado-trabajan-para-reducir-riesgo-quedar-incomunicados
[6] https://international.bonn.de/press-releases/august/forest-fires-in-spain.php#:~:text=When%20the%20German%20forest%20firefighting,new%20operational%20area%20remained%20tense.
[7] https://www.bbc.com/news/articles/cd6n8qqlj8go
[8] https://www.xatakamovil.com/conectividad/malla-b-sirdee-sistemas-comunicacion-segura-estado-trabajan-para-reducir-riesgo-quedar-incomunicados
[9] https://invescon.es/proteccion-de-infraestructuras-criticas-en-espana/
[10] https://www.welt.de/vermischtes/gallery4182874/Braende-Suedeuropa.html

Ein zentrales Marktsegment im Bereich der zivilen Sicherheit stellt der Schutz kritischer Infrastrukturen dar, darunter Energieversorgung, Gesundheitssysteme, Transport, Kommunikation und Wasserversorgung. Diese sind gesetzlich verpflichtet, spezifische Schutzmaßnahmen umzusetzen, wie sie im Nationalen Schutzplan (NPP) und im Katalog kritischer Infrastrukturen definiert sind. Für Anbieter ergeben sich Marktchancen etwa im Bereich Zugangskontrolle, Videoüberwachung, Drohnenerkennung, Zutrittsmanagement oder Redundanzsysteme. Die Marktstruktur ist komplex: Verantwortlichkeiten liegen verteilt zwischen Ministerien, Behörden auf nationaler und regionaler Ebene sowie privaten Betreibern. Die dezentrale Verwaltungsstruktur Spaniens bedingt zudem regionale Unterschiede bei Zuständigkeiten, Investitionen und Ausschreibungen – ein wesentlicher Aspekt für Markterschließungsstrategien. Besonders sicherheitsrelevant sind Ballungsräume, Transportknotenpunkte sowie Regionen mit hoher touristischer Dichte.[11]

Der spanische Markt für zivile Sicherheits- und Cybersicherheitslösungen ist durch eine wachsende Vielfalt an Anwendungsfeldern geprägt, die sich aus der zunehmenden Digitalisierung aller Wirtschaftsbereiche ergeben. Die steigende Nutzung digitaler Plattformen und die Ausweitung des E-Commerce-Sektors führen zu einem erhöhten Bedarf an Cybersicherheitsmaßnahmen, insbesondere im Bereich Datenschutz, Zugriffskontrollen und Netzwerk Resilienz. Damit ergibt sich ein relevantes Marktsegment für Anbieter, die skalierbare Sicherheitslösungen für unterschiedlich digitalisierte Unternehmen bereitstellen. Kleine und mittlere Unternehmen (KMU) sind besonders vulnerabel, da ihnen oft interne Ressourcen für IT-Sicherheit fehlen. Der spanische Staat fördert diesen Bereich über Programme wie das „Digital Kit“ sowie die „Agenda España Digital 2025“, wodurch gezielt Nachfrage nach externer Cybersicherheitskompetenz entsteht. Deutsche Anbieter mit standardisierten, skalierbaren Produkten finden hier einen klar definierten Markt mit hoher Eintrittsrelevanz[12].

Die Bedrohungslage zeigt sich auch in einer Zunahme von Angriffen wie Phishing, Ransomware oder gezielter Datenverschlüsselung, die zu erheblichen wirtschaftlichen Schäden führen können. Dies betrifft nicht nur private Unternehmen, sondern zunehmend auch öffentliche Einrichtungen und Verwaltungen, was das Spektrum potenzieller Kunden erweitert.[13]

3.1.2 Sozioökonomische, politische und gesellschaftlich-kulturelle Rahmenbedingungen

Die wirtschaftliche Stärke Spaniens und seine enge internationale Vernetzung schaffen ein attraktives Investitionsumfeld. Deutsche Unternehmen sind in zentralen Branchen wie Automobil und Handel seit Jahrzehnten fester Bestandteil des Marktes. Die wirtschaftliche Entwicklung wird zunehmend durch staatliche Investitionsförderprogramme gelenkt, die insbesondere in strukturschwachen Regionen attraktive Förderkonditionen bieten. Je nach Unternehmensgröße und Standort können Förderquoten von bis zu 70 Prozent erreicht werden, wodurch auch kleinere deutsche Firmen gezielt angesprochen werden. Zusätzlich unterstützen EU-Förderprogramme wie Next Generation EU die Transformation hin zu mehr Nachhaltigkeit und Digitalisierung. Regionale und kommunale Förderstellen agieren dabei eigenständig und bieten spezifische Anreize, z. B. Steuererleichterungen in Barcelona für Start-ups und technologieintensive Unternehmen.[14]

Die politische Struktur Spaniens ist stark dezentralisiert, was Auswirkungen auf Verwaltungsprozesse, Entscheidungswege und die Umsetzung von Investitionsvorhaben hat. Die 17 Autonomen Gemeinschaften und viele Gemeinden verfügen über eigene Zuständigkeiten, insbesondere in Bildungs-, Wirtschafts- und Infrastrukturfragen, was zu teils komplexen und langwierigen Genehmigungsprozessen führen kann. Das föderale System kann eine Koordination zwischen Zentralstaat, Regionen und Kommunen erschweren – etwa beim Ausbau strategischer Infrastrukturen wie Elektromobilität oder digitaler Netze. Gleichwohl eröffnet es unternehmerische Handlungsspielräume: Regionale Parlamente verfügen über Budgetautonomie und setzen eigene wirtschaftspolitische Impulse, was gerade bei Pilotprojekten, kommunalen Sicherheitslösungen oder technologischen Initiativen gezielte Ansätze ermöglicht.[15]

Die aktuelle politische Lage ist geprägt von einer fragilen Mehrheitsregierung, die sich auf eine Vielzahl kleinerer Parteien sowie regionaler Akteure stützt, unter anderem aus Katalonien und dem Baskenland. Diese Konstellation erhöht die Verhandlungsmacht regionaler Vertreter, die für politische Zugeständnisse oftmals regionale Autonomierechte oder

[11] https://www.gndr.org/2024-spain-floods-early-warning-action-coordination-and-localisation/
[12] https://www.mordorintelligence.com/de/industry-reports/spain-cybersecurity-market
[13] https://www.grupocibernos.com/blog/ciberseguridad-en-españa
[14] https://www.gtai.de/de/trade/spanien-wirtschaft/wirtschaftsstandort
[15] https://www.gtai.de/de/trade/spanien-wirtschaft/wirtschaftsstandort

wirtschaftliche Sonderregelungen einfordern. Insbesondere in Katalonien ist das Spannungsverhältnis zwischen zentralstaatlichen Vorgaben und regionalen Interessen weiterhin spürbar – etwa im Bereich Sprache, Bildung und Verwaltung. Für internationale Unternehmen bedeutet dies, sich auf politische Mehrdimensionalität einzustellen und lokale Gegebenheiten differenziert zu analysieren. Gesellschaftlich ist Spanien stark von sprachlich-kultureller Vielfalt geprägt, insbesondere durch das Spannungsverhältnis zwischen der Landessprache Spanisch und den regionalen Amtssprachen wie Katalanisch oder Baskisch. Dies wirkt sich nicht nur auf das Bildungssystem, sondern auch auf geschäftliche Kommunikation und Personalrekrutierung aus. In wirtschaftsnahen Kontexten dominiert jedoch Spanisch, während Fremdsprachenkenntnisse – insbesondere in Englisch – regional und altersbezogen stark variieren. Internationale Geschäftsbeziehungen profitieren tendenziell von jüngeren, urban geprägten Arbeitskräften mit höherem Sprachniveau, während in ländlichen oder traditionellen Bereichen Sprachbarrieren bestehen können.[16]

Die bilateralen Beziehungen zwischen Spanien und Deutschland sind eng und freundschaftlich. Eine breite Übereinstimmung in außenpolitischen Grundwerten und Überzeugungen macht die beiden Ländern zu wichtigen bi- und multilateralen Partnern. Der politische Austausch ist eng und vertrauensvoll. Die Umsetzung des Deutsch-Spanischen Aktionsplans von 2022 steht im Fokus des bilateralen Verhältnisses und der EU-Zusammenarbeit.[17]

Die wirtschaftliche Situation Spaniens ist von einer paradoxen Konstellation geprägt: Trotz europaweit hoher Arbeitslosigkeit herrscht ein signifikanter Fachkräftemangel in spezialisierten Bereichen. Unternehmen berichten regelmäßig von Schwierigkeiten, geeignetes Personal zu finden – oft mangelt es an regionaler Verfügbarkeit, passenden Qualifikationen oder an der Kompatibilität bei Gehaltsvorstellungen. Besonders technologische Wachstumsfelder wie Digitalisierung, Cybersicherheit oder GreenTech sind betroffen, was die Nachfrage nach ausländischen Fachkräften oder Investitionen in Aus- und Weiterbildung erhöht.[18]

Im Bereich des Katastrophenschutzes und der Krisen Resilienz verfügt Spanien über eine Vielzahl institutioneller Mechanismen, die auf europäischer und nationaler Ebene ineinandergreifen. Der EU-Solidaritätsfonds (EUSF) stellt finanzielle Hilfe für Mitgliedstaaten nach Naturkatastrophen oder großen Gesundheitskrisen bereit und wurde in Spanien mehrfach genutzt, zuletzt nach dem DANA-Ereignis 2024 in der Region Valencia.[19] Der Begriff DANA (Depresión Aislada en Niveles Altos) beschreibt in Spanien eine hochgelegene, abgeschlossene Tiefdruckzone, die in der Region Valencia regelmäßig zu extremen Wetterphänomenen führt – etwa sintflutartigen Regenfällen, Hagel oder sogar Tornados, wenn kalte Luft aus dem Norden auf warme, feuchte Luftmassen über dem Mittelmeer trifft. Dieses Wetterphänomen war verantwortlich für verheerende Überschwemmungen im Jahr 2024 in der Region Valencia, bei denen hunderte Menschen ums Leben kamen und die Dringlichkeit von Katastrophenresilienz unterstrichen wurde.[20] In Folge dieser extremen Ereignisse wurde der EU-Solidaritätsfonds (EUSF) aktiviert – ein Mechanismus, der gezielt Soforthilfen, Wiederaufbau und Infrastrukturmaßnahmen unterstützt und damit eine wichtige Rolle bei der Krisenbewältigung spielt. Diese Verknüpfung von Naturgefahren, institutionellen Reaktionen und Förderinstrumenten zeigt, wie entscheidend integrierter Katastrophenschutz für Marktteilnehmer ist. Besonders hoch war die Inanspruchnahme dieses Instruments nach Überschwemmungen, die auch in der Vergangenheit erhebliche Schäden verursacht haben – etwa 2019 in Murcia und Alicante. Die EUSF-Mittel werden gezielt für Soforthilfemaßnahmen, Wiederherstellung von Infrastruktur (Wasser, Energie, Bildung etc.) sowie Säuberungs- und Wiederaufbaumaßnahmen verwendet. Der Mechanismus sieht strenge Kriterien vor – u. a. müssen die Schäden über 0,6 Prozente des Bruttonationaleinkommens oder über drei Milliarden Euro (in Preisen von 2011) liegen, damit ein Ereignis als „schwerwiegend“ gilt. In Ausnahmefällen können auch Regionen mit außergewöhnlichen Auswirkungen auf das Leben der Bevölkerung oder die wirtschaftliche Stabilität berücksichtigt werden. Dies verleiht dem Instrument eine hohe strategische Bedeutung für Risikomanagement, Krisenvorsorge und Wiederaufbau – insbesondere für Anbieter sicherheitsrelevanter Technologien, Ausrüstungen oder Infrastrukturdienstleistungen.[21]

[16] https://www.gtai.de/de/trade/spanien-wirtschaft/wirtschaftsstandort
[17] https://www.auswaertiges-amt.de/de/service/laender/spanien-node/bilateral-210216
[18] https://www.gtai.de/de/trade/spanien-wirtschaft/wirtschaftsstandort
[19] https://maldita.es/malditateexplica/20241111/fondo-solidaridad-union-europea-dana/
[20] https://www.reuters.com/business/environment/spains-deadly-dana-weather-phenomenon-its-links-climate-change-2024-10-30/
[21] https://maldita.es/malditateexplica/20241111/fondo-solidaridad-union-europea-dana/

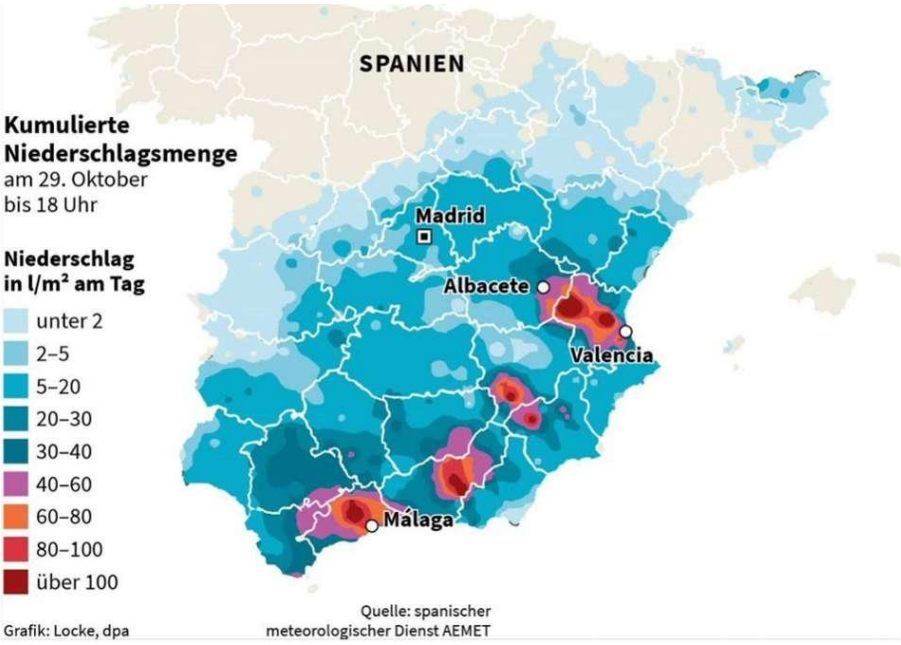


Abbildung 3 Überschwemmungsregionen in Spanien, Oktober 2024[22]

3.1.3 Marktentwicklung

Der spanische Markt für zivile Sicherheits- und insbesondere Cybersicherheitslösungen verzeichnet seit einigen Jahren ein starkes Wachstum, das sich durch mehrere Faktoren erklären lässt. Ein wesentlicher Treiber ist die Bedrohungslage: Spanien ist laut Angaben des spanischen IT-Beraters Secure&IT das weltweit am zweithäufigsten von Cyberangriffen betroffene Land nach den USA. Das starke Wachstum digitaler Kriminalität zeigt sich in einem Anstieg von Cyberangriffen um 35 Prozent allein im Jahr 2024, mit über 45.000 dokumentierten Attacken täglich. Vor diesem Hintergrund plant die spanische Regierung Investitionen von über drei Milliarden Euro in den Ausbau der Cybersicherheit, ein Großteil davon im Kontext der NATO-Verteidigungsausgaben.[23] Diese geplanten Mittel fallen in eine breitere Digitalstrategie, die unter anderem auch Maßnahmen zur Erhöhung der Resilienz von Unternehmen und Infrastrukturen umfasst. Die im Aufbau- und Resilienzplan verankerte sogenannte „Komponente 15“ bündelt Investitionen in Internetsicherheit, 5G-Netzausbau und digitale Konnektivität mit einem Volumen von rund vier Milliarden Euro.[24]

Die Marktentwicklung ist aber nicht nur national getrieben, sondern auch strukturell verankert in internationalen Partnerschaften und Regulierung. Spanien unterhält bilaterale Cybersecurity-Abkommen mit Ländern wie Deutschland, Frankreich, Großbritannien und den USA, um Know-how-Austausch, gemeinsame Übungen und Verteidigungsstrategien zu fördern.[25] So gibt es beispielsweise zwischen Spanien und den USA den ‚Cyber and Digital Dialogue‘, der im Juni 2024 in Washington stattfand – diese Plattform zielt darauf ab, Zusammenarbeit in den Bereichen Cybersicherheit, Krisenresilienz und verantwortliches Verhalten im Cyberraum zu stärken.[26] Des Weiteren vereinbarten Spanien und Deutschland 2022 eine verstärkte industrielle und Forschungstechnologie-Kooperation, etwa im Bereich Mikroelektronik, Cloud-Infrastruktur und High-Performance-Computing, um die technologische Souveränität der EU zu erhöhen.[27] Große Anbieter wie Telefónica Tech, IBM, Cisco oder Entelgy positionieren sich im Markt über neue Plattformlösungen, etwa für SASE-Architekturen oder verteilte Netzwerksicherheit.[28]

Auch der Bereich Katastrophenschutz entwickelt sich technologisch weiter. Künstliche Intelligenz kommt zunehmend zum Einsatz, um Risikogebiete zu kartieren, Echtzeitdaten zu analysieren und Entscheidungsprozesse im

[22] https://www.stuttgarter-nachrichten.de/inhalt.wo-sind-die-ueberschwemmungen-in-spanien-70-tote-gota-fria.27fa464c-1153-46f8-b12c-5ffb8234e2ec.html
[23] https://www.fuchsbriefe.de/spanien-investiert-in-cybersecurity
[24] https://www.gtai.de/de/trade/spanien/wirtschaftsumfeld/unternehmen-lassen-sich-cybersicherheit-mehr-kosten-930418
[25] https://www.mordorintelligence.com/de/industry-reports/spain-cybersecurity-market
[26] https://2021-2025.state.gov/joint-statement-on-the-second-u-s-spain-cyber-and-digital-dialogue/?safe=1
[27] https://www.lamoncloa.gob.es/presidente/actividades/Documents/2022/051022_Anexo-Plan-Accion-conjunto-hispano-aleman.pdf?utm
[28] https://www.mordorintelligence.com/de/industry-reports/spain-cybersecurity-market

Katastrophenmanagement zu unterstützen. Behörden nutzen KI zur dynamischen Überwachung, etwa zur frühzeitigen Erkennung von Waldbränden, und zur Planung von Evakuierungen auf Basis von Szenario Simulationen. Auch soziale Medien werden in Echtzeit ausgewertet, um akuten Bedarf an Wasser, Lebensmitteln oder medizinischer Hilfe besser einschätzen zu können.[29] Diese technologischen Entwicklungen sind bereits Teil strategischer Dokumente auf nationaler Ebene. Im Oktober 2024 wurde die neue spanische Zivilschutzstrategie verabschiedet, die Künstliche Intelligenz als prioritären Bestandteil der Gefahrenprävention und des Krisenmanagements definiert. Sie verfolgt das Ziel, Risiken nicht nur zu begegnen, sondern durch Früherkennung, Ressourcenkontrolle und Schadensprognosen möglichst zu verhindern.[30]

Auch europäische Instrumente wie der EU-Zivilschutzmechanismus und das Copernicus-Programm kommen regelmäßig zum Einsatz, etwa bei Hochwasserkatastrophen wie der DANA 2024 in der Region Valencia. Über 60 Satellitenkarten unterstützten dabei die Einsatzkräfte bei der Schadensbewertung und Ressourcenlenkung. Zusätzlich kamen internationale Hilfsteams über EU-Koordinierungsstrukturen zum Einsatz, was die enge Verzahnung nationaler und europäischer Akteure unterstreicht.[31]

Gleichzeitig schreitet die Gesetzgebung voran: Mit dem neuen Gesetz zum Schutz und zur Resilienz kritischer Einrichtungen (CER) wird eine europaweit harmonisierte Grundlage geschaffen, die Sicherheitsanforderungen in den Sektoren Energie, Wasser, Gesundheit, Verwaltung und Transport verschärft. Die neue nationale Koordinationsstelle CNPREC erhält dabei weitreichende Befugnisse, um länderübergreifende Sicherheitsvorgaben durchzusetzen und den Schutz kritischer Infrastrukturen zu gewährleisten.[32]

Das spanische Cybersecurity-Institut INCIBE unterstützt aktiv Forschung und Innovation, insbesondere durch das Netzwerk RENIC, das Universitäten, Forschungseinrichtungen und Technologiezentren im Bereich Cybersecurity vernetzt und gemeinsame Forschungsprojekte fördert. Zudem stellt RENIC über Katalog und Wissenslandkarte detaillierte Informationen zu Forschungszentren, Projekten und Forschungsschwerpunkten bereit – ideal zur Stärkung von Kooperationen zwischen Wissenschaft und Industrie.[33] [34] Im Bereich Katastrophenschutz verbindet der Nationale Aktionsplan „Horizon 2035“ gezielt Forschung mit Governance und Innovation: Der vom spanischen Regierungsrat im Oktober 2022 verabschiedete Plan verankert einen wissenschaftlichen Beirat und Forschungsförderlinien, um Krisenprävention und evidenzbasiertes Management zu stärken.[35]

3.1.4 Der Arbeitsmarkt und das (Aus-)Bildungswesen

Ein funktionierender Arbeitsmarkt und ein leistungsfähiges Bildungssystem sind zentrale Rahmenbedingungen für sicherheitsrelevante Branchen, da technologische Entwicklung und Umsetzung maßgeblich von gut qualifiziertem Personal abhängen.[36] Der spanische Arbeitsmarkt ist trotz rückläufiger Arbeitslosigkeit weiterhin von strukturellen Herausforderungen geprägt. Zwar lag die Arbeitslosenquote im Jahr 2024 laut EU-Kommission bei 11,6 Prozent und soll bis 2025 auf 11,1 Prozent sinken, dennoch gehört Spanien weiterhin zu den Ländern mit den höchsten Arbeitslosenquoten Europas. Besonders deutlich ist der demografische Wandel spürbar: Die Geburtenrate liegt auf einem historischen Tief bei 1,12 Geburten pro Frau[37], während die Lebenserwartung steigt – ein Trend, der zu einer rasch alternden Erwerbsbevölkerung führt.[38] So liegt der Anteil der unter 15-Jährigen aktuell bei nur 12,62 Prozent, während 21,64 Prozent der Bevölkerung 65 Jahre und älter sind – ein klares Zeichen für den Strukturwandel hin zu einer älteren Gesellschaft.[39] Parallel dazu beträgt die durchschnittliche Lebenserwartung bei der Geburt bei rund 83 Jahre (Stand: 2023).[40] Diese Diskrepanz – immer weniger Geburten bei einer zunehmend langlebigen Bevölkerung –

[29] https://www.laecuaciondigital.com/tecnologias/inteligencia-artificial/cinco-aplicaciones-de-la-ia-en-la-prevencion-y-mitigacion-de-desastres-naturales/
[30] https://www.democrata.es/analisis-y-opinion/inteligencia-artificial-para-la-proteccion-civil/
[31] https://civil-protection-humanitarian-aid.ec.europa.eu/news-stories/stories/flash-floods-spain-joining-forces-rapid-recovery_en
[32] http://crick1.subsec.mir.es:11990/es/detail-page/articulo/EL-CNPIC-FUTURO-CNPREC-SERA-EL-EJE-CENTRAL-EN-LA-PROTECCION-Y-RESILIENCIA-DE-LAS-ENTIDADES-CRITICAS/
[33] https://www.incibe.es/en/incibe/corporate-information/who-we-work-with/network-excellence-cybersecurity-rdi?utm
[34] https://renic.es/en/about-us/?utm
[35] https://www.lamoncloa.gob.es/lang/en/gobierno/councilministers/paginas/2022/20221031_council.aspx
[36] https://www.gtai.de/de/trade/spanien-wirtschaft/wirtschaftsstandort
[37] https://datacommons.org/place/country/ESP?utm_medium=explore&mprop=fertilityRate&popt=Person&cpv=gender,Female&hl=en
[38] https://www.gtai.de/de/trade/spanien-wirtschaft/arbeitsmarkt
[39] https://www.gtai.de/de/trade/spanien-wirtschaft/arbeitsmarkt
[40] https://www.dsw.org/laenderdatenbank/?utm

führt zu einer rasch alternden Erwerbsbevölkerung, was insbesondere für die nationale wie unternehmensbezogene Zukunftsplanung relevant ist. Gleichzeitig verzeichnet Spanien einen Fachkräftemangel in vielen Bereichen, insbesondere in technologieintensiven Branchen wie der Cybersicherheit. Unternehmen berichten regelmäßig von Schwierigkeiten bei der Besetzung offener Stellen, die sowohl auf mangelnde regionale Verfügbarkeit als auch auf unpassende Qualifikationen und unterschiedliche Gehaltsvorstellungen zurückzuführen sind. Obwohl im zweiten Quartal 2024 ein Rekord von 21,7 Millionen sozialversicherungspflichtig Beschäftigten erreicht wurde, bleibt die Passung zwischen Angebot und Nachfrage weiterhin unzureichend. Besonders betroffen ist die Privatwirtschaft in Bereichen wie Großhandel und wissenschaftlich-technische Dienstleistungen, wo trotz vergleichsweise geringer Vakanz-Quote weiterhin Engpässe bestehen.[41]

Diese Entwicklungen spiegeln sich auch in den Gehältern wider: Laut der Personalberatung Hays sind die Löhne 2024 weiter gestiegen, mit besonders hohen Zuwächsen im Kundendienst (+8 Prozent) sowie in der Digitalwirtschaft (+5 Prozent). Parallel dazu rückt das Thema Arbeitszeit verstärkt in den Fokus: Ab dem 1. Januar 2025 plant das Arbeitsministerium eine Reduzierung der Wochenarbeitszeit von 40 auf 37,5 Stunden. Unternehmen wie Telefónica testen sogar Modelle mit einer 36-Stunden-Woche. Während Arbeitnehmer diese Entwicklung mit Blick auf eine bessere Work-Life-Balance überwiegend begrüßen, äußern Arbeitgeber – insbesondere im Gastgewerbe – Kritik wegen erwarteter Kostensteigerungen. Insgesamt befindet sich der Arbeitsmarkt in einem Wandel, was auch durch eine gestiegene Wechselbereitschaft unter Beschäftigten belegt wird: Laut Hays stieg diese von 2023 auf 2024 um sieben Prozentpunkte auf 70 Prozent. Als Hauptgründe gelten fehlende Entwicklungsperspektiven, unzureichende Karrierechancen und Gehälter unter den Erwartungen. Im Umkehrschluss können eine wertschätzende Unternehmenskultur, gezieltes Feedback sowie klare Weiterentwicklungsmöglichkeiten die Mitarbeiterbindung erheblich stärken.[42]

Im Bereich Cybersicherheit ist der Fachkräftemangel besonders ausgeprägt: Die Nachfrage nach spezialisierten Arbeitskräften übersteigt das Angebot deutlich, was sich auch in vergleichsweise hohen Gehältern widerspiegelt – z. B. durchschnittlich 39.600 Euro für Einsteiger und bis zu 44.000 Euro für erfahrene Fachkräfte im Bereich IT-Audit.[43] Die Zahl der Cybersicherheitsexperten in Spanien lag 2021 laut ISC bei 124.226 (0,25 Prozent der Bevölkerung), während sie in den USA bei über 1,1 Millionen lag (0,32 Prozent der Bevölkerung).[44] Damit verfügte Spanien über rund 11 Prozent der Fachkräfte im Vergleich zu den USA. Der Wettbewerb um Talente wird zusätzlich durch internationale Großunternehmen verstärkt, die qualifiziertes Personal vom Markt absorbieren.[45]

Gebiet	2023	2022	Veränderung 2023/2022[2)]
Landesdurchschnitt Spanien	2.213,0	2.112,7	4,7%
Hauptstadt (Madrid)	2.670,0	2.529,0	5,6%
Hochlohnregion (Madrid, Baskenland)	2.590,0	2.474,9	4,6%
Niedriglohnregion (Kanaren, Extremadura)	1.778,1	1.729,9	2,8%

1) Jahresdurchschnittslohn geteilt durch zwölf Monate; Hoch- und Niedriglohnregionen wurden mit dem Durchschnitt der beiden Regionen errechnet; 2) nominale Veränderung 2023 gegenüber 2022

Tabelle 22 Durchschnittliche Bruttomonatslöhne nach Region [1)] [46]

Um dieser Entwicklung zu begegnen, reagiert das Bildungssystem mit einer zunehmenden Ausdifferenzierung spezialisierter Ausbildungsgänge und Studienangebote im Bereich Cybersicherheit. Gefragt sind dabei nicht nur klassische IT-Profile, sondern zunehmend auch interdisziplinäre Rollen wie Cyberjuristen, Analysten für staatliche Cyberoperationen, Psychologen für Social Engineering oder Journalisten zur Aufdeckung von Desinformationskampagnen. Besonders nachgefragt sind praxisnahe Ausbildungsgänge wie die Fachrichtung

[41] https://www.gtai.de/de/trade/spanien-wirtschaft/wirtschaftsstandort
[42] https://www.gtai.de/de/trade/spanien-wirtschaft/arbeitsmarkt
[43] https://www.gtai.de/de/trade/spanien/wirtschaftsumfeld/unternehmen-lassen-sich-cybersicherheit-mehr-kosten-930418
[44] https://www.mordorintelligence.com/de/industry-reports/spain-cybersecurity-market
[45] https://www.gtai.de/de/trade/spanien/wirtschaftsumfeld/unternehmen-lassen-sich-cybersicherheit-mehr-kosten-930418
[46] Statistikamt INE, Encuesta Anual de Coste Laboral 2023; Berechnungen von Germany Trade & Invest

„Administration von Netzwerksystemen mit Schwerpunkt Cybersicherheit“, aber auch spezialisierte Masterprogramme in Cyberintelligence und KI-gestützter Sicherheitstechnologie.[47]

3.1.5 Sicherheitspolitische Entwicklungen im Zielmarkt

In den vergangenen Jahren hat sich die sicherheitspolitische Ausrichtung Spaniens spürbar verschärft. Die Zahl und Komplexität von Cyberangriffen nehmen rasant zu: Allein 2024 wurden über 45.000 Attacken pro Tag registriert – ein Anstieg um 35 Prozent gegenüber dem Vorjahr. Damit folgt Spanien einem globalen Trend, der laut internationalen Studien einen Zuwachs von 64 Prozent verzeichnete. Diese Entwicklung erhöht den Druck auf Politik und Wirtschaft, digitale Schutzmaßnahmen deutlich auszuweiten. Die spanische Regierung reagiert darauf mit umfassenden Investitionen: Bis 2027 sollen rund 3 Mrd. Euro in die Cybersicherheit fließen. Ein Großteil dieser Mittel wird im Rahmen der NATO-Verteidigungsausgaben verortet, was die Umsetzungschancen für Projekte erhöht und die europäische sicherheitspolitische Koordinierung weiter vorantreibt.[48]

Parallel zu diesen digitalen Entwicklungen treibt Spanien den Einsatz künstlicher Intelligenz (KI) im Bevölkerungsschutz voran. In der Risikoanalyse erlaubt KI die Auswertung historischer Daten zur Erstellung präziser Gefahrenkarten. In Spanien sind rund 2,7 Millionen Haushalte in Hochwassergebieten angesiedelt, weshalb die Identifikation gefährdeter Zonen hohe Priorität genießt. Bei extremen Wetterereignissen wie der DANA-Episode in Málaga unterstützte KI-basierte Information die Behörden bei rechtzeitigen Evakuierungsentscheidungen. Auch in der operativen Planung leistet KI wertvolle Beiträge. Dynamisch gepflegte Datenbanken liefern Echtzeitinformationen zu verfügbaren Ressourcen, wie Löschmitteln oder schwerem Gerät, die in Szenario Simulationen integriert werden können. Damit lassen sich Handlungsstrategien an das konkrete Schadensbild und die aktuelle Verfügbarkeit von Einsatzmitteln anpassen. Besonders Einsatzkräfte wie die spanische militärische Notfalleinheit MUE profitieren von dieser erhöhten Planungssicherheit. Ein weiteres sicherheitsrelevantes Anwendungsfeld von KI ist die Überwachung und Früherkennung von Waldbränden. Durch die Kombination von KI, Sensorik und Überwachungskameras werden Hitzepunkte frühzeitig identifiziert. Ergänzend liefern Drohnen und Satelliten in Echtzeit Lagekarten, die eine schnelle und gezielte Reaktion der Einsatzkräfte ermöglichen. Diese Technologien sind insbesondere in von Hitze und Dürre bedrohten Regionen ein zentrales Instrument der präventiven Gefahrenabwehr.[49]

Die konsequente Integration digitaler Technologien in den Zivilschutz stellt einen sicherheitspolitischen Paradigmenwechsel dar. Spanien verfolgt das Ziel, zivile und militärische Sicherheitsinfrastrukturen technologisch enger zu verzahnen und so nationale Resilienz gegenüber multiplen Bedrohungen zu erhöhen. Durch die zunehmende Bedeutung von KI und Cybersicherheit entstehen gleichzeitig neue Marktpotenziale für Anbieter entsprechender Technologien. Auch deutsche Unternehmen aus den Bereichen Sensorik, KI-basierte Analyse, kritische Infrastruktur und Cybersicherheit können in Spanien vom technologischen Modernisierungskurs profitieren.[50] [51]

3.1.6 Die aktuelle Gesetzeslage und geplante Reformen

Die zivile Sicherheitsarchitektur Spaniens befindet sich im Spannungsfeld zwischen europäischer Harmonisierung, nationaler Souveränität und technologischer Transformation. Ein zentrales Regelwerk zur finanziellen Unterstützung nach Naturkatastrophen oder Gesundheitskrisen ist der Europäische Solidaritätsfonds (EUSF), der auch Spanien mehrfach zugutekam – zuletzt im Rahmen der COVID-19-Pandemie. Die gesetzliche Grundlage erlaubt es der EU, Mittel bei Großschadensereignissen bereitzustellen, wobei Mindestschwellen für Schäden und Auswirkungen auf Bevölkerung, Umwelt oder Wirtschaft definiert sind.[52] Auf nationaler Ebene wurde die Gesetzeslage im Bereich der Cybersicherheit zuletzt über mehrere strategischen Instrumente fortentwickelt. Die sogenannte Komponente 15 des nationalen Auf- und Resilienzplans bündelt Maßnahmen zur Internetsicherheit, 5G-Ausbau und digitaler Konnektivität und ist mit rund 4 Milliarden Euro ausgestattet.[53] Ein expliziter gesetzlicher Rahmen für Sicherheit in 5G-Netzen wurde

[47] https://elpais.com/economia/formacion/2024-11-29/se-buscan-expertos-en-cibersegurdad.html
[48] https://www.fuchsbriefe.de/spanien-investiert-in-cybersecurity
[49] https://www.laecuaciondigital.com/tecnologias/inteligencia-artificial/cinco-aplicaciones-de-la-ia-en-la-prevencion-y-mitigacion-de-desastres-naturales/
[50] https://www.fuchsbriefe.de/spanien-investiert-in-cybersecurity
[51] https://www.laecuaciondigital.com/tecnologias/inteligencia-artificial/cinco-aplicaciones-de-la-ia-en-la-prevencion-y-mitigacion-de-desastres-naturales/
[52] https://maldita.es/malditateexplica/20241111/fondo-solidaridad-union-europea-dana/
[53] https://www.gtai.de/de/trade/spanien/wirtschaftsumfeld/unternehmen-lassen-sich-cybersicherheit-mehr-kosten-930418

durch das Königliche Gesetzesdekret zur 5G-Cybersicherheit im April 2022 geschaffen. Es überträgt die EU-weiten Anforderungen aus dem sogenannten 5G-Toolbox in spanisches Recht.[54]

Mit dem neuen Gesetz zum Schutz und zur Resilienz kritischer Einrichtungen (CER) verfolgt Spanien das Ziel, die Anforderungen der EU-Richtlinie zum Schutz kritischer Infrastrukturen systematisch umzusetzen. Dieses Gesetz schafft neue Zuständigkeiten für das Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC), das zum CNPREC (Centro Nacional para la Protección y Resiliencia de las Entidades Críticas) mit erweiterten Aufgaben ausgebaut wird. Kritische Betreiber in Sektoren wie Energie, Gesundheit, Transport oder Wasserversorgung werden verpflichtet, Resilienz Pläne zu erstellen, Sicherheitsbeauftragte zu benennen und sicherheitsrelevante Vorfälle unverzüglich zu melden. Die rechtlichen Maßnahmen zielen darauf ab, den kontinuierlichen Betrieb lebenswichtiger Dienste sicherzustellen, insbesondere in Krisensituationen. Der Gesetzentwurf sieht zudem die Einrichtung eines strukturierten strategischen Planungs- und Meldeverfahrens vor, das in die Nationale Bedrohungs- und Risikoanalyse eingebettet ist. Die Dringlichkeit des Vorhabens spiegelt sich auch im politischen Prozess wider: Das Gesetz wird im beschleunigten Verfahren durch die ministeriellen Gremien gebracht, wodurch sich die Bearbeitungsfristen halbieren.[55]

Ein flankierendes Element zur nationalen Resilienz ist das spanische Zivilschutzgesetz, das bereits mit dem Gesetz 17/2015 zur Organisation des Sistema Nacional de Protección Civil verankert ist. Dieses nationale System sieht abgestimmte Maßnahmen von Zentralregierung, autonomen Gemeinschaften und Kommunen vor und umfasst alle Phasen des Katastrophenzyklus: Prävention, Vorbereitung, Reaktion, Wiederherstellung und Evaluation.

Zusätzlich wurden in den letzten Jahren sektorale Notfallpläne weiterentwickelt, etwa für Hochwasser- oder Waldbrandrisiken. So verpflichten die Flood Risk Management Plans die Behörden zur Erstellung von Gefahrenkarten, Risikoeinschätzungen und technischen Leitlinien zur Risikovorsorge in gefährdeten Regionen.[56] Zukünftige gesetzgeberische Entwicklungen dürften stärker auf die Verzahnung von Technologie und Sicherheitsarchitektur abzielen. Die Rolle von KI bei der Vorhersage, Analyse und Koordination von Notfällen wird dabei nicht nur strategisch verankert, sondern auch regulatorisch flankiert werden müssen.[57]

3.1.7 Regelungen für öffentliche Aufträge und deren Vergabe

Spanien verfolgt im Bereich der öffentlichen Beschaffung einen zweigleisigen Ansatz: Einerseits setzt die nationale Gesetzgebung auf Transparenz, Digitalisierung und Wettbewerb, andererseits bestehen föderale Spielräume auf Ebene der Autonomen Gemeinschaften. Im Zentrum der staatlichen Vergabestrategie stehen Maßnahmen zur Förderung unterentwickelter Regionen und strukturschwacher Gebiete. So können kleine Unternehmen bei Projekten in dünn besiedelten Regionen Zuschüsse von bis zu 70 Prozent erhalten, wobei Förderhöhe und Bedingungen unter anderem von der Unternehmensgröße abhängen. Die zentralstaatliche Agentur ICEX sowie regionale Wirtschaftsförderinstitutionen koordinieren Investitions- und Förderprogramme und fungieren auch als zentrale Ansprechpartner für öffentliche Ausschreibungen mit Auslandsbezug. Zusätzlich agieren einzelne Kommunen eigenständig, wie etwa Barcelona, das durch gezielte Steuererleichterungen Investitionsanreize für innovative Unternehmen und Start-ups schafft. Ein wichtiges Element der öffentlichen Vergabepolitik ist zudem die Einbindung europäischer Fördermittel, insbesondere aus dem Next Generation EU-Programm und der EU-Kohäsionsförderung. Diese Mittel fließen nicht nur in Infrastruktur- und Umweltprojekte, sondern auch gezielt in innovationsgetriebene öffentliche Beschaffungsvorhaben.[58]

Gerade bei Digitalisierungs- und Sicherheitsprojekten haben spanische Behörden die strategische Beschaffung als Steuerungsinstrument entdeckt. Öffentliche Auftraggeber legen zunehmend Kriterien zu Cybersecurity, Datenschutz und nachhaltiger Digitalisierung als Vergabevoraussetzung fest. Die sogenannte Komponente 15 des nationalen Wiederaufbauplans verknüpft Investitionen in Internetsicherheit, 5G-Infrastruktur und Konnektivität mit gezielten öffentlichen Ausschreibungen. Die Finanzierungsrahmen belaufen sich hierbei auf knapp 4 Milliarden Euro, wodurch auch zahlreiche öffentliche Großprojekte für Anbieter aus dem Bereich ziviler Sicherheitslösungen geöffnet werden.[59]

---

[54] https://www.mordorintelligence.com/de/industry-reports/spain-cybersecurity-market
[55] http://crick1.subsec.mir.es:11990/es/detail-page/articulo/EL-CNPIC-FUTURO-CNPREC-SERA-EL-EJE-CENTRAL-EN-LA-PROTECCION-Y-RESILIENCIA-DE-LAS-ENTIDADES-CRITICAS/
[56] https://4elitech.com/seguridad-en-infraestructuras-criticas-en-espana/
[57] Modor Intelligence
[58] https://www.gtai.de/de/trade/spanien-wirtschaft/wirtschaftsstandort
[59] https://www.gtai.de/de/trade/spanien/wirtschaftsumfeld/unternehmen-lassen-sich-cybersicherheit-mehr-kosten-930418

Zusätzlich bestehen branchenspezifische Notfall- und Schutzpläne, etwa für den Hochwasserschutz oder für den Fall von Waldbränden, die ebenfalls vergaberelevante Maßnahmen auslösen. Die Umsetzung erfolgt dabei im Rahmen regionaler und lokaler Zuständigkeiten, was eine dezentrale Vergabepraxis mit sich bringt. Ausländische Unternehmen, insbesondere aus der EU, sind grundsätzlich zur Teilnahme an spanischen Ausschreibungen berechtigt, müssen sich jedoch mit dem föderal geprägten Aufbau und den lokalen Ausschreibungsportalen vertraut machen.[60]

3.2 Aktuelle Vorhaben, Projekte und Ziele

Spanien verfolgt derzeit eine Vielzahl strategischer Projekte zur Stärkung seiner zivilen Sicherheitsinfrastruktur sowie im Bereich der Cybersecurity, um zukünftigen Bedrohungslagen besser begegnen zu können. Ein zentrales Vorhaben ist die verstärkte Nutzung von KI in der Katastrophenprävention, insbesondere zur Identifikation hochgefährdeter Gebiete wie Überschwemmungsregionen. Hier gilt beispielsweise die Region Murcia als besonders gefährdet: Laut aktuellen Risikokarten befinden sich dort 26,9 Prozent aller Immobilien in Hochwasserzonen – der höchste Anteil in Spanien. Dieses Risiko unterstreicht die Bedeutung von KI-gestützten Analysen, um Überschwemmungsregionen frühzeitig zu identifizieren und Evakuierungsmaßnahmen gezielt einzuleiten.[61] Über 2,7 Millionen Wohnhäuser in Spanien befinden sich laut Umweltministerium in Risikozonen – mithilfe KI-gestützter Risikoanalysen konnten Behörden bereits gezielte Evakuierungsmaßnahmen durchführen, wie im Fall der DANA-Episode in Málaga. Darüber hinaus kommt KI bei der Ressourcenplanung in Notfällen zum Einsatz: Dynamische Datenbanken ermöglichen in Echtzeit eine optimierte Verteilung von Rettungsressourcen wie Maschinen oder Löschsystemen. Im Bereich der Frühwarnsysteme für Waldbrände setzt Spanien verstärkt auf sensorbasierte Überwachung, kombiniert mit Drohnen- und Satellitentechnologien. Diese generieren Echtzeitkarten und ermöglichen so schnelle Interventionen in Hochrisikozonen. Einen innovativen Ansatz stellt die Auswertung sozialer Medien dar, um in Krisensituationen aktuelle Bedürfnisse der Bevölkerung wie Wasser, Nahrung oder medizinische Versorgung zu identifizieren. Dazu durchsucht die KI Beiträge wie beispielsweise Tweets oder Instagram-Posts auf Schlagworte oder Hashtags zu grundlegenden Bedarfen wie „Wasser“, „Nahrung“, „Medizin“ oder „Unterkunft“, klassifiziert diese automatisch und nutzt Geodaten, um Echtzeit-Cluster von Hilfsanfragen zu identifizieren – etwa um herauszufiltern, wer was braucht und wo (z. B. medizinische Hilfe, Nahrung, Unterkunft). Auch in der Wiederaufbauphase nach Katastrophen spielt KI eine tragende Rolle: Auf Grundlage gesammelter Daten kann der Zustand von Infrastruktur und wirtschaftlichen Auswirkungen erfasst und daraus notwendige Investitionsmaßnahmen abgeleitet werden. [62] [63] Im Bereich der kritischen Kommunikation modernisiert Spanien derzeit seine Netzinfrastrukturen, insbesondere die Systeme Malla B und SIRDEE, die im Krisenfall sichere Verbindungen zwischen Regierung, Sicherheitskräften und Rettungsdiensten gewährleisten sollen. Nach Schwachstellenanalysen aus vorherigen Krisen (z. B. Stromausfall April 2025) wird die Integration beider Systeme forciert, ergänzt durch neue Verschlüsselungstechnologien wie „Secret T“, um eine durchgängige Kommunikation sicherzustellen. Parallel dazu investiert Spanien im Rahmen europäischer Programme wie IRIS sowie im nationalen Projekt „SpainSat NG“ in satellitengestützte Kommunikation zur vollständigen Redundanz im Krisenfall.[64] Zudem werden bauliche Präventionsmaßnahmen forciert: Neue Gebäude in gefährdeten Regionen sollen erdbebensicher konstruiert werden – etwa durch Basis-Isolierungen oder flexible Materialien, die horizontale Erschütterungen abfedern. Bestehende Gebäude lassen sich durch strukturelle Verstärkungen nachrüsten, um die Widerstandsfähigkeit gegenüber Naturkatastrophen zu erhöhen. In ländlichen Regionen will die Regierung lokale Anwohner in die Waldbrandprävention einbinden, indem sie aktiv an der Säuberung von Risikozonen beteiligt werden.[65]

Auch auf legislativer Ebene wurde durch das Gesetz 8/2011 zur Infrastrukturkritikalität sowie den Nationalen Schutzplan ein umfassender Rahmen zur Identifikation und Absicherung kritischer Einrichtungen geschaffen. Diese beinhalten sektorale Risikobewertungen, Maßnahmenkataloge und ein koordinierendes Zentrum (CNPIC), das im Krisenfall zentrale Steuerungsaufgaben übernimmt.[66] Im Bereich der Cybersicherheit verfolgt Spanien ambitionierte Ziele: Mit einem Marktvolumen von 2,27 Mrd. USD (2024) und einer prognostizierten jährlichen Wachstumsrate von 7,16 Prozent entwickelt sich dieser Sektor dynamisch. Treiber sind neben zunehmender Digitalisierung auch staatliche

[60] Planning and management of resources against disasters in Spain by Jose Alberto Piñeiro Ramirez
[61] https://www.waternewseurope.com/new-maps-double-flood-risks-of-spanish-homes/?utm
[62] https://www.researchgate.net/publication/391538352_AI-Driven_Social_Media_Analysis_for_Disaster_Situational_Awareness_in_Smart_Urban_Environments?utm
[63] https://www.laecuaciondigital.com/tecnologias/inteligencia-artificial/cinco-aplicaciones-de-la-ia-en-la-prevencion-y-mitigacion-de-desastres-naturales/
[64] https://www.xatakamovil.com/conectividad/malla-b-sirdee-sistemas-comunicacion-segura-estado-trabajan-para-reducir-riesgo-quedar-incomunicados
[65] https://www.laecuaciondigital.com/tecnologias/inteligencia-artificial/cinco-aplicaciones-de-la-ia-en-la-prevencion-y-mitigacion-de-desastres-naturales/
[66] https://invescon.es/proteccion-de-infraestructuras-criticas-en-espana/

Förderprogramme wie das „Digital Kit“ sowie Investitionen in Höhe von 8,8 Mrd. Euro im Rahmen der „Agenda España Digital 2025“.[67] Außerdem verfolgt die Regierung das Ziel, die nationale Rüstungs- und Sicherheitsindustrie durch gezielte Aufträge zu stärken, etwa mit dem „Plan Industrial y Tecnológico para la Seguridad y la Defensa“, der auch zivilschutzrelevante Komponenten beinhaltet. Hiervon profitieren auch KMU und Start-ups, insbesondere in den Bereichen Cybersicherheit, Kommunikationstechnologien und Notfallmanagement.[68]

Der spanische Technologiekonzern Indra ist dabei einer der wichtigsten industriellen Partner bei der Umsetzung nationaler Sicherheits- und Digitalisierungsprojekte. Im Rahmen des Projekts „SpainSat NG“ ist Indra unter anderem an der Entwicklung von Erdstationen und Kryptosystemen für die sichere Satellitenkommunikation beteiligt. Zudem engagiert sich das Unternehmen in Bereichen wie Frühwarnsysteme, sichere Behördenkommunikation und KI-gestützte Analytik im Katastrophenschutz.[69]

3.3 Wettbewerbssituation / Politische und Rechtliche Rahmenbedingungen

Der Markt für zivile Sicherheitstechnologien in Spanien befindet sich in einer dynamischen Entwicklung und ist geprägt von einem Zusammenspiel staatlicher Impulse, strategischer Industriepartnerschaften sowie wachsender regulatorischer Anforderungen.[70] Die spanische Regierung hat in den letzten Jahren umfangreiche Pläne zur Digitalisierung, Infrastrukturmodernisierung und Krisenprävention auf den Weg gebracht. Diese werden sowohl auf nationaler Ebene – etwa durch das Innen- und Verteidigungsministerium – als auch durch europäische Programme koordiniert.[71] Dabei nimmt der Staat eine aktive Rolle als Auftraggeber und Regulierer ein, insbesondere durch sektorübergreifende Strategien wie den „Nationalen Katastrophenschutzplan“ oder die Programme zur kritischen Infrastrukturabsicherung.[72]

Die Marktstruktur ist geprägt durch einige große Systemanbieter mit starker internationaler Vernetzung, flankiert von spezialisierten kleinen und mittleren Unternehmen, die sich auf Nischenlösungen konzentrieren – etwa im Bereich KI-basierter Analytik, Frühwarnsysteme oder verschlüsselter Kommunikation. Aufgrund der sicherheitsrelevanten Natur vieler Produkte unterliegt der Markt zugleich komplexen regulatorischen Anforderungen, etwa im Hinblick auf Zulassungen, technische Standards, Exportkontrollen sowie Datenschutzbestimmungen. Darüber hinaus existieren vielfältige Förderinstrumente zur Markteinführung, Forschung und Internationalisierung, wobei insbesondere Digitalisierungs- und Resilienz Programme eine zentrale Rolle spielen. [73]

3.3.1 Wichtige Akteure des zivilen Sicherheitsmarktes

Der spanische Markt für zivile Sicherheit ist geprägt von einer engen Verzahnung staatlicher Institutionen, halbstaatlicher Akteure sowie privatwirtschaftlicher Unternehmen mit strategischer Bedeutung. Die spanische Regierung verfolgt eine gezielte Industriepolitik, um nationale Schlüsselakteure im Bereich Sicherheit und Verteidigung zu fördern und international wettbewerbsfähig zu positionieren.[74] Ein zentrales Beispiel hierfür ist das börsennotierte Technologieunternehmen Indra, das zunehmend als nationaler Champion aufgebaut wird. Über die staatliche Beteiligungsgesellschaft SEPI hält der Staat knapp 28 Prozent an Indra, was politischen Einfluss auf strategische Unternehmensentscheidungen ermöglicht. In den letzten Jahren hat Indra gezielt in strategisch relevante Segmente investiert – etwa durch die Übernahme von Deimos Space, die geplante Akquisition von EM&E sowie durch den Einstieg in den Bereich Weltraumkommunikation mit der Gründung von Indra Space nach der Übernahme des Satellitenbetreibers Hispasat.[75]

Ein weiterer relevanter Akteur im Bereich der zivilen Sicherheit ist die Militärische Notfalleinheit (Unidad Militar de Emergencias – UME), die dem Verteidigungsministerium unterstellt ist und für Großschadenslagen, Naturkatastrophen sowie internationale Hilfseinsätze eingesetzt wird. Seit ihrer Gründung im Jahr 2005 wurde der rechtliche Rahmen kontinuierlich angepasst, um ihre Einsatzfähigkeit, Interventionsgeschwindigkeit und institutionelle Anbindung zu

[67] https://www.mordorintelligence.com/de/industry-reports/spain-cybersecurity-market
[68] https://www.gtai.de/de/trade/spanien/branchen/spanien-investiert-kraeftig-in-die-verteidigung-1894360
[69] https://www.xatakamovil.com/conectividad/malla-b-sirdee-sistemas-comunicacion-segura-estado-trabajan-para-reducir-riesgo-quedar-incomunicados
[70] Planning and management of resources against disasters in Spain by Jose Alberto Piñeiro Ramirez
[71] https://www.mordorintelligence.com/de/industry-reports/spain-cybersecurity-market
[72] https://invescon.es/proteccion-de-infraestructuras-criticas-en-espana/
[73] https://www.mordorintelligence.com/de/industry-reports/spain-cybersecurity-market
[74] https://www.gtai.de/de/trade/ausschreibungen-projekte/geber/spanische-agentur-internationale-entwicklungszusammenarbeit
[75] https://www.gtai.de/de/trade/spanien/branchen/spanien-investiert-kraeftig-in-die-verteidigung-1894360

stärken. Die UME agiert heute nicht nur national, sondern auch im Rahmen von EU- und UN-Missionen, was sie zu einem wichtigen Bestandteil des staatlichen Katastrophenschutzsystems macht.[76] Auf institutioneller Ebene spielt das CNPIC (Centro Nacional para la Protección de las Infraestructuras Críticas) eine zentrale Rolle im Schutz kritischer Infrastrukturen. Mit der jüngsten Reform soll es künftig als CNPREC agieren und ist dabei als nationales Koordinationszentrum für Resilienzplanung, Risikobewertung und sektorübergreifende Kooperation konzipiert. Der Fokus liegt auf der Sicherstellung von essenziellen Dienstleistungen in Bereichen wie Energie, Gesundheit, öffentlicher Verwaltung und Transport.[77]

Auf internationaler Ebene arbeitet Spanien eng mit Partnern in der EU und der NATO zusammen und ist in verschiedene Kooperationsmechanismen eingebunden, etwa über bilaterale Cybersecurity-Abkommen mit Deutschland, Frankreich, dem Vereinigten Königreich und den USA.[78] Die Einbindung in europäische Förderprogramme wie den EU-Solidaritätsfonds ermöglicht es zudem, externe Finanzmittel für Infrastrukturwiederaufbau und Krisen Resilienz zu mobilisieren, wie zuletzt nach der DANA-Katastrophe 2024.[79] Neben staatlichen und halbstaatlichen Akteuren ist auch die private Sicherheitswirtschaft von hoher Bedeutung. Unternehmen wie Telefónica Tech, Microsoft, NTT Data, Innotec, Minsait und Cisco Systems kooperieren eng mit Behörden und leisten technologische Beiträge in Bereichen wie Cybersecurity, Blockchain-Infrastruktur und Cloud-Diensten. Die zunehmende Digitalisierung öffentlicher und privater Strukturen schafft dabei neue Bedarfe für Sicherheitslösungen, was wiederum den Marktzugang für deutsche Anbieter mit speziellem Know-how begünstigen kann.[80] Insgesamt ist der spanische zivile Sicherheitsmarkt stark institutionell eingebettet, technologisch ambitioniert und durch strategische Allianzen geprägt. Für deutsche Unternehmen ergeben sich daraus vielfältige Kooperations- und Markteintrittsmöglichkeiten – insbesondere im Umfeld öffentlicher Ausschreibungen, technologischer Partnerschaften und strukturierter Projektfinanzierung.[81]

Kategorie	Akteure	Rolle/Bedeutung
Staatlich/halbstaatlich	SEPI	Staatliche Beteiligungsgesellschaft (28% an Indra)
	UME	Militärische Notfalleinheit für Katastrophenschutz
	CNIPIC/CNPREC	Schutz kritischer Infrastrukturen, Resilienz-Planung
Nationale Unternehmen	Indra	Nationaler Champion für Sicherheit & Verteidigung
	Deimos Space, EM&E, Indra Space, Hispasat	Strategische Beteiligung/Tochtergesellschaften
Private Unternehmen	Telefónica Tech, Microsoft, NTT Data, Innotec, Minsait, Cisco	Technologische Lösungen in Cybersecurity, Cloud, digitale Infrastruktur
International/Kooperationen	EU (rescEU, EU-Solidaritätsfonds), NATO, bilaterale Partner (DE, FR, UK, USA)	Finanzierung, Sicherheitspolitische Kooperation, Cybersecurity-Abkommen

Tabelle 33 Wichtige Akteure des spanischen Marktes für zivile Sicherheit

3.3.2 Untersuchung der Wettbewerbssituation

Der Bereich Katastrophenschutz gewinnt in Spanien zunehmend an Relevanz und entwickelt sich zu einem eigenständigen Wettbewerbsfeld innerhalb der zivilen Sicherheit. Wiederkehrende Extremwetterereignisse – zuletzt die DANA-Fluten in Valencia 2024 mit über 220 Todesopfern – haben die Nachfrage nach moderner Ausrüstung, resilienter Infrastruktur und digitalen Krisenmanagementlösungen deutlich verstärkt.[82] Nationale und regionale Behörden investieren verstärkt in KI-gestützte Frühwarnsysteme, smarte Sensorik zur Risikoüberwachung sowie integrierte Kommunikations- und Einsatzplattformen, die den Austausch zwischen Zivilschutz, Energieversorgern und Einsatzkräften verbessern. Auch der europäische Katastrophenschutzmechanismus bietet internationalen Anbietern Marktzugang, da grenzüberschreitende Kooperationen bei Beschaffung und Technologieentwicklung gefördert werden.

[76] https://www.defensa.gob.es/ume/CONOCENOS/que-es/
[77] http://crick1.subsec.mir.es:11990/es/detail-page/articulo/EL-CNPIC-FUTURO-CNPREC-SERA-EL-EJE-CENTRAL-EN-LA-PROTECCION-Y-RESILIENCIA-DE-LAS-ENTIDADES-CRITICAS/
[78] https://www.defensa.gob.es/ume/CONOCENOS/que-es/
[79] https://maldita.es/malditateexplica/20241111/fondo-solidaridad-union-europea-dana/
[80] https://www.mordorintelligence.com/de/industry-reports/spain-cybersecurity-market
[81] https://www.gtai.de/de/trade/ausschreibungen-projekte/geber/spanische-agentur-internationale-entwicklungszusammenarbeit
[82] https://data.europa.eu/doi/10.2824/5410466

Für ausländische Unternehmen mit innovativen Technologien zur Prävention, Resilienz Steigerung und Notfalllogistik eröffnen sich damit wachsende Chancen, in diesem dynamischen Segment Fuß zu fassen.[83]

Der Markt für zivile Sicherheitslösungen in Spanien ist durch ein dynamisches, aber auch stark fragmentiertes Wettbewerbsumfeld gekennzeichnet. Während große nationale und internationale Unternehmen zentrale Marktsegmente dominieren, herrscht insbesondere im Bereich der Cybersicherheit ein intensiver Wettbewerb unter zahlreichen mittelständischen Anbietern. Die zunehmende Digitalisierung von Geschäftsmodellen, öffentlichen Dienstleistungen und kritischen Infrastrukturen führt zu einer konstant wachsenden Nachfrage nach Sicherheitslösungen – insbesondere im Bereich Cybersecurity. Der spanische Markt für Cybersicherheit wird bis Ende 2024 auf rund 2,27 Mrd. USD geschätzt, mit einer erwarteten Steigerung auf 3,21 Mrd. USD bis 2029 und einer jährlichen Wachstumsrate (CAGR) von 7,16 Prozent.[84]

Eine Schlüsselrolle auf dem Markt spielen etablierte Anbieter wie Telefónica Tech, die gezielt neue Dienste für Betriebstechnologie- (OT) und IoT-Umgebungen eingeführt haben. Diese Dienste basieren auf Partnerschaften mit spezialisierten Technologieunternehmen wie Nozomi Networks und heben sich durch zertifizierte Managed Services für Industrie- und IoT-Kunden ab. Auch Microsoft verfolgt durch seine Kooperation mit Minsait, einem Tochterunternehmen des spanischen Konzerns Indra, eine klare Marktstrategie im Bereich Cloud-Security und Datenschutz. Ein bedeutender Wettbewerbsfaktor ist die Fähigkeit zur Integration gesetzlicher und technischer Anforderungen, insbesondere bei sensiblen Datenverarbeitungen in regulierten Branchen und Behörden. Dies schafft Markteintrittshürden für kleinere Anbieter, aber gleichzeitig auch Nischenchancen für hochspezialisierte Sicherheitslösungen.[85]

Laut einer aktuellen Analyse von Deloitte beklagen 51 Prozent der spanischen Unternehmen, dass sie noch keine spezifische Cybersecurity-Strategie für KI-Systeme implementiert haben, was auf einen erheblichen Nachholbedarf und Marktöffnungspotenzial hinweist. Nur ein Viertel der Unternehmen verwendet gezielte Kontrollmaßnahmen oder führt fokussierte Tests durch, um die Sicherheit ihrer KI-Infrastrukturen zu gewährleisten. Hinzu kommen steigende Anforderungen an die Sicherheit in Lieferketten, die als strategischer Risikofaktor wahrgenommen werden. 68 Prozent der befragten Unternehmen betrachten Third-Party-Risiken als eine der drei größten Herausforderungen der kommenden Jahre. Das zeigt, dass auch Anbieter mit Spezialisierung auf Supply-Chain-Security wachsende Chancen auf dem spanischen Markt haben. Cyberangriffe nehmen sowohl in Häufigkeit als auch in Komplexität zu: 90 Prozent der befragten Organisationen gaben an, dass die Zahl der Angriffe gestiegen oder gleichgeblieben ist. Dennoch verfügen nur 30 Prozent über belastbare Verfahren zur quantitativen Bewertung der durch Angriffe verursachten Schäden – ein Indikator für die Relevanz von Monitoring-, Analyse- und Bewertungsdiensten.[86]

Die staatlichen Institutionen reagieren auf diese Entwicklung mit umfassenden Programmen, um KMU bei der Digitalisierung und der Implementierung von Cybersicherheitsmaßnahmen zu unterstützen. Unter anderem stellt das spanische Wirtschaftsministerium über die Digital Spain Agenda 2025 rund 8,8 Mrd. Euro aus europäischen Wiederaufbau- und Resilienz Fonds bereit, wobei ein erheblicher Anteil in die Verbesserung der Cybersicherheit fließt. Programme wie das „Digital Kit“ fördern gezielt kleine Unternehmen und Selbstständige und treiben so sowohl die Digitalisierung als auch den Sicherheitsbedarf voran. Diese staatlichen Fördermaßnahmen erhöhen nicht nur die Nachfrage, sondern verändern auch die Marktbedingungen: Anbieter, die staatliche Anforderungen erfüllen und Zugang zu Fördermechanismen haben, sichern sich einen Wettbewerbsvorteil. Gleichzeitig intensiviert sich der Wettbewerb in Bereichen wie KI-Sicherheit, Cloud-Services und hybriden IT-Architekturen.[87]

Ein zusätzlicher Aspekt betrifft die internationale Wettbewerbsfähigkeit Spaniens. 2024 verzeichnete Spanien einen Anstieg von Cybervorfällen um 16 Prozent im Vergleich zum Vorjahr, was zu einer Marktausweitung auf insgesamt 2,5 Mrd. Euro führte – ein Zuwachs von über 14 Prozent innerhalb eines Jahres. Die zentralen Bedrohungen sind Malware (über 42.000 Fälle), Phishing (über 21.000 Fälle) und Online-Betrug mit mehr als 38.000 registrierten

[83] https://www.incibe.es/ciudadania/tematicas/inteligencia-artificial
[84] https://www.deloitte.com/es/es/services/risk-advisory/perspectives/estado-ciberseguridad-2024.html
[85] https://www.deloitte.com/es/es/services/risk-advisory/perspectives/estado-ciberseguridad-2024.html
[86] https://www.gtai.de/de/trade/spanien/wirtschaftsumfeld/unternehmen-lassen-sich-cybersicherheit-mehr-kosten-930418
[87] https://www.deloitte.com/es/es/services/risk-advisory/perspectives/estado-ciberseguridad-2024.html

Vorfällen. Besonders betroffen sind kritische Infrastrukturen: Unter dem neuen NIS2-Regime wurden 341 Vorfälle in sicherheitsrelevanten Sektoren gemeldet. [88]

Auch im europäischen Vergleich zeigt sich der Wettbewerbsdruck: Laut einem Bericht der ENISA ist der Finanzsektor europaweit besonders stark betroffen – allein 488 öffentlich bekannte Vorfälle wurden zwischen Januar 2023 und Juni 2024 registriert. Dabei zielen Cyberkriminelle auf Banken, Versicherungen und deren Kunden ab, mit Schäden durch Social Engineering, Datenlecks und Ransomware. Spanien ist ein zentraler Teil dieser Bedrohungslage, was auch internationalen Anbietern Zugangschancen eröffnet – sofern sie über die notwendigen Zertifizierungen und Partnerschaften verfügen.[89]

Insgesamt ist der Markt in starker Bewegung. Große Unternehmen sichern sich durch Technologiepartnerschaften und staatliche Unterstützung ihre Position, während spezialisierte Anbieter durch Innovation und Nischenfokus punkten können. Für deutsche Unternehmen mit fortgeschrittener Technologie, zuverlässiger Compliance und internationaler Erfahrung ergeben sich dadurch gute Chancen für einen Markteintritt – insbesondere in den Segmenten Cloud-Sicherheit, KI-gestützte Cyberabwehr und kritische Infrastruktursicherheit.[90]

3.3.3 Bestehende Bestimmungen und Lizenzierung

Der rechtliche Rahmen für sicherheitsrelevante Bereiche in Spanien ist stark durch die Dezentralisierung des politischen Systems geprägt. Sowohl der Zentralstaat als auch die Autonomen Gemeinschaften und Gemeinden verfügen über eigene Regelungskompetenzen, was zu komplexen, teils fragmentierten Genehmigungs- und Verwaltungsprozessen führt. Diese Vielschichtigkeit wirkt sich auf Vorhaben im Bereich der Infrastruktur, Technologieentwicklung und sicherheitsrelevanten Dienstleistungen aus – und betrifft somit auch ausländische Anbieter.[91]

Ein Beispiel für regulatorische Fragmentierung zeigt sich im Bereich kritischer Infrastrukturen. Die Verantwortung für Schutzmaßnahmen ist auf verschiedene Ebenen verteilt: nationale Behörden, autonome Regionen sowie private Betreiber tragen jeweils spezifische Aufgaben.[92] Die gesetzlichen Grundlagen umfassen nationale Schutzpläne (National Protection Plan), sektorspezifische Maßnahmen, Krisenreaktionsmechanismen sowie Notfallprotokolle für den Schutz essenzieller Dienstleistungen wie Energie, Wasser, Kommunikation oder Transport.[93] Diese Pläne werden regelmäßig angepasst und unterliegen strikten Vorschriften, die im spanischen Gesetzblatt (BOE) oder im Handelsregister (BORME) veröffentlicht werden.[94]

Für Unternehmen, die sicherheitsrelevante Projekte umsetzen möchten, ist ein Verständnis dieser komplexen rechtlichen und administrativen Landschaft unerlässlich. Dies gilt insbesondere für Anbieter von Systemen für den Schutz kritischer Infrastrukturen, die in einem gesetzlich regulierten Rahmen mit klar definierten Zuständigkeiten operieren müssen. Der Zugang zu Ausschreibungen oder der Erhalt von Lizenzen hängt daher nicht nur von der technischen Qualifikation, sondern auch von der Einhaltung spezifischer gesetzlicher Anforderungen auf verschiedenen Verwaltungsebenen ab. Beispielsweise benötigen Anbieter von Videoüberwachungssystemen in öffentlichen Einrichtungen neben einer technischen Zulassung oft auch eine gesonderte Datenschutzfreigabe durch regionale Behörden – insbesondere, wenn biometrische oder personenbezogene Daten verarbeitet werden sollen.[95] Auch im Bereich der Informationssicherheit gelten definierte Standards und internationale Normen, etwa in Anlehnung an ISO-Richtlinien. Informationssicherheit umfasst in Spanien die drei zentralen Prinzipien Vertraulichkeit, Integrität und Verfügbarkeit – sowohl für staatliche als auch private Akteure. Besonders in regulierten Branchen, etwa im Finanz- oder Infrastruktursektor, ist die Einhaltung entsprechender Sicherheitsstandards nicht nur Best Practice, sondern gesetzlich verankert. Unternehmen müssen daher interne Informationssicherheitsmanagementsysteme (ISMS) einführen, um rechtlichen und wirtschaftlichen Risiken vorzubeugen.[96]

[88] https://civil-protection-humanitarian-aid.ec.europa.eu/news-stories/stories/flash-floods-spain-joining-forces-rapid-recovery_en
[89] https://elpais.com/economia/formacion/2024-11-29/se-buscan-expertos-en-ciberseguridad.html
[90] https://www.deloitte.com/es/es/services/risk-advisory/perspectives/estado-ciberseguridad-2024.html
[91] https://www.gtai.de/de/trade/spanien-wirtschaft/wirtschaftsstandortt
[92] https://4elitech.com/seguridad-en-infraestructuras-criticas-en-espana/
[93] https://www.itgovernance.eu/es-es/information-security-es
[94] https://4elitech.com/seguridad-en-infraestructuras-criticas-en-espana/
[95] https://4elitech.com/seguridad-en-infraestructuras-criticas-en-espana/
[96] https://www.gtai.de/de/trade/ausschreibungen-projekte/geber/spanische-agentur-internationale-entwicklungszusammenarbeit

Für Anbieter aus dem Ausland, einschließlich deutscher Unternehmen, bestehen bislang keine systematischen Einschränkungen für Direktinvestitionen im Sicherheitsbereich, solange sie nicht aus dem Nicht-EU-Ausland stammen oder strategische Sektoren betreffen. Allerdings kann es je nach Branche und geographischer Lage spezifische Genehmigungserfordernisse geben – insbesondere in autonomen Regionen mit politisch sensibler Interessenlage, wie Katalonien oder dem Baskenland.[97] Zusätzlich zu den staatlichen Vorschriften haben auch internationale Vorgaben wie das Sendai-Rahmenwerk für Katastrophenvorsorge (2015–2030) sowie die EU-Hochwasserrichtlinie (2007) Einfluss auf nationale Planungs- und Lizenzierungsstrukturen. Diese Programme wurden in spanische Gesetzgebung integriert und beeinflussen heute z. B. Anforderungen an Frühwarnsysteme, Risikobewertungen und kommunale Gefahrenabwehrpläne.[98]

Für Projekte im Bereich der zivilen Sicherheit gilt es deshalb, regulatorische Anforderungen nicht nur auf staatlicher Ebene, sondern auch im regionalen und kommunalen Kontext zu prüfen. Entscheidend ist dabei nicht zuletzt die Fähigkeit zur Zusammenarbeit mit lokalen Behörden und die Bereitschaft, sich in bestehende Strukturen und rechtliche Verfahren einzuarbeiten.[99]

3.3.4 Hinweise zu Finanzierungsmöglichkeiten, staatliche Anreize und Angebote

Spanien bietet deutschen Unternehmen eine Vielzahl an staatlichen und europäischen Finanzierungsinstrumenten zur Förderung von Investitionen, Digitalisierung und Sicherheitsprojekten. Dabei verfolgt die spanische Regierung explizit das Ziel, durch gezielte finanzielle Anreize strukturschwache Regionen zu stärken und Investitionen in strategisch relevante Sektoren zu lenken. Ein zentrales Element ist die staatliche Investitionsförderung in unterentwickelten Gebieten: Kleine Unternehmen können dort Fördermittel von bis zu 70 Prozent erhalten – abhängig von der Unternehmensgröße und dem Standort des Projekts. Besonders hervorgehoben wird das Sonderförderregime Zona Especial Canaria (ZEC), das durch steuerliche Vergünstigungen, Import-/Exporterleichterungen und vereinfachte Verwaltungsverfahren Investitionen auf den Kanarischen Inseln bis mindestens 2027 fördern soll. Eine Verlängerung über dieses Jahr hinaus wird derzeit in Abstimmung mit der EU geprüft. Zusätzlich profitiert Spanien in erheblichem Umfang von den europäischen Wiederaufbau- und Kohäsionsfonds. Das Förderpaket Next Generation EU fließt unter anderem in Programme zur Digitalisierung, Nachhaltigkeit und technologischen Transformation – allesamt Bereiche, in denen sicherheitsbezogene Lösungen eine Rolle spielen. Die nationale Förderagentur ICEX sowie die Förderinstitutionen der Autonomen Gemeinschaften bewerben aktiv ausländische Direktinvestitionen, insbesondere im Technologiesektor. Regionen wie das Baskenland und Navarra verfügen dabei über besonders weitreichende steuerliche Autonomien und damit über eigene Förderstrukturen. Auch auf kommunaler Ebene entstehen gezielte Anreize. So hat die Stadt Barcelona unter dem neuen Oberbürgermeister Jaume Collboni im Oktober 2023 Steuererleichterungen für Start-ups, Innovationszentren und arbeitsplatzintensive Unternehmen eingeführt – ein deutlicher Richtungswechsel im Vergleich zur wirtschaftspolitisch skeptischeren Haltung der Vorgängerregierung[100].

Die EU bietet zusätzlich finanzielle Soforthilfe in Krisensituationen. Der Europäische Solidaritätsfonds (EUSF) stellt Mittel bereit, um Schäden durch Naturkatastrophen oder Gesundheitskrisen zu kompensieren. Spanien hat bereits sieben Mal auf diesen Fonds zurückgegriffen – zuletzt nach der DANA-Katastrophe 2024 – mit insgesamt über 153 Mio. Euro an Hilfen. Der Großteil dieser Mittel wurde für Hochwasserschäden verwendet, was die Relevanz für sicherheitsbezogene Infrastruktur- und Wiederaufbauprojekte unterstreicht.[101] Neben akuter Hilfe stellt die EU auch Mittel zur Katastrophenprävention bereit. Spanien nutzt Förderprogramme wie rescEU, EFRE, LIFE oder Horizont Europa, um in Frühwarnsysteme, resilientere Infrastruktur und Waldbrand- wie Hochwasserschutz zu investieren. Damit werden Prävention, Resilienz und digitale Innovation gezielt gestärkt.“ [102]

Ein weiterer Fokus der Finanzierung liegt im Bereich Cybersicherheit. Die spanische Regierung investiert im Rahmen ihres digitalen Aufbau- und Resilienzplans rund 4 Mrd. Euro in Programme zur Internetsicherheit, 5G und Konnektivität. Diese sogenannte Komponente 15 bietet auch deutschen Anbietern von Cyberlösungen Chancen im Bereich öffentlicher und privatwirtschaftlicher Digitalisierungsprojekte. Für kleinere Unternehmen und Selbstständige wurde zudem das Programm „Kit Digital“ geschaffen. Dieses umfasst rund 3 Mrd. Euro und soll die Digitalisierung von

[97] https://www.gtai.de/de/trade/spanien-wirtschaft/wirtschaftsstandort
[98] https://invescon.es/proteccion-de-infraestructuras-criticas-en-espana/
[99] https://4elitech.com/seguridad-en-infraestructuras-criticas-en-espana/
[100] https://maldita.es/malditateexplica/20241111/fondo-solidaridad-union-europea-dana/
[101] https://maldita.es/malditateexplica/20241111/fondo-solidaridad-union-europea-dana/
[102] https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes_de

rund 1,1 Mio. Kleinstunternehmen und über 1,6 Mio. Solo-Selbstständigen fördern – auch mit Blick auf deren IT-Sicherheitsstandards. Solche Programme schaffen einen stark wachsenden Markt für standardisierte wie auch spezialisierte Sicherheitslösungen.[103] Wie relevant diese Themen geworden sind, zeigt eine Umfrage von Deloitte: 98 Prozent der Unternehmen haben ihre IT-Sicherheitsbudgets erhöht oder beibehalten – lediglich 2 Prozent haben sie gesenkt. Das signalisiert nicht nur einen hohen Reifegrad in der Unternehmenswahrnehmung, sondern auch ein dauerhaftes Investitionspotenzial für Anbieter entsprechender Technologien.[104]

Auch im Bereich der öffentlichen Entwicklungszusammenarbeit entstehen Geschäftschancen für ausländische Firmen. Die AECID (spanische Agentur für internationale Entwicklungszusammenarbeit) verwaltet mehrere Fonds – darunter FONPRODE und der Wasserfonds FCAS – aus denen Projekte im In- und Ausland finanziert werden. Über diese Fonds werden regelmäßig Ausschreibungen für Bau-, Liefer- und Beratungsleistungen veröffentlicht, an denen sich auch deutsche Anbieter beteiligen können. Besonders relevant sind dabei Projekte im Kontext humanitärer Hilfe, technischer Infrastruktur und IT-Dienstleistungen.[105]

[103] https://www.gtai.de/de/trade/spanien-wirtschaft/wirtschaftsstandort
[104] https://www.gtai.de/de/trade/spanien/wirtschaftsumfeld/unternehmen-lassen-sich-cybersicherheit-mehr-kosten-930418
[105] https://www.deloitte.com/es/es/services/risk-advisory/perspectives/estado-ciberseguridad-2024.html

3.4 SWOT-Analyse

SWOT Spanien

Stärken (Strengths)	Chancen (Opportunities)
• Viertgrößter Markt der EU • Hochentwickelte Infrastruktur • Breites Zuliefernetz • Exportstarke Spitzenunternehmen • Internationalisierung über Handel, Investitionen, Konzessionen	• Bis zu 164 Mrd. Euro EU-Mittel für Investitionen • Enormes Potenzial erneuerbarer Energien • Produktion von günstigem grünem Wasserstoff • Technikbedarf innovativer Unternehmen • Brücke nach Lateinamerika und Portugal
Schwächen (Weaknesses)	**Risiken (Threats)**
• Hohe Staatsverschuldung • Viele wenig produktive Kleinstunternehmen • Höchste Arbeitslosigkeit in der EU • Vorschriften auf drei Verwaltungsebenen • Teils schwache Englischkenntnisse	• Instabile politische Mehrheitsverhältnisse • Ausgeprägte Links-Rechts-Spaltung • Demografischer Druck auf das Rentensystem • Wasserstress in weiten Teilen des Landes • Folgen des steigenden Zinsniveaus

Tabelle 44 SWOT Analyse Spanien

SWOT-Sicherheitssektor Spanien

Stärken (Strengths)	Chancen (Opportunities)
• Staatliche Strukturförderung für Sicherheitstechnologien, besonders in unterentwickelten Regionen • Enge Verflechtung mit der EU und Zugriff auf EU-Fonds wie Next Generation EU, EUSF, Resilienz- und Kohäsionsprogramme • Ausgebaute nationale Sicherheitsinstitutionen: UME, CNPIC/CNPREC, koordinierte Schutzpläne für kritische Infrastrukturen • Technologische Vorreiterprojekte in KI-gestütztem Katastrophenschutz und Cybersicherheit • Strategische Unternehmen mit staatlicher Beteiligung, z. B. Indra – aktiv in Raumfahrt, Cybersicherheit und Kommunikation • Hoher Digitalisierungsgrad im öffentlichen Bereich, z. B. über 8,8 Mrd. EUR Investitionen in Agenda España Digital 2025	• Wachsender Markt für zivile und digitale Sicherheitslösungen, v. a. durch zunehmende Bedrohungslagen Große Investitionsvolumina in KI, Satellitenkommunikation und Frühwarnsysteme, • z. B. über „SpainSat NG“ oder „Komponente 15“ • Verfügbarkeit öffentlicher Mittel und Ausschreibungen, z. B. AECID, FONPRODE, FCAS • Smart City Projekte & Innovationsräume in Großstädten, z. B. Barcelona, Valencia Starkes öffentliches Sicherheitsbewusstsein – sowohl in Bevölkerung als auch Verwaltung
Schwächen (Weaknesses)	**Risiken (Threats)**
• Komplexe Verwaltungsstruktur mit teils fragmentierter Zuständigkeit (zentral, regional, kommunal) • Langer Genehmigungsprozess, insbesondere bei Sicherheitsprojekten mit regionaler Relevanz • Fachkräftemangel, v. a. im Bereich Cybersicherheit, IT und KI • Geringe IT-Resilienz bei KMU trotz Fördermaßnahmen wie „Kit Digital“ – viele haben keine umfassende Sicherheitsstrategie • Unzureichende Umsetzung europäischer Normen auf lokaler Ebene, z. B. NIS2, CER	• Instabile politische Mehrheitsverhältnisse – Einfluss regionaler Parteien, z. B. in Katalonien oder dem Baskenland • Cyberbedrohungen mit steigender Intensität – Spanien weltweit unter den am häufigsten angegriffenen Ländern • Abhängigkeit von großen Tech-Anbietern im Sicherheitsbereich (z. B. Microsoft, Cisco) → Gefahr von technologischer Abhängigkeit • Regionale Disparitäten bei Förderstrukturen, Verwaltungskapazitäten und Projektumsetzung • Steigende Kosten und Personalknappheit bei sicherheitsrelevanten Fachkräften

Tabelle 55 SWOT Analyse Sicherheitsmarkt Spanien

4 Kontaktadressen

Institution	Kurzbeschreibung
Centro de Operaciones de Ciberseguridad (COCS)	Das Centro de Operaciones de Ciberseguridad (COCS) in Spanien ist eine zentrale Einrichtung zur Prävention, Erkennung und Reaktion auf Cyberangriffe für die staatliche Verwaltung und öffentliche Einrichtungen. Es bietet umfassende Sicherheitsdienste, darunter Überwachung, Forensik, Frühwarnsysteme und Unterstützung bei der Krisenbewältigung, um die digitale Sicherheit der öffentlichen Verwaltung zu stärken.
CNPIC	Das Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) ist eine Behörde des spanischen Innenministeriums, die für die Koordination und Überwachung des Schutzes kritischer Infrastrukturen im Land zuständig ist. Es entwickelt und aktualisiert den Nationalen Schutzplan, bewertet die Kritikalität von Infrastrukturen und koordiniert Maßnahmen zur Sicherstellung der Funktionsfähigkeit von wichtigen Diensten wie Energie, Wasser und Telekommunikation.
Departamento de Seguridad Nacional (DSN)	Das Departamento de Seguridad Nacional (DSN) ist das Beratungsorgan des spanischen Ministerpräsidenten für nationale Sicherheit. Es koordiniert Krisenmanagement, überwacht Risiken und Bedrohungen und sorgt für den reibungslosen Betrieb des Krisenmanagementzentrums. Das DSN unterstützt auch den Sicherheitsrat und vertritt Spanien in internationalen Sicherheitsfragen.
INCIBE-CERT	INCIBE-CERT ist das nationale spanische Reaktionszentrum für Cybervorfälle, das Unternehmen und Bürger im Bereich Cybersicherheit unterstützt. Es arbeitet unter dem Nationalen Cybersecurity-Institut (INCIBE) und koordiniert sich national und international, um Cyberkriminalität effektiv zu bekämpfen.
Indra	Indra ist ein weltweit führendes spanisches Technologie- und Beratungsunternehmen mit Schwerpunkt auf Transport-, Luftverkehrs- und Verteidigungslösungen. Das Unternehmen bietet zudem digitale Transformation und IT-Dienstleistungen an und ist in über 140 Ländern mit mehr als 60.000 Mitarbeitenden tätig.
Ministerium für Digitale Transformation und öffentliche Verwaltung	Das Ministerium für Digitale Transformation und öffentliche Verwaltung in Spanien ist verantwortlich für die Umsetzung der digitalen Transformation, die Förderung von künstlicher Intelligenz und die Modernisierung der öffentlichen Verwaltung. Es setzt Regierungsprogramme um, wie etwa Maßnahmen gegen Telefonbetrug, und unterstützt die Digitalisierung von Wirtschaft und Verwaltung.
Spanische Innenministerium	Das spanische Innenministerium (Ministerio del Interior) ist für die Sicherheit der Bürger zuständig. Es leitet und koordiniert die Polizei und andere Sicherheitskräfte, schützt Grundrechte und verwaltet das Asyl- und Ausländerwesen. Zudem trägt es Verantwortung für den Schutz der Gesellschaft, den Strafvollzug, den Katastrophenschutz, die Verkehrssicherheit und die Durchführung von Wahlen.
Unidad Militar de Emergencias (UME)	Die Unidad Militar de Emergencias (UME) ist eine Spezialeinheit der spanischen Streitkräfte, die 2005 gegründet wurde, um bei Katastrophen und Notfällen schnell zu reagieren. Sie ist in ganz Spanien mit sieben Standorten vertreten und spezialisiert auf Einsätze bei Waldbränden, Überschwemmungen, Chemieunfällen und anderen Krisen. Die UME arbeitet eng mit zivilen Behörden zusammen und kann auch international bei humanitären Einsätzen aktiv sein.

Tabelle 66 Wichtige Entscheidungsträger in der spanischen Wirtschaft

Institution	Kurzbeschreibung
AHK Spanien	Die Deutsche Handelskammer für Spanien (AHK Spanien) ist die zentrale Anlaufstelle für die Förderung und Beratung deutsch-spanischer Wirtschaftsbeziehungen. Sie unterstützt Unternehmen mit einem breiten Dienstleistungsangebot, darunter Markteintrittsberatung, Vermittlung von Geschäftskontakten und Personalservices.
CEPYME	Die Confederación Española de la Pequeña y Mediana Empresa (CEPYME) ist der wichtigste spanische Verband zur Vertretung und Förderung der Interessen kleiner und mittlerer Unternehmen (KMU) sowie selbstständiger Unternehmer. CEPYME setzt sich für die Interessen der KMU auf nationaler und europäischer Ebene ein, bietet Beratung, Information und Dienstleistungen an und vertritt die Unternehmen zudem in verschiedenen Gremien.

Deutsche Botschaft Madrid	Die Deutsche Botschaft Madrid ist die offizielle diplomatische Vertretung Deutschlands in Spanien und auch für Andorra zuständig. Sie pflegt die deutsch-spanischen Beziehungen, vertritt die Interessen Deutschlands gegenüber der spanischen Regierung und bietet umfassende konsularische Dienstleistungen für deutsche Staatsangehörige an.
EUGO España	Das Portal EUGO ist die zentrale Online-Anlaufstelle („Ventanilla Única“) für Dienstleister aus der EU, um alle notwendigen Verwaltungsverfahren und Anträge für die Aufnahme und Ausübung einer Tätigkeit in Spanien digital abzuwickeln. Es richtet sich sowohl an Gründerinnen und Gründer als auch an etablierte Unternehmen und stellt umfassende Informationen zu rechtlichen Anforderungen, Genehmigungen und Kontaktstellen bereit.
Germany Trade & Invest	Germany Trade & Invest (GTAI) ist die Außenwirtschaftsagentur der Bundesrepublik Deutschland. Mit 60 Standorten weltweit und dem Partnernetzwerk unterstützt Germany Trade & Invest deutsche Unternehmen bei ihrem Weg ins Ausland, wirbt für den Standort Deutschland und begleitet ausländische Unternehmen bei der Ansiedlung in Deutschland.

Tabelle 7 Wichtige Partner für deutsche Unternehmen

Institution	Kurzbeschreibung
AECID	Die AECID (Agencia Española de Cooperación Internacional para el Desarrollo) ist die spanische Agentur für internationale Entwicklungszusammenarbeit und dem Außenministerium unterstellt. Sie entwirft, implementiert und verwaltet Projekte zur Armutsbekämpfung, nachhaltigen Entwicklung und humanitären Hilfe in über 30 Ländern.
ICEX-Invest	ICEX-Invest in Spain unterstützt internationale Investoren dabei, in Spanien zu investieren, indem es Informationen, Beratung und Aftercare-Services anbietet. Das Unternehmen fördert Projekte, erleichtert den Markteintritt und betreut Investoren auch nach der Ansiedlung, mit besonderem Fokus auf innovative und audiovisuelle Sektoren.
Zona Especial Canaria (ZEC)	Die Zona Especial Canaria (ZEC) ist eine Sonderwirtschaftszone auf den Kanarischen Inseln, die Unternehmen attraktive steuerliche Vorteile bietet, insbesondere einen reduzierten Körperschaftssteuersatz von nur 4 %. Ziel ist es, die wirtschaftliche Entwicklung und Diversifizierung des Archipels zu fördern, wobei Unternehmen u.a. bestimmte Investitions- und Arbeitsplatzauflagen erfüllen müssen.

Tabelle 8 Wichtige Finanzierungsinstitutionen in Spanien

Messe	Kurzbeschreibung	Datum
Security Essen	Die Security Essen ist eine führende Fachmesse für zivile Sicherheit, die als zentrale Plattform für Innovationen, aktuelle Branchenthemen und persönlichen Austausch dient. Ab 2024 rückten die Schwerpunkte Bevölkerungsschutz und zivile Verteidigung verstärkt in den Fokus, im Kontext politischer, gesellschaftlicher und ökologischer Entwicklungen. Die Messe adressiert aktuelle Themen wie Cybersicherheit, Zutrittslösungen und Schutz sensibler Bereiche.	22.09.-25.09.2026
it-sa365	Die it-sa 365 ist die ganzjährige digitale Dialogplattform der IT-Sicherheitsbranche. Hier vernetzen sich IT-Sicherheitsverantwortliche und Anbieter, tauschen sich über Cybersicherheit, Lösungen und aktuelle Branchentrends aus und profitieren von digitalen Vorträgen, Networking-Möglichkeiten und Fachwissen. Sie ergänzt die jährlich stattfindende it-sa Expo&Congress in Nürnberg als digitalen Marktplatz und Wissens-Hub der Branche.	Ganzjährig
Polizeitag Mainz	Der Polizeitag Mainz widmet sich der Stärkung der Krisenresilienz von Sicherheitsbehörden im Kontext von Katastrophen wie der Flut 2021 im Landkreis Ahrweiler. Im Mittelpunkt stehen die vier Dimensionen Prozesse, Organisation und Mensch, Recht sowie Technik – mit dem Ziel, Strukturen und Führung der Polizei so weiterzuentwickeln, dass künftige Krisen besser bewältigt werden können.	27.08.2025
Digitaler Katastrophenschutz Kongress	Der Digitale Katastrophenschutz-Kongress 2025 befasst sich mit den aktuellen und künftigen Herausforderungen der nichtpolizeilichen Gefahrenabwehr in Deutschland. Im Fokus stehen Themen wie die Anpassung an den demografischen Wandel, internationale Spannungen und die Auswirkungen des Klimawandels. Diskutiert werden sowohl bewährte als auch innovative Ansätze, um den Bevölkerungsschutz effektiv aufzustellen und neue technische Lösungen einzubinden.	09.09.-10.09.2025
ISD – Internet Security Days	Die Internet Security Days (ISD) 2025 richtet sich an IT-Sicherheits-Expert:innen, Sicherheitsverantwortliche und Unternehmen und bietet ein umfangreiches Programm mit den Schwerpunkten Cyberresilienz, sichere E-Mail-Kommunikation und sichere digitale Infrastrukturen. Es gibt Workshops zu E-Mail-Sicherheit für Unternehmen, gefolgt von der Internet Security Night im Stadionfenster als Networking-Event. Außerdem umfasst das Programm hochkarätige Keynotes, Impulsvorträge und Paneldiskussionen zu aktuellen IT-Sicherheitsthemen.	15.09.-16.09.2025
ko:mon	Der ko:mon Kongress ist eine Fachveranstaltung für die Leitstand-, Kontrollraum- und Monitoringbranche, bei der Experten, Praktiker und Anwender aus Industrie, Verwaltung und Dienstleistung zusammenkommen. Im Fokus stehen der Austausch von Know-how, innovative Technologien sowie spannende Fachvorträge, Workshops und Experten-Dialoge rund um Überwachungs- und Kontrolltechnik.	16.09.-18.09.2025
SicherheitsExpo Berlin	Die SicherheitsExpo Berlin ist eine Fachmesse für Sicherheitstechnik, die Lösungen für den Schutz kritischer Infrastrukturen, IT-Sicherheit sowie mechanische und bauliche Sicherheit präsentiert. Die Messe richtet sich an Unternehmen, öffentliche Einrichtungen und Sicherheitsverantwortliche und bietet neben den Ausstellungen auch eine kostenfreie Konferenz mit Fachvorträgen und Workshops.	17.09.-18.09.2025
RETTER	Die RETTER Messe ist Österreichs Leitmesse für Einsatzorganisationen und Sicherheitsbehörden. Sie präsentiert innovative Technologien und Lösungen aus Feuerwehr, Rettung, Polizei und Katastrophenschutz und fördert den Austausch zwischen Wissenschaft, Praxis und Industrie.	18.09.-20.09.2025
rescueDays 2025	Die rescueDAYS sind die weltweit größte Ausbildungsveranstaltung für technische Hilfeleistung mit Trainings zu verschiedenen Unfallrettungsszenarien. Zusätzlich gibt es Spezialprogramme und Seminare, die auch online als E-Learning mit Zertifikat verfügbar sind.	18.09.-21.09.2025
ZFBS-Kongress	Der ZFBS Kongress 2025 in Kempten fokussiert sich auf Führung im Bevölkerungsschutz und bietet Fachvorträge, Workshops und Diskussionen zu ziviler Verteidigung, Krisenmanagement und Resilienz	24.09.-25.09.2025

	kritischer Infrastrukturen.	
Rethink! Cloud Security	Der Rethink! Cloud Security Kongress 2025 in Berlin bringt IT- und Cloud-Sicherheits-Experten zusammen, um wichtige Themen wie Data Loss Prevention, Multi-Cloud-Sicherheit, Identity Management und Compliance zu diskutieren. Ziel ist es, Cloud-Umgebungen sicherer und widerstandsfähiger zu machen.	24.09.-25.09.2025
SCALTEL Techupdate 2025	Das SCALTEL TechUpdate 2025 ist ein IT-Event für Entscheider und Experten mit Fokus auf Künstliche Intelligenz, IT-Sicherheit und Datensouveränität. Es bietet hochkarätige Keynotes, Breakout-Sessions, eine Hausmesse mit führenden Herstellern sowie Networking. Zum Abschluss gibt es ein besonderes Oktoberfest-Event auf dem Firmengelände.	26.09.2025
VSW-Sicherheitstag	Der VSW-Sicherheitstag ist eine eintägige Veranstaltung für Fach- und Führungskräfte aus Wirtschaft, Behörden und Sicherheitsorganisationen, die sich mit aktuellen Bedrohungen und Sicherheitsstrategien beschäftigen. Themenschwerpunkte sind Cybersecurity, Künstliche Intelligenz, hybride Bedrohungen, Drohnen sowie geopolitische Entwicklungen. Die Veranstaltung bietet Fachvorträge, Austausch und Networking in kompakter Form, um praxisnah Lösungen und Best Practices zu vermitteln.	29.09.2025
Information Security Network DACH	Das DACH Information Security Network ist ein exklusives Treffen für CISOs großer Unternehmen aus der DACH-Region, bei dem aktuelle Sicherheitsherausforderungen, Best Practices und kollaborative Lösungen für den Schutz gegen Cyberangriffe diskutiert werden. Schwerpunkt liegt auf Bedrohungen wie Supply-Chain-Schwachstellen und Ransomware sowie auf der Verbesserung von Sicherheitsstrategien und Personalentwicklung in der IT-Security.	22.09-23.09.2025
FLORIAN	Die FLORIAN ist eine Fachmesse für Feuerwehr, Zivil- und Katastrophenschutz, die innovative Technologien und Konzepte aus den Bereichen Rettungswesen, Feuerwehr und Bevölkerungsschutz präsentiert. Die Messe bietet Fachvorträge, Weiterbildungen und Live-Demonstrationen zu aktuellen Themen wie Gefahrstoffmanagement, Atemschutz, Waldbrandbekämpfung und technische Hilfeleistung. Sie ist eine wichtige Plattform für Austausch und Networking innerhalb der Branche.	09.10.-11.10.2025
German Itelligence Community Conference	Die German Intelligence Community Conference (GICC) 2025 bringt Fachleute aus Wirtschaft, Behörden und Sicherheitsdiensten zusammen, um aktuelle Intelligence-Themen zu diskutieren und Wissen auszutauschen. Vorab gibt es ein Training zu Strukturierten Analysetechniken für Open Source Intelligence. Die Teilnahme erfolgt auf Einladung mit verschiedenen Ticketoptionen, darunter vergünstigte Tarife für den öffentlichen Dienst sowie Studierende und Rentner.	16.10.-17.10.2025
IT-Sicherheitstag NRW	Der IT-Sicherheitstag NRW 2025 richtet sich besonders an kleine und mittlere Unternehmen. Die Veranstaltung bietet Vorträge, Fachforen und eine Ausstellung zu aktuellen Bedrohungen, IT-Sicherheitsmaßnahmen und praxisnahen Tipps. Ziel ist es, Unternehmen konkrete Hilfestellungen und einen Austausch sowie Netzwerke zu ermöglichen.	03.12.2025
Risk Management Kongress	Der Risk Management Congress 2026 ist eine der führenden Fachkonferenzen im deutschsprachigen Raum zu Risikomanagement, Rating und Krisenmanagement. Es bietet Experten sowie Entscheidern umfassendes Wissen in Theorie und Praxis.	18.05.-19.05.2026
Datenschutzkongress	Der Euroforum Datenschutzkongress 2026 ist ein zentraler Treffpunkt für Datenschutzverantwortliche, IT-Sicherheitsexperten, Juristen und Entscheider aus Wirtschaft und Verwaltung. Themenschwerpunkte sind unter anderem Datenschutz in Zusammenhang mit KI, regulatorische Anforderungen, Datenethik und europäisches Datenrecht.	19.05.-21.05.2026

Tabelle 9 Relevante Messen im Bereich der zivilen Sicherheit und Cybersicherheit

Quellenverzeichnis

4elitech. *Seguridad en infraestructuras críticas en España.*
https://4elitech.com/seguridad-en-infraestructuras-criticas-en-espana/

Auswärtiges Amt. *Spanien: bilaterale Beziehungen.*
https://www.auswaertiges-amt.de/de/service/laender/spanien-node/bilateral-210216

Comisión Europea. *EU funding programmes.*
https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes_de

Consejo de Ministros (Gobierno de España).
https://www.lamoncloa.gob.es/lang/en/gobierno/councilministers/paginas/2022/20221031_council.aspx

Crick1. *El CNPIC futuro CNPREC será el eje central en la protección y resiliencia de las entidades críticas.*
http://crick1.subsec.mir.es:11990/es/detail-page/articulo/EL-CNPIC-FUTURO-CNPREC-SERA-EL-EJE-CENTRAL-EN-LA-PROTECCION-Y-RESILIENCIA-DE-LAS-ENTIDADES-CRITICAS/

Data Commons. *Spain – Fertility rate (Female).*
https://datacommons.org/place/country/ESP?utm_medium=explore&mprop=fertilityRate&popt=Person&cpv=gender,Female&hl=en

Data Europa. *Cybersecurity Report.*
https://data.europa.eu/doi/10.2824/5410466

Defensa.gob.es. *Unidad Militar de Emergencias (UME).*
https://www.defensa.gob.es/ume/CONOCENOS/que-es/

Deloitte. *Estado de la Ciberseguridad 2024.*
https://www.deloitte.com/es/es/services/risk-advisory/perspectives/estado-ciberseguridad-2024.html

Democrata.es. *Inteligencia Artificial para la Protección Civil.*
https://www.democrata.es/analisis-y-opinion/inteligencia-artificial-para-la-proteccion-civil/

DSW. *Länderdatenbank.*
https://www.dsw.org/laenderdatenbank/?utm

El País. *Se buscan expertos en ciberseguridad.*
https://elpais.com/economia/formacion/2024-11-29/se-buscan-expertos-en-ciberseguridad.html

EU Civil Protection & Humanitarian Aid. *Flash floods Spain – joining forces for rapid recovery.*
https://civil-protection-humanitarian-aid.ec.europa.eu/news-stories/stories/flash-floods-spain-joining-forces-rapid-recovery_en

Experteninterview LP

Fuchsbriefe. *Spanien investiert in Cybersecurity.*
https://www.fuchsbriefe.de/spanien-investiert-in-cybersecurity

GNDR. *Spain floods – Early warning, action, coordination and localisation.*
https://www.gndr.org/2024-spain-floods-early-warning-action-coordination-and-localisation/

GTAI. *Arbeitsmarkt in Spanien.*
https://www.gtai.de/de/trade/spanien-wirtschaft/arbeitsmarkt

GTAI. *Spanien investiert kräftig in die Verteidigung.*
https://www.gtai.de/de/trade/spanien/branchen/spanien-investiert-kraeftig-in-die-verteidigung-1894360

GTAI. *Spanische Agentur für internationale Entwicklungszusammenarbeit.*
https://www.gtai.de/de/trade/ausschreibungen-projekte/geber/spanische-agentur-internationale-entwicklungszusammenarbeit

GTAI. *Unternehmen lassen sich Cybersicherheit mehr kosten.*
https://www.gtai.de/de/trade/spanien/wirtschaftsumfeld/unternehmen-lassen-sich-cybersicherheit-mehr-kosten-930418

GTAI. *Wirtschaftsstandort Spanien.*
https://www.gtai.de/de/trade/spanien-wirtschaft/wirtschaftsstandort

Grupo Cibernos. *Ciberseguridad en España.*
https://www.grupocibernos.com/blog/ciberseguridad-en-españa

INCIBE. *Artificial Intelligence – Ciudadanía.*
https://www.incibe.es/ciudadania/tematicas/inteligencia-artificial

INCIBE. *Network of Excellence Cybersecurity RDI.*
https://www.incibe.es/en/incibe/corporate-information/who-we-work-with/network-excellence-cybersecurity-rdi?utm

Invescon. *Protección de infraestructuras críticas en España.*
https://invescon.es/proteccion-de-infraestructuras-criticas-en-espana/

IT Governance EU. *Information Security.*
https://www.itgovernance.eu/es-es/information-security-es

La Ecuación Digital. *Cinco aplicaciones de la IA en la prevención y mitigación de desastres naturales.*
https://www.laecuacion digital.com/tecnologias/inteligencia-artificial/cinco-aplicaciones-de-la-ia-en-la-prevencion-y-mitigacion-de-desastres-naturales/

La Moncloa. *Plan de Acción Conjunto Hispano-Alemán (2022).*
https://www.lamoncloa.gob.es/presidente/actividades/Documents/2022/051022_Anexo-Plan-Accion-conjunto-hispano-aleman.pdf?utm

Maldita.es. *Fondo de Solidaridad de la Unión Europea (DANA).*
https://maldita.es/malditateexplica/20241111/fondo-solidaridad-union-europea-dana/

Mordor Intelligence. *Spain Cybersecurity Market.*
https://www.mordorintelligence.com/de/industry-reports/spain-cybersecurity-market

Piñeiro Ramírez, José Alberto. *Planning and management of resources against disasters in Spain.*

RENIC. *About us.*
https://renic.es/en/about-us/?utm

ResearchGate. *AI-Driven Social Media Analysis for Disaster Situational Awareness in Smart Urban Environments.*
https://www.researchgate.net/publication/391538352_AI-Driven_Social_Media_Analysis_for_Disaster_Situational_Awareness_in_Smart_Urban_Environments?utm

Reuters. *Spain's deadly DANA weather phenomenon & its links to climate change.*
https://www.reuters.com/business/environment/spains-deadly-dana-weather-phenomenon-its-links-climate-change-2024-10-30/

State.gov. *Joint Statement on the Second U.S.-Spain Cyber and Digital Dialogue (2021–2025).*
https://2021-2025.state.gov/joint-statement-on-the-second-u-s-spain-cyber-and-digital-dialogue/?safe=1

Stuttgarter Nachrichten. *Wo sind die Überschwemmungen in Spanien? 70 Tote durch „Gota Fría".*
https://www.stuttgarter-nachrichten.de/inhalt.wo-sind-die-ueberschwemmungen-in-spanien-70-tote-gota-fria.27fa464c-1153-46f8-b12c-5ffb8234e2ec.html

Water News Europe. *New maps double flood risks of Spanish homes.*
https://www.waternewseurope.com/new-maps-double-flood-risks-of-spanish-homes/?utm

Welt. *Brände in Südeuropa.*
https://www.welt.de/vermischtes/gallery4182874/Braende-Suedeuropa.html

Xataka Móvil. *Malla B y SIRDEE: sistemas de comunicación segura del Estado.*
https://www.xatakamovil.com/conectividad/malla-b-sirdee-sistemas-comunicacion-segura-estado-trabajan-para-reducir-riesgo-quedar-incomunicados

www.gtai.de/mep