ICEX España Exportación e Inversiones

FS FICHA SECTOR

DINAMARCA

Ciberseguridad en Dinamarca

A. CIFRAS CLAVE

El sector de la ciberseguridad en Dinamarca se enfrenta a retos importantes debido fundamentalmente a la alta incidencia de ciberataques. En particular, el 10 % de las pequeñas y medianas empresas (pymes) en el país escandinavo denuncian haber sido víctimas de ataques de seguridad, mientras que un preocupante 40 % de estas admite tener niveles de protección insuficientes. De hecho, sólo el 45 % de estas empresas había realizado formalmente evaluaciones de riesgo hasta el año 2020. Por otro lado, el Centro Nacional de la Policía para Delitos Económicos Relacionados con Tecnologías de la Información (LCIK, por sus siglas en danés) ha registrado un promedio anual de 27.000 informes de ciberataques financieros entre 2019 y 2022, originando un creciente interés por fortalecer la seguridad en línea en el país. A esta realidad se suma que el 65 % de las entidades gubernamentales danesas no cumple los estándares de seguridad básicos y que el 24 % de las pymes carece de sistemas de respaldo, destacando la imperiosa necesidad de mejorar la infraestructura de ciberseguridad.

Datos	Cifras	Impacto
Pymes víctimas de incidentes de ciberseguridad (%) [1]	10,0 %	Vulnerabilidad significativa de las pequeñas y medianas empresas frente a las amenazas cibernéticas.
Pymes con niveles de seguridad inadecuados (%)	40,0 %	Oportunidad para ofrecer servicios de ciberseguridad de preparación y protección contra ciberataques.
Media anual informes delitos financieros 2019-2022	27.000	Necesidad crítica de robustecer servicios de defensa y respuesta a incidentes.
Instituciones públicas danesas que han adoptado la ISO27001 (%)	57,0 %	Margen considerable para mejorar y expandir la implementación de estas prácticas críticas en el sector público.
Agencias gubernamentales danesas que no cumplen con medidas de seguridad básicas (%)	65,0 %	Necesidad urgente de mejora de la ciberseguridad en el sector público.

[1] Véase: https://en.digst.dk/media/27024/digst_ncis_2022-2024_uk.pdf

Sistemas críticos del Gobierno danés en estado vulnerable (%)	46,0 %	Necesidad de invertir en la protección y actualización de estos sistemas para salvaguardar servicios esenciales.
Empresas incapaces de encontrar personal cualificado en ciberseguridad (%)	22,0 %	Existencia de oportunidades de negocio para empresas que ofrezcan externalización de estos servicios.

B. CARACTERÍSTICAS DEL MERCADO

B.1. Definición y alcance del sector objeto de estudio

El mercado global de ciberseguridad, valorado en 148.000 millones de euros en 2021, se encuentra en una fase de expansión acelerada, estimándose un crecimiento anual del 14,5 %[2] hasta el año 2026. Este dinamismo se debe a la digitalización creciente de la economía y a una mayor conciencia de las vulnerabilidades digitales. En este contexto, se puede dividir el mercado en dos segmentos, soluciones (productos) y servicios. La primera rama consiste en las **soluciones de ciberseguridad** y estas se clasifican en *hardware, software* o una combinación de ambos, y se destinan principalmente a proveedores de servicios. Estas se agrupan en:

- **Soluciones de prevención:** herramientas como el ***Unified Threat Management*** (**UTM**) y los sistemas **IDS/IPS**, junto con cortafuegos **(*firewalls*)**, **antivirus** y ***antimalware***, se dedican a bloquear accesos no autorizados y evitar la fuga de información confidencial.

- **Soluciones de control:** se basan en la **Gestión de Identidades y Accesos** (**IAM**) y la **Gestión de Información y Eventos de Seguridad (SIEM)** para permitir sólo el acceso autorizado a recursos críticos y detectar comportamientos anómalos o brechas de seguridad, respectivamente. Son esenciales para proteger la integridad de los datos y cumplir las **normativas.**

- En cuanto a las **soluciones de mitigación,** incluyen tanto estrategias contra ataques **DDoS** (Ataque de Denegación de Servicio Distribuido) como planes de continuidad de negocio cruciales para reducir el impacto de incidentes y poder adaptar las defensas frente a nuevas amenazas.

Resulta relevante destacar aquí que la entrada al mercado nórdico con soluciones de ciberseguridad supone un desafío importante para las empresas españolas, ya que tienen que persuadir a los clientes daneses para que reemplacen sus soluciones vigentes, a menudo de procedencia no europea, por soluciones alternativas que sí satisfagan los rigurosos estándares requeridos. En estos supuestos, no sólo la calidad del producto es crucial, sino también lo es el desarrollo de una estrategia de promoción eficaz.

La segunda rama del mercado está constituida por los **servicios de ciberseguridad** (ofrecidos habitualmente por **consultoras, empresas integradoras y proveedores de servicios gestionados**) y juega una función esencial en la implementación y el mantenimiento de las soluciones expuestas previamente. Estos servicios abarcan desde la evaluación de riesgos y la implementación técnica hasta la gestión continua de la infraestructura de seguridad, incluyendo un enfoque centrado en la formación y educación para mejorar la concienciación de los empleados sobre la importancia de preservar la seguridad.

B.2. Tamaño del mercado

Dinamarca, con una superficie de 42.933 km² y una población de aproximadamente 5,9 millones de habitantes, cuenta con un PIB aproximado de 368.000 millones de euros. El país, reconocido por su alto nivel de vida y su desarrollado sistema de bienestar social, es sede de numerosas organizaciones internacionales relevantes como es el caso, por ejemplo, de la Agencia Europea del Medio Ambiente y de diversos organismos especializados de las Naciones Unidas: UNICEF, UNOPS o la UNFPA, todos ubicados en la capital danesa, Copenhague.

[2] Al respecto, véase: https://www.eib.org/attachments/lucalli/20220206-european-cybersecurity-investment-platform-en.pdf

En el ecosistema empresarial danés, especialmente entre las pymes, la preocupación por la ciberseguridad está en aumento. En este sentido, la Agencia danesa de Gobierno Digital (*Digitaliseringstyrelsen*) indica que alrededor del 10 % de las pymes ha experimentado incidentes de ciberseguridad. Más preocupante aun es que el 40 % de estas empresas no cuenta con un nivel de seguridad adecuado para protegerse de riesgos específicos. Esta realidad se agrava si se observa el siguiente dato: hasta el año 2020, sólo el 45 % de las pymes había realizado una evaluación de riesgos de ciberseguridad de manera formal.

Tras la creación del Centro Nacional de la Policía para el Delito Económico Relacionado con TI (LCIK, por sus siglas en danés) en diciembre de 2018, se han recibido una media de 27.000 informes de ciberdelitos financieros al año. Dado que hay alrededor de 290.000 pymes activas, este asunto es crítico para el sector y urge adoptar medidas contra la creciente amenaza cibernética.

B.3. Principales actores

El escenario danés de proveedores de soluciones TI y ciberseguridad se caracteriza por su gran diversidad, destacando la presencia desde consultoras generales hasta especialistas, conocidos como '*pure players'.*

Entre las firmas danesas más destacadas figuran las siguientes: **NetCompany A/S**, con ingresos de 249 MEUR, aunque no está especializada en temas de ciberseguridad. Asimismo, cabe citar a **KMD A/S** y **SDC A/S**, que ofrecen servicios de consultoría TI y soluciones para el sector financiero nórdico, respectivamente. De igual modo, debe mencionarse a la empresa **NNIT A/S** centrada en ciencias de la vida y con experiencia en el ámbito relativo al cumplimiento (*compliance*) en ciberseguridad, con unos ingresos de 63 MEUR.

AEVEN A/S y KOMBIT A/S son también empresas relevantes: en concreto, **KOMBIT A/S** (56 MEUR) está centrada en el área TI para el sector público. Por su parte, las empresas **CONSCIA (45 MEUR) y COLUMBUS (37 MEUR)** se distinguen por su enfoque exclusivo en ciberseguridad, sobresaliendo de manera especial **CONSCIA** por sus soluciones concretas e infraestructuras TI seguras.

Además de estas entidades con sede social en Dinamarca, cabe hacer referencia a las grandes consultoras globales como son **Deloitte**, **EY**, **KPMG**, y **PWC** (*The big four*), que ofrecen servicios de consultoría en ciberseguridad en sus amplios catálogos de servicios TI. Existe, además, una gama de empresas más pequeñas, pero cuyos ingresos provienen al 100 % de la ciberseguridad, a las que se conoce como *pure players*. Entre este tipo de empresas, resulta oportuno mencionar a **Dubex A/S** que lidera como consultora especializada en ciberseguridad y que cuenta con unos ingresos de 16,9 millones de euros; seguida por una variedad de firmas como **CAP MON** (1,2 MEUR) especializada en productos de ciberseguridad como SIEM y Log Management; y **Fortinet** (9 MEUR) dedicada a la venta de soluciones de ciberseguridad. Otras empresas destacables incluyen a **NetNordic** (6,4 MEUR), **CheckPoint Software** (3,9 MEUR), **Criipto** (0,5 MEUR), **CSIS Security Group** (10 MEUR), **Entrust** (5 MEUR), **Exclusive Networks** (1,3 MEUR), **PaloAlto Networks** (6,5 MEUR), **Trustzone** (3,2 MEUR), **Improsec** (5,3 MEUR), y **Truesec** (2,3 MEUR), contribuyendo cada una soluciones específicas y servicios de consultoría dentro del sector.

C. LA OFERTA ESPAÑOLA

En la última versión del Índice Global de Ciberseguridad (IGC)[3], publicado por la Unión Internacional de Telecomunicaciones (UIT) en 2021, España ocupa el cuarto puesto, sólo por detrás de EE. UU., Reino Unido y Estonia. Dinamarca, en cambio, ocupa el 32.º puesto; lo que indica que todavía tiene gran margen de mejora y que la posición española en este sector es fuerte y respetada.

Junto a las grandes consultoras internacionales activas tanto en España como a nivel mundial, existen empresas españolas especializadas en servicios de ciberseguridad que destacan de una manera especial por su fortaleza en el mercado. A modo de ejemplo, podemos destacar las siguientes: **Tarlogic (8 MEUR)** ofrece servicios de

[3] Informe de la UIT que, sobre la base de una serie de baremos técnicos, legales, organizativos y de crecimiento, trata de establecer un *ranking* mundial de ciberseguridad. Más información sobre dicho informe se encuentra disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

ciberseguridad. **BeDisruptive (82 MEUR)** se centra en servicios gestionados y consultoría en ciberseguridad. **Innotec (26 MEUR)** forma parte de Accenture, también proporciona una amplia gama de servicios en ciberseguridad. **SIA (105 MEUR)**, que forma parte de Indra Sistemas S.A., ofrece soluciones integrales que abarcan desde la identificación de riesgos hasta la recuperación. Por último, **S2 Grupo (31 MEUR)** crea tecnología propia para la gestión de amenazas y se sitúa dentro de la categoría de servicios, proporcionando consultoría y gestión de incidentes.

D. OPORTUNIDADES DEL MERCADO

La última Estrategia Nacional de Ciberseguridad danesa, de diciembre de 2021 (*Strategi om Cyber og Informationsikkerhed)*[4], vigente para el trienio 2022-2024, subraya la necesidad y urgencia de robustecer las defensas digitales en áreas clave para asegurar el progreso y bienestar de la sociedad. Este plan se articula en torno a varios ejes fundamentales:

- **Proteger la infraestructura digital:** la creciente dependencia de sistemas digitales para el funcionamiento de sectores críticos, como el sanitario, energético y alimentario hace imprescindible reforzar su protección contra interrupciones y ciberataques. Al respecto, la Estrategia danesa pone énfasis en blindar estos sistemas frente a amenazas conocidas que ya han impactado a estas cadenas de suministro esenciales.

- **Elaborar e implementar normativa sobre Seguridad en instituciones públicas:** se destaca la necesidad de que las entidades públicas implementen la norma ISO27001[5], cuya adopción actual en el país escandinavo apenas alcanza el 57 %. El texto de la Estrategia anticipa la introducción de mayores exigencias de seguridad, en contraste con la realidad de que un 65 % de las agencias gubernamentales danesas incumplen actualmente las medidas de seguridad elementales; mientras que un 46 % de los sistemas gubernamentales críticos muestran vulnerabilidades significativas**.**

- **Dar prioridad a la ciberseguridad en el sector empresarial:** la Estrategia danesa reconoce la ciberseguridad como un pilar crucial para el tejido empresarial danés y, en especial, para las pymes que se ven cada vez más afectadas por casos de ciberataques. En concreto, la Estrategia revela que un 24 % de las pymes no cuentan con sistemas de respaldo adecuados y apunta a una notable escasez de liderazgo competente en materia de ciberseguridad. Este último aspecto se evidencia por el dato que refleja que un 22 % de las empresas danesas se enfrentan a dificultades para contratar un *Chief Information Security Officer* (CISO)[6].

- **Educación ciudadana en materia de Seguridad digital:** con la vida diaria cada vez más digitalizada y el ascenso del cibercrimen, resulta esencial elevar la conciencia y las habilidades de la población danesa en materia de ciberseguridad. Sin embargo, la Estrategia indica que sólo un 16 % de los daneses sigue prácticas recomendadas para la creación de contraseñas seguras; mientras que un 21 % ha sido víctima de intentos de fraude telefónico.

La **regulación europea** también está abriendo bastantes oportunidades en el sector y continuará haciéndolo en un futuro próximo, ya que la normativa en el ámbito de la ciberseguridad se está ampliando de manera considerable y, a su vez, complicándose en cuanto a su contenido. La Unión Europea ha aprobado dos nuevas directivas comunitarias en esta materia: la **NIS2**[7] **y la CER**[8], aunque aún no se han transpuesto en Dinamarca, pero se espera lo hagan en el transcurso del presente año. La NIS2 incrementará los requisitos de notificación de incidentes y de informes para empresas esenciales en sectores críticos; mientras que la CER exigirá a las entidades danesas designadas como críticas realizar y actualizar análisis de riesgos, así como adoptar medidas de resiliencia

[4] *Strategi om Cyber og Informationsikkerhed,* de diciembre de 2021. Se puede acceder a dicha Estrategia en el siguiente enlace: https://digst.dk/strategier/cyber-og-informationssikkerhed/

[5] La norma ISO 27001 es un estándar internacional, aprobado en octubre de 2005 y cuya última versión fue publicada en octubre de 2022, que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información.

[6] *Vid.* https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

[7] *Vid.* Directiva NIS2: Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a medidas para garantizar un elevado nivel común de ciberseguridad en la Unión.

[8] *Vid.* Directiva CER: Directiva (UE) 2022/2557 del Parlamento Europeo y el Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas.

adecuadas. Así pues, la transposición de ambas directivas en el ordenamiento jurídico danés generará una serie de obligaciones formales para las grandes empresas en sectores críticos, lo que provocará un aumento de la demanda de servicios de ciberseguridad.

En este contexto, se anticipa un aumento de la demanda de las ya mencionadas empresas *pure players* en los próximos años[9]. Esto se debe, principalmente, a que las soluciones de ciberseguridad se están volviendo cada vez más complejas y su desarrollo e implementación exigirá la intervención de profesionales especializados, dado que los expertos en TIC más generales no siempre tienen conocimientos suficientes y adecuados para abordar estos desafíos.

E. CLAVES DE ACCESO AL MERCADO

E.1. Distribución

La estrategia de distribución difiere notablemente entre productos y servicios. En la distribución de productos, cabe destacar dos vías distintas de acceso: la primera vía consiste en la venta **directa**, óptima para soluciones específicas dirigidas a particulares o empresas con departamentos de ciberseguridad propios. Sin embargo, esta opción a menudo es difícil por dos motivos: los particulares, en general, no demandan muchos productos de ciberseguridad, más allá de los antivirus y a las empresas es complicado venderle un solo producto si no se les ofrece un servicio complementario, o un paquete de productos que cumplan una función específica.

La segunda vía consiste en la comercialización **indirecta**, que se perfila como la más conveniente por facilitar el acceso al mercado a través de socios tales como distribuidores, integradores, consultoras, o proveedores de servicios gestionados que necesitan estos productos para ofertar sus paquetes. Colaborar con socios locales resulta especialmente ventajoso, ya que permite una integración fluida del producto en la cartera de un proveedor establecido, aprovechando su base de clientes y relaciones previas, o comercializándolo directamente a estos proveedores. La decisión de asociarse con un socio local en vez de uno internacional es clave, ya que los locales simplifican y agilizan la entrada al mercado al conocer este de primera mano, además del idioma local y no sólo el inglés. También es conveniente considerar colaboraciones con grandes firmas de servicios no especializadas en ciberseguridad que busquen ampliar su catálogo. Si se opta por un socio internacional, es mejor elegir uno de gran tamaño que pueda aportar valor añadido a la oferta con su servicio o producto específico.

En cuanto a la distribución de **servicios** en Dinamarca, la dinámica es ligeramente diferente. Los clientes potenciales pueden ser tanto entidades públicas como empresas privadas. En los contratos de servicios con organismos públicos que superen los 143.000 euros[10] es obligatorio publicar la convocatoria de la licitación en el *Tenders Electronic Daily*, es decir, el Diario de Licitaciones Públicas de la UE (https://ted.europa.eu/). Este enlace permite a las empresas informarse sobre licitaciones abiertas y participar en ellas si cumplen los requisitos detallados en las bases/pliegos. En cuanto a los clientes privados, lo ideal es acceder a ellos a través de un socio ya establecido en el país que actúe en calidad de agente comercial o representante, ofreciendo ventajas competitivas como la cercanía, conocimiento profundo del mercado, la ventaja del idioma y la confianza. El sector de la ciberseguridad, con su amplia gama de servicios complementarios, abre puertas a colaboraciones estratégicas. Por ejemplo, la unión de un proveedor de servicios gestionados con una oferta de consultoría y análisis de riesgos, o al revés, es una gran oportunidad para que las empresas españolas entren y crezcan en este mercado. Acceder a clientes finales directamente con un servicio es posible, pero gran parte del éxito dependerá de la confianza y la reputación que tenga la empresa en Dinamarca. Si la empresa es totalmente nueva en el país, no se considera el modo más recomendado para acceder al mercado danés.

[9] Para más información, puede consultarse: https://op.europa.eu/en/publication-detail/-/publication/0be963c5-ca06-11e9-992f-01aa75ed71a1

[10] Todos los concursos públicos que superen unos determinados valores contractuales deben publicarse en el Suplemento del *Diario Oficial de la Unión Europea* que está disponible exclusivamente en formato electrónico y también puede accederse a él desde el sitio web del TED de manera gratuita: https://ted.europa.eu/ El importe de los contratos a partir del cual el concurso debe publicarse a nivel comunitario aparece recogido en las directivas de la UE. Los baremos que se aplican en la actualidad se encuentran previstos en: https://ted.europa.eu/es/simap/european-public-procurement

E.2. Marco legislativo y otras medidas aplicables

La legislación vigente en materia de ciberseguridad se caracteriza por ser diversa debido a su alto grado de especialización y complejidad técnica y, además, en Dinamarca, en tanto que país miembro de la UE, está armonizada con el Derecho comunitario. Este acervo normativo comunitario, que comprende desde reglamentos más generales hasta directivas específicas, crea oportunidades para los proveedores de ciberseguridad al requerir que las empresas adopten protocolos, obtengan certificaciones o adquieran productos específicos.

La pieza central de esta legislación es el Reglamento General 2016/679 de Protección de Datos (GDPR)[11] que obliga a las empresas a establecer medidas y protocolos de seguridad robustos para el tratamiento de los datos personales. Esta normativa no sólo protege la privacidad y los datos, sino que también abre oportunidades para muchos proveedores de ciberseguridad. Se complementa con esta ley interna danesa que exige realizar una Evaluación de Impacto (DPIA, por sus siglas en inglés) para evaluar y mitigar riesgos antes de procesar datos de alto riesgo y notificar a la Agencia de Datos Danesa (*Datatilsynet*) las brechas de seguridad en un plazo de 72 horas.

La Directiva de Seguridad de las Redes y Sistemas de Información (Directiva NIS)[12], de 19 de julio de 2016 y transpuesta en Dinamarca en mayo del 2018, exige que los proveedores de servicios esenciales en sectores clave como energía, transporte, finanzas, salud y telecomunicaciones, adopten medidas adecuadas para salvaguardar sus infraestructuras contra riesgos cibernéticos. Estas medidas y obligaciones jurídicas motivaron la creación en el país de entidades especializadas como, por ejemplo, el Centro de Ciberseguridad Danés (CFCS, por sus siglas en inglés) ante la necesidad de gestionar eficazmente estos riesgos.

Además, las empresas públicas deben adherirse a y cumplir el citado estándar internacional ISO/IEC 27001 sobre gestión de la seguridad de la información, lo que abre otra oportunidad de negocio para expertos en este campo.

La UE ha aprobado, el 17 de enero de 2023, la Ley de Resiliencia Operacional Digital (DORA) que establece un marco regulatorio para que las entidades financieras fortalezcan su capacidad de respuesta y recuperación frente a amenazas cibernéticas, contemplando incluso sanciones para las que no lo cumplan. Dicha Ley entrará en vigor en enero del 2025.

Únicamente resta indicar que hay una serie de leyes danesas que establecen obligaciones concretas en materia de ciberseguridad, aunque la mayoría de ellas están relacionadas con la obligación que tienen determinadas empresas de cumplir con la ISO 27001 antes mencionada:

- La Ley de 05/12/2023: sobre instituciones financieras exige que estas instituciones implementen *"medidas de control y seguridad adecuadas en el ámbito de la tecnología de la información (TI)".*
- Otra Ley de 12/12/2023: dirigida a los *Gatekeepers*, establece obligaciones formales en materia de ciberseguridad.
- Ley del 30/11/2023: que obliga a proveedores de redes y servicios electrónicos a cumplir una serie de obligaciones de seguridad cibernética, incluida la provisión de información detallada al ya referido Centro de Ciberseguridad CFCS.
- Ley de 08/06/2021: que permite al Centro de Ciberseguridad anular contratos con proveedores en infraestructuras críticas en base a su perfil de riesgo e historial.

E.3. Ferias

En Dinamarca, cabe destacar las siguientes ferias sectoriales que se celebrarán en el presente año y en las que se reúnen las principales empresas de ciberseguridad del país escandinavo, con otras muchas de fuera.

[11] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Para conocer el contenido de dicho Reglamento, puede consultarse el enlace: https://eur-lex.europa.eu/ES/legal-content/summary/general-data-protection-regulation-gdpr.html

[12] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión. Puede accederse a dicha Directiva a través del siguiente enlace: https://www.retsinformation.dk/eli/lta/2018/436

TABLA 1. FERIAS SOBRE CIBERSEGURIDAD EN DINAMARCA

Evento	Fecha	Lugar	Web
V2 Security Expo	1 al 2 de mayo de 2024	Øksnehallen, Copenhague	www.v2security.dk/24
Nordic Cybersecurity Summit 2024	17 al 18 de septiembre de 2024	Copenhague	https://nordic.cyberseries.io/
Nordic Information Security Network 2024	2 al 3 de diciembre de 2024	Scandic Copenhagen Hotel, Copenhague	https://thenetwork-group.com/nordic-information-security-network/

Fuente: 10times.com

Aparte de las ferias arriba mencionadas, hay una serie de charlas, conferencias y eventos que podrían ser de interés para interactuar con empresas y clientes locales.

TABLA 2. CONFERENCIAS, SEMINARIOS, *WORKSHOPS* Y EVENTOS SOBRE CIBERSEGURIDAD

Evento	Fecha	Lugar	Web
Cyber Security Strategy Day 2024	11 de junio de 2024	Hotel Ottilia, Frederiksberg	https://computerworldevents.dk/1378/cyber-security-strategy-day-2024
Information Security Conference and Privacy	13 al 17 de junio de 2024	DTU, Lyngby	https://ifipsec.org/
5th International Conference on HCI for Cybersecurity, Privacy and Trust	23 al 28 de julio de 2024	Copenhague	https://2023.hci.international/hci-cpt
The International Conference on Science of Cyber Security 2024	12 al 14 de agosto de 2024	Scandic Copenhagen Hotel, Copenhague	https://scisec.org/
Computerworld's Cyber Security Summit 2024	27 de agosto de 2024	Sav-vaerket, Tranbjerg J,	https://computerworldevents.dk/1420/cyber-security-summit-2024-jylland
Cyber Security in the Financial Sector 2024	18 al 19 de septiembre de 2024	Charlottehaven, Copenhague	https://10times.com/cyber-safety-in-financial-sector
Copenhagen CyberCrime Conference 2024	19 de septiembre de 2024	Industriens Hus, Copenhague	https://www.cyberhagen.com/event/54a48e52-6585-46bd-9e0b-b937229c7d8d/summary

Fuente: 10times.com

E.4. Instituciones y actores relevantes

1. ***Center for Cybersikkerhed* –Centro de Ciberseguridad–** (https://www.cfcs.dk/da/)**:** actúa como la autoridad nacional en materia de seguridad TIC. Ofrece servicios de asesoramiento y tiene la capacidad de detectar y advertir sobre ciberataques avanzados. Además, emite alertas sobre amenazas específicas y elabora informes de situación y evaluaciones de amenazas a nivel nacional y sectorial.
2. ***Forsvarets Efterretningstjeneste* –Servicio de Seguridad e Inteligencia de Dinamarca–** (https://www.fe-ddis.dk)**:** es la autoridad nacional en seguridad y ofrece consultoría y asistencia en asuntos de seguridad a autoridades y empresas privadas, incluyendo la gestión y almacenamiento seguro de documentos.

3. ***Digitaliseringsstyrelsen* –Agencia Danesa de Gobierno Digital–** (https://digst.dk/)**:** apoya la seguridad de la información en el sector público, proporcionando orientación sobre la norma ISO 27001 y estableciendo requisitos para las agencias gubernamentales. También lleva a cabo tareas de información orientadas al ciudadano y coordina la implementación de estrategias de seguridad digital junto con el Ministerio de Defensa danés.
4. ***Erhvervsstyrelsen* –Autoridad de Negocios de Dinamarca–** (https://erhvervsstyrelsen.dk/)**:** desarrolla conocimiento, directrices y herramientas para fortalecer la seguridad digital en la comunidad empresarial, enfocándose especialmente en las pequeñas y medianas empresas (pymes).
5. ***Dansk Industri* –Confederación de la Industria Danesa–** (https://www.danskindustri.dk/)**:** Confederación de la Industria Danesa, una organización privada financiada, propiedad y administrada en su totalidad por 10.000 empresas de las industrias manufacturera, comercial y de servicios.

E.5. Asociaciones sectoriales

- ***IT-Branchen* –Asociación de Empresas de TI–** (https://itb.dk/)**:** se centra en asesorar y asistir a sus miembros, la industria y la sociedad para crecer mediante la creación de una sociedad digital que beneficie al clima, la economía y las personas. Su objetivo es hacer de Dinamarca un referente mundial en el uso de la tecnología.

- ***DPO-Foreningen* –Asociación Danesa de Protección de Datos–** (https://www.danmarksdpoforening.dk/)**:** tiene como objetivo principal el promover un entendimiento común sobre el cumplimiento del Reglamento General de Protección de Datos (GDPR) y la Ley de Protección de Datos antes mencionados.

F. CONTACTO

La ***Oficina Económica y Comercial de España en Copenhague*** está especializada en ayudar a la internacionalización de la economía española y la asistencia a empresas y emprendedores en **Dinamarca.**

Entre otros, ofrece una serie de **Servicios Personalizados** de consultoría internacional con los que facilitar a dichas empresas: el acceso al mercado de Dinamarca, la búsqueda de posibles socios comerciales (clientes, importadores/distribuidores, proveedores), la organización de agendas de negocios en destino, y estudios de mercado ajustados a las necesidades de la empresa. Para cualquier información adicional sobre este sector contacte con:

Vestebrogade, 10, 1er piso
Copenhague V, 1620, Dinamarca
Teléfono: +45 3331 2210
Correo electrónico: copenhague@comercio.mineco.es
http://Dinamarca.oficinascomerciales.es

Si desea conocer todos los servicios que ofrece ICEX España Exportación e Inversiones para impulsar la internacionalización de su empresa contacte con:

Ventana Global
913 497 100 (L-J 9 a 17 h; V 9 a 15 h)
informacion@icex.es

Para buscar más información sobre mercados exteriores siga el enlace

INFORMACIÓN LEGAL: Este documento tiene carácter exclusivamente informativo y su contenido no podrá ser invocado en apoyo de ninguna reclamación o recurso.

ICEX España Exportación e Inversiones no asume la responsabilidad de la información, opinión o acción basada en dicho contenido, con independencia de que haya realizado todos los esfuerzos posibles para asegurar la exactitud de la información que contienen sus páginas.

AUTOR
Jesús Rodríguez-Nogueras Candau

Oficina Económica y Comercial
de España en Copenhague
copenhague@comercio.mineco.es
Fecha: 05/03/2024

NIPO: 22424012X